УТВЕРЖДЕНО
приказом директора ГБУК «Самарская областная библиотека для слепых» от 20 сентября 2022 г.
№ 130

ПОЛОЖЕНИЕ О ПОРЯДКЕ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ КУЛЬТУРЫ «САМАРСКАЯ ОБЛАСТНАЯ БИБЛИОТЕКА ДЛЯ СЛЕПЫХ»

г. Самара, 2022 г.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение разработано в соответствии с положениями Трудового кодекса Российской Федерации (в действующей редакции), введённого в действие Федеральным законом Российской Федерации от 30 декабря 2001 г. № 197-ФЗ, Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных (в действующей редакции), нормативными правовыми актами Российской Федерации в области персональных данных, и предназначено для определения порядка работы с персональными данными работников в ГБУК «Самарская областная библиотека для слепых».

2. Настоящим Положением регулируются отношения, связанные с обработкой персональных данных, осуществляемой в ГБУК «Самарская областная библиотека для слепых» с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств позволяет осуществлять поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Действие настоящего Положения распространяются на информацию, являющуюся персональными данными, независимо от вида носителя, на котором она зафиксирована, за исключением персональных данных, отнесенных в соответствии с законодательством Российской Федерации к сведениям, составляющим государственную тайну.

3. Настоящее Положение вступает в силу с момента утверждения приказом директора ГБУК «Самарская областная библиотека для слепых» и действует до его отмены либо до принятия нового локального акта.

Внесение изменений и дополнений в настоящее Положение осуществляется после утверждения их приказом директора ГБУК «Самарская областная библиотека для слепых». Указанные изменения и дополнения доводятся до сведения всех работников ГБУК «Самарская областная библиотека для слепых», допущенных в установленном порядке к работе с персональными данными, под личную подпись.

4. В настоящем Положении используются следующие основные понятия:

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

Персональные данные, разрешенные субъектом персональных

данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

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;

Р**аспространение 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.

Подразделение ГБУК «Самарская областная библиотека для слепых» - подразделение, обозначенное в организационной структуре ГБУК «Самарская областная библиотека для слепых» в качестве самостоятельного объекта, не входящего в структуру другого подразделения.

Федеральный закон - Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных (с изменениями и дополнениями)

5. Перечень сведений, относящихся к персональным данным работников ГБУК «Самарская областная библиотека для слепых», представлен в приложении № 1 к Положению.

II. ПРАВА И ОБЯЗАННОСТИ РАБОТОДАТЕЛЯ (ОПЕРАТОРА) В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

1. ГБУК «Самарская областная библиотека для слепых» в соответствии с положениями пункта 2 статьи 3 Федерального закона Российской Федерации является оператором при работе с персональными данными.

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

− До начала обработки персональных данных оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

− Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законодательства Российской Федерации и иных нормативных правовых актов, содействия в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

− При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными нормативными правовыми актами Российской Федерации;

− Оператор не имеет права получать и обрабатывать сведения, относящиеся в соответствии с законодательством Российской Федерации в области персональных данных к специальным категориям персональных данных, за исключением случаев, предусмотренных Трудовым Кодексом и иными нормативными правовыми актами Российской Федерации;

− Оператор не имеет права получать и обрабатывать персональные данные о членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым Кодексом и иными нормативными правовыми актами Российской Федерации;

− Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, когда имеется согласие в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами Российской Федерации, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных

Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

Оператор обязан рассмотреть возражение, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

− Защита персональных данных от неправомерного их использования или утраты обеспечивается Оператором за счет его средств в порядке, установленном Трудовым Кодексом и иными нормативными правовыми актами Российской Федерации;

− Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом Российской Федерации.

− Все персональные данные следует получать у субъектов. Если персональные данные возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение;

− Оператор обязан ознакомить субъектов и их представителей с документами, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области, под личную подпись;

− Оператор совместно с субъектами и их представителями должны совместно вырабатывать меры защиты персональных данных.

− При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных и предусмотренную Федеральным законом и разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

3. Если персональные данные получены не от субъекта персональных данных, оператор до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

− наименование либо фамилия, имя, отчество и адрес оператора или его представителя,

− цель обработки персональных данных и ее правовое основание;

− предполагаемые пользователи персональных данных,

− установленные Федеральным законом Российской Федерации права субъекта персональных данных;

− источник получения персональных данных.

