УТВЕРЖДАЮ:
Директор КОГБУК «Кировская областная специальная библиотека для слепых»
_____Т.Н.Мурина
приказ от «13» 07 2023 г. № 54-ОД

Политика в области обработки и защиты персональных данных в Кировском областном государственном бюджетном учреждении культуры «Кировская областная специальная библиотека для слепых» (далее - Политика)

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая политика разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «0 персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Трудовым кодексом РФ, Указом Президента Российской Федерации № 188 «Об утверждении Перечня сведений конфиденциального характера», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Правилами внутреннего трудового распорядка, Правилами пользования библиотекой.

Политика раскрывает основные категории персональных данных, обрабатываемых в КОГБУК «Кировская областная специальная библиотека для слепых» (далее - Оператор), цели, способы и принципы обработки Оператором персональных данных, права и обязанности Оператора при обработке персональных данных, права субъектов персональных данных, а также перечень мер, применяемых Оператором в целях обеспечения безопасности персональных данных при их обработке.

Положения Политики служат для обеспечения защиты прав и свобод граждан при обработке персональных данных, определения порядка обработки персональных данных, установления ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, а также служат основой для разработки локальных нормативных актов, регламентирующих вопросы обработки персональных данных сотрудников, пользователей и других субъектов персональных данных.

Основные понятия, используемые в Политике:

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

оператор 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) с персональными данными, совершаемых с использованием средств автоматизации или без их использования.

Обработка персональных данных включает в себя, в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

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.

2. ИНФОРМАЦИЯ ОБ ОПЕРАТОРЕ, ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Сведения об Операторе персональных данных.

Название организации: Кировское областное государственное бюджетное учреждение культуры «Кировская областная специальная библиотека для слепых».
ИНН: 4345523873.
Адрес: 610035, Кировская область, г. Киров, ул. Сурикова, д. 10. пом. 5.
Тел.:(8332) 325-100.
Сайт: www.kirovsbs.ru.
ОГРН: 1234300002420.

2.2. Цели обработки персональных данных:

- подготовка, заключение и обеспечение обязательств по трудовым договорам, договорам гражданско-правового характера и договоров с контрагентами;

– обеспечения пропускного и внутриобъектового режимов;

– повышение оперативности и качества обслуживания пользователей библиотеки;

– обеспечение сохранности библиотечного фонда в соответствии с правилами пользования библиотекой;

– в иных законных целях.

3. ОСНОВНЫЕ ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Согласно ст. 5 Закона № 152-ФЗ при обработке персональных данных должны соблюдаться следующие принципы:

– обработка персональных данных должна осуществляться на законной и справедливой основе;

– обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

– не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

– обработке подлежат только персональные данные, которые отвечают целям их обработки;

– содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки;

– хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. ОБРАБАТЫВАЕМЫЕ КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИСТОЧНИКИ ИХ ПОЛУЧЕНИЯ

Оператором обрабатываются персональные данные следующих категорий субъектов:

– персональные данные сотрудников Оператора, бывших сотрудников, кандидатов на замещение вакантных должностей. Источник получения: субъект персональных данных. Основание: письменное согласие субъекта, Трудовой кодекс РФ;

– персональные данные пользователей и иных контрагентов Оператора. Источник получения: субъект персональных данных. Основание: письменное согласие субъекта, Гражданский кодекс РФ.

4.1. Состав, получение и обработка персональных данных, доступ к персональным данным сотрудников, права сотрудников

4.1.1. В состав персональных данных сотрудников Оператора входят документы, сопровождающие процесс оформления трудовых отношений при их приеме, переводе и увольнении.

4.1.2. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет администрации Оператора:

– паспорт или иной документ, удостоверяющий личность;

– трудовую книжку, за исключением случаев, когда трудовой договор заключается

впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

– страховое свидетельство государственного пенсионного страхования;

– документы воинского учета для военнообязанных и лиц, подлежащих воинскому учету;

– документ об образовании, о квалификации или наличии специальных знаний при поступлении на работу, требующую специальных знаний или специальной подготовки;

– свидетельство о присвоении ИНН (при его наличии у работника).

4.1.3. При приеме на работу инспектором по кадрам Оператора заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

– общие сведения (Ф.И.О. работника, число, месяц и год рождения, место рождения, гражданство, образование, профессия, стаж работы, паспортные данные, сведения об инвалидности);

– сведения о воинском учете; данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

– сведения о переводах на другую работу;

– сведения об аттестации;

– сведения о повышении квалификации;

– сведения о профессиональной переподготовке;

– сведения о наградах (поощрениях), почетных званиях;

– сведения об отпусках;

– сведения о социальных гарантиях;

– сведения о месте жительства и контактных телефонах.

4.1.4. Инспектором по кадрам Оператора создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

– документы, содержащие персональные данные работников (подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу, подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству библиотеки, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);

– документация по организации работы библиотеки: штатное расписание, положения о структурных подразделениях, должностные инструкции, приказы, распоряжения, указания администрации, документы по планированию, учету, анализу и отчетности в части работы с персоналом.

4.1.5. Источником персональных данных о работнике является сам субъект персональных данных. Если персональные данные работника, возможно получить только у третьей стороны, то работник уведомляется об этом заранее и от него получается письменное согласие. Администрация сообщает работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказ работника дать письменное согласие на их получение.

4.1.6. Согласие работника не требуется в следующих случаях:

– обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

– обработка персональных данных осуществляется в целях исполнения трудового договора;

– обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

4.1.7. Право доступа к персональным данным работников имеют:

- директор библиотеки;
- юрисконсульт;
- сотрудники бухгалтерии;
- руководители структурных подразделений по направлению деятельности (доступ к персональным данным только работников своего подразделения).

4.1.8. Сотрудники Оператора имеют право:

– получать свободный доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей их персональные данные;

– требовать от администрации уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для администрации персональных данных;

– получать от администрации 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 субъекта персональных данных может повлечь за собой обработка его персональных данных;

– требовать извещения администрацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжаловать в уполномоченный орган по заушите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия администрации при обработке и защите их персональных данных.

4.1.9. Копировать и делать выписки персональных данных работника разрешается исключительно в служебных целях с письменного разрешения юрисконсульта.

4.1.10. Передача информации третьей стороне возможна только при письменном согласии сотрудника, если иное не установлено федеральным законом.

4.1.11. Для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться к Оператору. Оператор в течение 5-ти рабочих дней рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

4.2. Состав, получение и обработка персональных данных, доступ к персональным данным пользователей, права пользователей

4.2.1. В состав персональных данных пользователей Оператора входят сведения необходимые для повышения оперативности и качества обслуживания, организации адресного, дифференцированного и индивидуального обслуживания, а также соблюдения пропускного режима, установленного Правилами пользования библиотекой; обеспечения сохранности библиотечного фонда в соответствии с Правилами пользования библиотекой;

исполнения Приказа Федеральной службы государственной статистики от 30 декабря 2015 г. N 671 «Об утверждении статистического инструментария для организации Министерством культуры РФ статистического наблюдения за деятельностью учреждений культуры».

4.2.2. Перечень персональных данных, вносимых в формуляр пользователя (см. Приложение 2):

- фамилия, имя и отчество пользователя;
- число, месяц и год рождения;
- сведения о документе, удостоверяющем личность (название, серия, номер и т.д.);
- контактный телефон;
- адрес электронной почты;
- адрес регистрации по месту жительства;
- адрес по месту временного пребывания;
- род деятельности;
- группа инвалидности;
- данные о сопровождающих лицах (ФИО, степень родства, контактный телефон).

4.2.3. Персональные данные пользователей являются конфиденциальной информацией, не подлежащей разглашению, и не могут быть использованы библиотекой или ее сотрудниками для целей, не перечисленных в п. 4.2.1 настоящей Политики.

4.2.4. Условия и порядок обработки персональных данных пользователей:

– персональные данные пользователей Оператора на бумажных носителях хранятся в отделе регистрации и контроля (регистрационная карточка, см. Приложение 2), отделах с функциями обслуживания (формуляр) в запираемых на замок ящиках. Доступ к ящикам с персональным данными пользователей имеют только сотрудники соответствующего отдела. Обработка персональных данных на бумажных носителях выполняется в соответствии с Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– персональные данные пользователя уточняются ежегодно при первом посещении пользователем библиотеки в году, следующем за годом регистрации, либо годом последнего уточнения персональных данных;

– персональные данные пользователей хранятся в течение 5 лет с момента последней перерегистрации пользователя;