4. Оператор освобождается от обязанности предоставить субъекту персональных данных указанные выше сведения в случаях, если:

− Субъект персональных данных уведомлен об осуществлении обработки его персональных данных оператором;

− Персональные данные получены оператором на основании Федерального закона Российской Федерации или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

− Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных Федеральным законом;

− Оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

− Предоставление субъекту персональных данных сведений, нарушает права и законные интересы третьих лиц.

5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан

Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

6. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

- Обрабатываемых в соответствии с трудовым законодательством;
- Полученных в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- Относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;
- Разрешенных субъектом персональных данных для распространения при условии соблюдения оператором запретов и условий, предусмотренных Федеральным законом;
- Включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- Необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;
- Включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- Обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;
- Обрабатываемых в случаях, предусмотренных законодательством

Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных

1. Оператор обязан сообщить в порядке, предусмотренном Федеральным законом, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

3. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения.

В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных

изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

4. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами.

2. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом Российской Федерации и принятыми в соответствии с ним нормативными правовыми актами.

В ГБУК «Самарская областная библиотека для слепых» принимаются следующие меры:

− Назначение должностного лица, ответственного за организацию обработки персональных данных;

− Издание документов, определяющих политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

− Применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

− Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону Российской Федерации и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

− Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона Российской Федерации, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом Российской Федерации;

− Ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите

персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

3. Оператор обязан обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

4. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

5. Оператор обязан представить указанные документы и локальные акты и (или) иным образом подтвердить принятие мер, достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом Российской Федерации, по запросу уполномоченного органа по защите прав субъектов персональных данных.

Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных

1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки.

В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим

лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

2. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять

обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом или другими федеральными законами.

5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

6. В случае отсутствия возможности уничтожения персональных данных в течение установленного срока, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

III. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКОВ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ХРАНЯЩИХСЯ У РАБОТОДАТЕЛЯ

1. Работники и клиенты ГБУК «Самарская областная библиотека для слепых» в соответствии с положениями пункта 2 статьи 3 Федерального закона Российской Федерации являются субъектами при работе с персональными данными.

2. Субъекты персональных данных обязаны представлять Оператору или его представителю достоверные персональные данные, а также в течение 30 дней, уведомлять об их изменении.

Представление субъектом недостоверных данных может служить основанием для расторжения трудового договора.

3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- Подтверждение факта обработки персональных данных оператором;
- Правовые основания и цели обработки персональных данных;
- Цели и применяемые оператором способы обработки персональных данных;
- Наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- Сроки обработки персональных данных, в том числе сроки их хранения;
- Порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
- Информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- Иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

4. Работники и их представители должны быть ознакомлены под личную подпись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

5. Субъект персональных данных имеет право на получение указанных сведений и вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Указанные сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта

персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5. В случае, если сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений и ознакомления с такими персональными данными не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, а также в целях ознакомления с обрабатываемыми персональными данными до истечения 30 дневного срока, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду должен содержать обоснование направления повторного запроса.

Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

6. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами Российской Федерации, в том числе если:

− Обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

− Обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в

совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

− Обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

− Доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

− Обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

7. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники и клиенты имеют право на:

− Полную информацию об их персональных данных и обработке этих данных;

− Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных законодательством;

− Определение своих представителей для защиты своих персональных данных;

− Доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору;

− Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового Кодекса и иных нормативных правовых актов Российской Федерации. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

− Требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо

всех произведенных в них исключениях, исправлениях или дополнениях;

− Обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных (если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона или иным образом нарушает его права и свободы.

8. 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.

IV. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Обработка персональных данных в ГБУК «Самарская областная библиотека для слепых» осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом Российской Федерации.

Обработке подлежат только персональные данные, которые отвечают целям их обработки, при этом обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

При обработке персональных данных не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

2. Обработка персональных данных допускается в следующих случаях:

− Обработка персональных данных осуществляется с письменного согласия субъекта персональных данных (работника) на обработку его персональных данных;

− Обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации на оператора (ГБУК «Самарская областная библиотека для слепых») функций, полномочий и обязанностей;

− Обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах или необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской

Федерации об исполнительном производстве;

− Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

− Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

− Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

− Обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

− Обработка персональных данных, подлежащих опубликованию или обязательному раскрытию, осуществляется в соответствии с Федеральным законом.

3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом Российской Федерации, на основании заключаемого с этим лицом договора, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом Российской Федерации. В поручении оператора определяются перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, устанавливается обязанность такого лица соблюдать конфиденциальность

персональных данных и обеспечивать безопасность персональных данных при их обработке, а также указываются требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона Российской Федерации.

Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает письменное согласие на их обработку. Электронный документ, подписанный электронной подписью, признается равнозначным согласию в письменной форме на бумажном носителе, содержащему личную собственноручную подпись субъекта персональных данных.

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено Федеральным законом Российской Федерации. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона Российской Федерации.

6. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

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

− Фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты

доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

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

− Цель обработки персональных данных;

− Перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

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

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

− Срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено Федеральным законом Российской Федерации.

− Подпись субъекта персональных данных.

7. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона Российской Федерации.

Особенности обработки специальных категорий персональных данных

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев:

− Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных (в действующей редакции);

− Обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

2. Обработка специальных категорий персональных данных допускается если:

− Субъект персональных данных дал согласие в письменной форме на

обработку своих персональных данных;

− Обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 г. № 8-ФЗ «О Всероссийской переписи населения»;

− Обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством и пенсионным законодательством Российской Федерации;

− Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

− Обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью;

− Обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

− Обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, в связи с осуществлением правосудия;

− Обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

− Обработка персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;

− Обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

− Обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации,

государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;

− Обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

3. Обработка персональных данных, касающихся состояния здоровья, полученных в результате обезличивания персональных данных, допускается в целях повышения эффективности государственного или муниципального управления.

4. Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами Российской Федерации.

5. Обработка специальных категорий персональных данных, должна быть незамедлительно прекращена, если устранены причины, вследствие которых она осуществлялась, если иное не установлено федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных (в действующей редакции).

Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения

1. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

2. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных согласился с распространением персональных данных, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без права распространения.

3. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом

персональных данных для распространения, не следует, что субъект персональных данных не установил запреты и условия на обработку персональных данных, а именно запреты на передачу (кроме предоставления доступа) персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) персональных данных неограниченным кругом лиц, или если в предоставленном субъектом персональных данных таком согласии не указаны категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с персональными данными неограниченному кругу лиц.

4. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору:

- Непосредственно;
- С использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

5. Правила использования информационной системы уполномоченного органа по защите прав субъектов персональных данных, в том числе порядок взаимодействия субъекта персональных данных с оператором, определяются уполномоченным органом по защите прав субъектов персональных данных.

6. Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

7. Оператор обязан в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения.

Особенности обработки биометрических персональных данных

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта

персональных данных.

2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации, законодательством Российской Федерации о нотариате.

Хранение и использование персональных данных

1. 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 Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

2. 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 Российской Федерации.

3. Использование и хранение биометрических персональных данных вне информационных систем персональных данных осуществляется только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

4. Хранение материальных носителей персональных данных осуществляется в специально выделенных помещениях в металлических шкафах (сейфах).

V. ПЕРЕДАЧА И РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

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 других случаях, предусмотренных Трудовым Кодексом и иными нормативными правовыми актами Российской Федерации

− 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 Трудовым Кодексом и иными нормативными правовыми актами Российской Федерации;

− Осуществлять передачу персональных данных работника в пределах одной организации в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под личную подпись;

− 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 работников в порядке, установленном Трудовым Кодексом и иными нормативными правовыми актами Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

VI. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

1. Работники ГБУК «Самарская областная библиотека для слепых», допущенные в установленном порядке к работе с персональными данными, обязаны выполнять требования, указанные в настоящем Положении.

2. Доступ к персональным данным работников ГБУК «Самарская

областная библиотека для слепых» имеют:

В полном объеме:

- директор;
- работники отдела кадров;
- главный бухгалтер и работники бухгалтерии;
- работник (исключительно к персональным данным в отношении себя).

3. В объеме, необходимом для выполнения должностных обязанностей:

- заместители директора (в отношении подчиненных должностных лиц);
- начальник и работники юридического отдела, к персональным данным, которые необходимы для оформления доверенностей, аналитических справок, ответов на запросы государственных органов, ответов на запросы, заявок на участие в процедурах закупок, договоров, подготовки исковых заявлений к работникам ГБУК «Самарская областная библиотека для слепых», а также отзывов на исковые заявления по трудовым спорам, другие подобные процессуальные документы;
- главный бухгалтер;
- руководители структурных подразделений (в отношении подчиненных должностных лиц), с письменного разрешения директора;
- заведующий и работники отдела абонентского обслуживания - для создания и настройки учетных записей пользователей для доступа в локальную вычислительную сеть, государственные информационные системы, информационно-телекоммуникационную сеть общего пользования, систему электронной почты;

4. Для допуска к персональным данным работников для выполнения должностных обязанностей, должностные лица направляют директору мотивированное ходатайство, в котором излагают:

- цель допуска к обработке персональных данных;
- перечень персональных данных, допуск к обработке которых необходим;
- обоснование необходимости и целесообразности допуска к обработке персональных данных других работников.