– по истечении пятилетнего срока, если пользователь не имеет задолженности перед библиотекой (выданная во временное пользование литература, пени) и не пользуется ее услугами, персональные данные пользователя подлежат уничтожению. Об уничтожении составляется соответствующий акт. Образец акта представлен в Приложении №3. В случае наличия задолженности персональные данные пользователя блокируются, а уничтожаются и обезличиваются только после снятия задолженности;

– сотрудники отдела регистрации и контроля вправе передавать персональные данные пользователей работникам других структурных подразделений Оператора в объёме, необходимом для исполнения ими служебных обязанностей и согласно их должностным инструкциям, а также в случаях, установленных законодательством и настоящей Политикой;

– директор библиотеки может передавать персональные данные пользователя третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровья пользователя, а также в иных случаях, установленных действующим законодательством;

– 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;

– хранить сведения, содержащие персональные данные, обязательно в запираемых ящиках, доступ к которым имеет ограниченный круг лиц, а именно сотрудники данного отдела;

– 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 допускается только при условии предварительного согласия пользователя, выраженного в письменной форме и прекращается немедленно по его письменному требованию;

– иные права, обязанности, действия сотрудников Оператора, в трудовые обязанности которых входит обработка персональных данных пользователей, определяются должностными инструкциями.

4.2.5. Пользователь имеет право на получение при обращении в библиотеку следующей информации:

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

Получение данной информации возможно только после предъявления паспорта.

4.2.6. Обязанности Оператора в отношении обработки персональных данных пользователей:

- Оператор 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;
- Оператор осуществляет передачу персональных данных пользователя только в соответствии с настоящей Политикой и законодательством РФ;
- Оператор обязан сообщить пользователю информацию о наличии его персональных данных, а также предоставить возможность ознакомления с ними (при предъявлении паспорта);
- Оператор обязан 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 Оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Оператор уведомляет пользователя или его законного представителя и третьих лиц, которым персональные данные этого пользователя были переданы;
- в случае выявления недостоверных персональных данных или неправомерных действий с ними Оператор при обращении или по запросу пользователя осуществляет блокирование персональных данных, относящихся к соответствующему пользователю, с момента такого обращения на период проверки;
- в случае подтверждения факта недостоверности персональных данных Оператор на основании документов, представленных пользователем или его законным представителем, уточняет персональные данные и снимает их блокирование;

- все обращения субъектов персональных данных фиксируются в журнале учета обращений (Приложение № 4). Журнал учета обращений хранится в канцелярии.

4.2.7. Для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться к Оператору. Оператор в течение 5-ти рабочих дней рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

5. ОТВЕТСТВЕННОСТЬ

5.1. Субъект персональных данных вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите прав субъектов персональных данных.

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

5.3. В случае нарушения норм, регулирующих обработку и защиту персональных данных лица, виновные в нарушении, несут гражданскую, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

6. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. Обеспечение безопасности персональных данных достигается, в частности:

- назначением руководителей структурных подразделений ответственными соблюдение настоящей Политики;
- осуществлением внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 N 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам;
- ознакомлением сотрудников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных;
- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;
- запрещается создавать электронные копии сведений, содержащих персональные данные, а также заниматься их автоматизированной обработкой на рабочих местах, не оборудованных средствами защиты информации;
- в случае, если рабочее место оборудовано средствами защиты информации, то от субъекта персональных данных должно быть получено письменное согласие на

обработку персональных данных, если иное не предусмотрено законодательство или локальными актами.

6.1. Управление учетными записями пользователей

С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах в конкретной информационной системе персональных данных, должна быть создана уникальная учетная запись пользователя.

6.2. Политика антивирусной защиты

- Лицензионное антивирусное ПО должно быть установлено на всех рабочих местах, задействованных в обработке данных пользователей и\или сотрудников.
- Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляются специалистами, ответственными за техническое обеспечение информационных систем Оператора.
- Обновление антивирусных баз должно производиться регулярно автоматическом режиме.
- Специалисты, ответственные за техническое обеспечение информационных систем Оператора, осуществляют периодическое обновление антивирусных пакетов и контроль их работоспособности.
- Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.
- На компьютеры запрещается установка программного обеспечения, не связанного

выполнением функций, предусмотренных технологическим процессом обработки информации.

- При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить обработку данных;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов специалистов, ответственные за техническое обеспечение, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

6.3. Политика «чистого стола» и «чистого экрана»

С целью минимизации риска неавторизованного доступа или повреждения документов на бумажных носителях, носителей данных и средств обработки информации следует применять политику «чистого стола» в отношении документов на бумажных носителях и сменных носителей данных, а также политику «чистого экрана» в отношении средств обработки информации с тем, чтобы уменьшить риски неавторизованного доступа, потери и повреждения информации как во время рабочего дня, так и при внеурочной работе. Носители информации. оставленные на столах, также могут быть повреждены или разрушены при бедствии, например, при пожаре, затоплении. Следует применять следующие мероприятия по управлению информационной безопасностью:

- чтобы исключить компрометацию информации, целесообразно бумажные и электронные носители информации, когда они не используются, хранить в запирающихся шкафах и/или в других защищенных предметах мебели, особенно в нерабочее время;
- носители со служебной информацией, сведениями, содержащими персональные данные, когда они не требуются, следует убрать со стола и запирать (например, в несгораемом сейфе или металлическом шкафу), особенно когда помещение пустует;
- персональные компьютеры и принтеры должны быть выключены по окончании работы;
- следует применять пароли, блокировку экрана (сочетание клавиш win+ L, команда Пуск - Блокировать) или другие мероприятия в отношении устройств, находящихся без присмотра;
- в нерабочее время фотокопировальные устройства следует запирать на ключ (или защищать от неавторизованного использования другим способом);
- напечатанные документы с персональными данными, необходимо изымать из принтеров немедленно;
- запрещается оставлять сведения, содержащие персональные данные, в свободном доступе на столах;
- ключи, электронные ключи от помещений, где могут храниться сведения, содержащие персональные данные, не следует оставлять в свободном доступе на столах.

6.4. Политика резервного копирования

Резервное копирование информации, размещенной на рабочих местах сотрудников, осуществляется сотрудниками структурных подразделений в выделенные сетевые каталоги на файловом сервере Оператора. Актуальность, глубина резервируемых данных также самостоятельно контролируется сотрудниками структурных подразделений.

Права доступа к сетевым каталогам должны исключать возможность доступа пользователей к резервным копиям других пользователей и система, хранящихся на сервере.

Резервное копирование информации, размещенной на серверах Оператора, осуществляется сотрудниками отдела автоматизации. Глубина серверных резервных копий должна составлять не менее 7 дней (минимум 7 исторических состояния). Резервное копирование баз данных должно осуществляться ежедневно.

6.5. Политика парольной защиты

Доступ к программному обеспечению, используемому пользователями и администраторами в рамках должностных обязанностей и подразумевающему наличие идентификации и аутентификации пользователя и разграничение полномочий, без использования пароля запрещено. Пароли доступа к различному прикладному программному обеспечению, используемому пользователями и администраторами в рамках должностных обязанностей должны отличаться от паролей доступа к автоматизированным рабочим местам или элементам сетевой инфраструктуры и не должны совпадать для различного программного обеспечения.

Минимальные требования к сложности пароля:

– пароль не должен содержать имя учетной записи пользователя или какую-либо его часть или включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (LAN, USER и т.п.);

– пароль должен состоять не менее чем из 8 (восьми) символов;

– в пароле должны присутствовать символы трех категорий из числа следующих четырех:

– прописные буквы английского алфавита от A до Z;

– строчные буквы английского алфавита от a до Z;

– десятичные цифры (от 0 до 9) и\или неалфавитные символы (например, !, S, #, %);

– хранение работником значений своих паролей на бумажном носителе НЕ допускается;

– в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых работников в их отсутствие, производится внеплановая смена пароля;

– внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой;

– контроль за сохранность пароля возлагается на владельца учетной записи;

– рекомендуется ежегодная плановая смена паролей.

6.6. Политика обеспечения сетевой безопасности

Доступ к серверам, сетевому оборудованию и иному оборудованию корпоративной сети должен быть ограничен. По возможности оборудование должно размещаться в отдельных помещениях с соблюдением требований к организации серверных помещений, запираться на ключ, доступ в помещения должен фиксироваться видеонаблюдением. Лица, не уполномоченные для работы с оборудованием иили лица, не являющиеся сотрудниками организации, должны допускаться в помещение только в сопровождении уполномоченных сотрудников Оператора.

В конфигурации оборудования обязательно должны быть заданы логин и пароль, устройства должны иметь ограниченный доступ в ЛВС организации, минимально необходимый для функционирования.

Запрещается подключение посторонних устройств к ЛВС организации, исключение составляет гостевая сеть wi-fi для пользователей Оператора.

6.7. Политика использования сети Интернет, социальных сетей и электронной почты

Вся информация, полученная из сети Интернет, должна считаться недостоверной, не будучи подтвержденной из других источников. Перед использованием свободно распространяемой информации из сети Интернет, такая информация должна быть перепроверена в других источниках. Оператор не несет ответственности за информацию, содержащуюся в сети Интернет. В случае открытия пользователем ресурсов, содержание которых может считаться незаконным или оскорбительным, например, материалы сексуального характера, расистские, дискредитирующие, оскорбительные, непристойные, уничижительные, дискриминационные, угрожающие, пользователь/сотрудник обязан прекратить работу с данным ресурсом.

Электронная почта и социальные сети должна быть использованы сотрудниками только для выполнения должностных обязанностей.

Запрещается переход по ссылкам, полученным в сообщениях электронной почты, если отправитель неизвестен получателю.

Запрещено использовать социальные сети, электронную почту для отправления сообщений следующего содержания:

- сообщения, содержащие сведения, составляющие персональные данные (подробнее см. Приложение 5);
- сообщения, содержание которых может считаться незаконным или оскорбительным, например, материалы сексуального характера, расистские,

дискредитирующие, непристойные, уничижительные, угрожающие, или иные подобные сообщения;

- любых подрывных, неэтичных, незаконных или недопустимых материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений или о национальном происхождении, гиперссылок или других ссылок на неприличные или очевидно оскорбительные веб-сайты и подобные материалы;
- сообщений, написанных таким образом, который может быть интерпретирован как официальная позиция или высказывание, если это не разрешено руководством Оператора.

6.8. Политика повышения осведомленности в области ИБ и кадровая политика

Рекомендуется проводить мероприятия, направленные на постоянное повышение осведомленности сотрудников Оператора в области информационной безопасности, в том числе по направлению защиты персональных данных. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов информационных систем, организаций-лицензиатов ФСТЭК России и ФСБ России.

Конкретные требования по обеспечению защиты персональных данных должны быть внесены в должностные регламенты всех сотрудников Оператора, в зависимости от их должностных обязанностей. Руководители структурных подразделений несут ответственность за осведомление сотрудников с данной Политикой. Каждый сотрудник песет личную ответственность за соблюдение данной Политики.

Подбор, и порядок вступления в договорные и трудовые отношения и их расторжения, а также ежедневное выполнение сотрудником его должностных обязанностей, должны соответствовать требованиям нормативно-правовых актов РФ, локальных актов Оператора в области зашиты персональных данных.

Порядок допуска сотрудника к работе с информацией ограниченного доступа, в том числе персональными данными, порядок работы с такой информацией и порядок прекращения допуска к такой информации, должен соответствовать нормативно-правовым актам РФ, локальным актам Оператора в области защиты персональных данных. К работе с персональными данными допускаются только сотрудники, прошедшие инструктаж по обеспечению безопасности персональных данных.

6.9. Действия, запрещенные сотруднику

Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных и имеющий доступ в помещение, в котором производится обработка персональных данных, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с персональными данными;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах;
- хранить в тайне свой пароль (пароли) и с установленной периодичностью менять свой пароль (пароли);
- хранить ключи в сейфе или ящике, закрывающемся на ключ;
- выполнять требования настоящей Политики в полном объеме.

Сотруднику категорически запрещается:

– предоставлять доступ к информации, содержащей персональные данные, лицам, не допущенным к их обработке;

– самостоятельно изменять конфигурацию аппаратно-программных средств;

– осуществлять действия по преодолению установленных ограничений на доступ к персональным данным;

– отключать или изменять конфигурацию средств защиты информации;

– устанавливать на автоматизированное рабочее место программное обеспечение, не связанное с исполнением служебных обязанностей;

– сообщать кому-либо устно или письменно личные атрибуты доступа к рабочему месту и учетным записям;

– производить какие-либо изменения в подключении и размещении технических средств;

– оставлять бесконтрольно, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры) автоматизированное рабочее место с загруженными персональными данными, с установленными маркированными носителями, а также распечатываемыми бумажными документами с персональными данными.

6.10. Права сотрудника

Сотрудник имеет право:

- обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленного объема и полномочий:
- получать от лиц, ответственных за защиту информации в автоматизированных системах, консультативную помощь по вопросам эксплуатации автоматизированных средств.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящая Политика вступает в силу с даты ее утверждения.

При необходимости приведения настоящей Политики в соответствие с вновь принятыми законодательными актами изменения вносятся на основании Приказа руководителя.

Настоящая Политика распространяется на всех пользователей и сотрудников, имеющих доступ и осуществляющих обработку персональных данных сотрудников и пользователей Оператора.

Пользователи, сотрудники, а также их законные представители имеют право ознакомится с настоящей Политикой.

Сотрудники Оператора подлежат ознакомлению с данным документом в порядке, предусмотренном Приказом руководителя, под личную подпись.

В обязанности сотрудников, осуществляющих первичный сбор персональных данных, входит получение согласия субъекта на обработку его персональных данных под личную подпись.

Пользователи, сотрудники, а также их законные представители имеют право ознакомиться с настоящей Политикой.

В обязанности сотрудников, осуществляющих первичный сбор персональных данных, входит получение согласия субъекта на обработку его персональных данных под личную подпись.

Ответственным сотрудником за организацию работы с персональными данными в учреждении назначен юрисконсульт (тел. 8(8332)325-100, kirov.sbs@yandex.ru).

Приложение 1

Регистрационная карточка пользователя

№ _____ к _____

Я, _____
(Ф.И.О.)

Паспорт (серия, номер) _____

Кем, когда, выдан _____

Адрес регистрации _____

Адрес проживания _____

Категория (заполняется сотрудником) _____

Дата рождения _____ Образование _____

Контактный тел. _____

E-mail: _____

Группа инвалидности _____

Данные о сопровождающих лицах (Ф.И.О., степень родства, контактный тел.)_____

_____

Сотрудник, проверивший введенные данные_____

Подтверждаю, что я ознакомлен и полностью согласен с условиями оказания мне библиотечных услуг КОГБУК «Кировская областная специальная библиотека для слепых» (ул. Сурикова, 10), изложенными в «Правилах пользования библиотекой». Я согласен(на) с тем, что Библиотека может отказать мне в обслуживании в случае их нарушения. Также даю свое согласие на обработку (сбор, систематизацию, хранение, уточнение, обезличивание и уничтожение) моих персональных данных, указанных в формуляре, в целях:

- повышения оперативности и качества обслуживания читателей;
- обеспечения сохранности библиотечного имущества;
- соблюдения Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- исполнения Постановления Правительства РФ от 02.06.2008 № 420 «О Федеральной службе государственной статистики».

Я согласен(на) с тем, что Библиотека вправе напоминать мне о взятых на дом изданиях, в случае просрочки и даты их возврата по телефону, направлением уведомления по почте.
Данное согласие действует до моего прямого отказа от пользования услугами Библиотеки выраженного мною лично в письменной форме либо до ликвидации учреждения.

_____ _____ _____

Дата Подпись Расшифровка подписи

Приложение 2

АКТ № _____

об уничтожении персональных данных пользователей библиотеки

г. Киров «___»_____ 20__ г.

Комиссия, созданная приказом директора библиотеки от «___» _____20__ г. № ___, в составе:

Председатель _____

(должность, Ф.И.О)

Члены комиссии:

_____

(должность, Ф.И.О)

_____

(должность, Ф.И.О)

_____

(должность, Ф.И.О)

в соответствии со ст. 21 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» составила настоящий акт об уничтожении персональных данных субъектов персональных данных, обрабатываемых КОГБУК «Кировская областная специальная библиотека для слепых», находящаяся по адресу: 610035, г. Киров, ул. Сурикова, д. 10.

Ф.И.О. субъектов, чьи персональные данные были уничтожены	**Перечень категорий уничтоженных персональных данных**	**Наименование ИСПДн, из которой были уничтожены персональные данные**	**Способ уничтожения персональных данных**	**Причина уничтожения персональных данных**	**Дата уничтожения персональных данных**