5. Персональные данные работников ГБУК «Самарская областная библиотека для слепых» по письменным запросам могут представляться в следующие государственные и негосударственные функциональные структуры:

- судебные, правоохранительные органы;
- налоговые органы;
- органы статистики;

− страховые агентства;
− военные комиссариаты;
− органы социального страхования;
− пенсионные фонды;
− подразделения муниципальных органов управления;
− аудиторские организации, проводящие аудиторские проверки на предприятии, в объеме, необходимом для проведения проверки.

6. Допуск к обработке персональных данных работников прекращается:
− при увольнении работника;
− при переводе работника на должность, выполнение должностных обязанностей по которой не требует работы с персональными данными.

Допуск к обработке персональных данных лицам также может быть прекращен по письменному решению директора.

7. До всех сотрудников, непосредственно осуществляющих обработку персональных данных, письменно, под личную подпись, доводятся положения законодательства Российской Федерации о персональных данных, в том числе требования по защите персональных данных.

VII. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры и обеспечивает их принятие 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.

2. Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

3. Обеспечение безопасности персональных данных достигается:
− 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;

− Применением сертифицированных средств защиты информации;

− Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

− Учетом машинных носителей персональных данных;

− Обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

− Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

− Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

− Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

4. Для обеспечения защиты персональных данных субъектов персональных данных при их обработке приказом директора назначаются должностные лица, ответственные за организацию обработки персональных данных, определяется перечень должностных лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей, назначаются должностные лица, ответственные за обеспечение безопасности персональных данных;

VII. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации (в действующей редакции), введённого в действие Федеральным законом Российской Федерации от 30 декабря 2001 г. № 197-ФЗ и иными нормативными правовыми актами Российской Федерации, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Уголовный кодекс Российской Федерации (в действующей редакции), введенный в действие Федеральным законом Российской Федерации от 13 июня 1996 г. № 63-ФЗ.

Статья 173.2. Незаконное использование документов для образования (создания, реорганизации) юридического лица.

2. Приобретение документа, удостоверяющего личность, или использование персональных данных, полученных незаконным путем, если эти деяния совершены для внесения в единый государственный реестр юридических лиц сведений о подставном лице, -

наказываются штрафом в размере от трехсот до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до трех лет, либо лишением свободы на тот же срок.

Статья 137. Нарушение неприкосновенности частной жизни

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, -

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

2. Те же деяния, совершенные лицом с использованием своего служебного положения, -

наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового, либо арестом на срок до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

Кодекс Российской Федерации об административных правонарушениях (в действующей редакции), введенный в действие Федеральным законом Российской Федерации от 30 декабря 2001 г. № 195-ФЗ.

Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных.

1. Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи, если эти действия не содержат уголовно наказуемого деяния, -

влечет наложение административного штрафа на граждан в размере от двух тысяч до шести тысяч рублей; на должностных лиц - от десяти тысяч до двадцати тысяч рублей; на юридических лиц - от шестидесяти тысяч до ста тысяч рублей.

1.1. Повторное совершение административного правонарушения, предусмотренного частью 1 настоящей статьи, -

влечет наложение административного штрафа на граждан в размере от четырех тысяч до двенадцати тысяч рублей; на должностных лиц - от двадцати тысяч до пятидесяти тысяч рублей; на индивидуальных предпринимателей - от пятидесяти тысяч до ста тысяч рублей; на юридических лиц - от ста тысяч до трехсот тысяч рублей.

2. Обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством Российской Федерации в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных, -

влечет наложение административного штрафа на граждан в размере от шести тысяч до десяти тысяч рублей; на должностных лиц - от двадцати тысяч до сорока тысяч рублей; на юридических лиц - от тридцати тысяч до ста пятидесяти тысяч рублей.

2.1. Повторное совершение административного правонарушения, предусмотренного частью 2 настоящей статьи, -

влечет наложение административного штрафа на граждан в размере от

десяти тысяч до двадцати тысяч рублей; на должностных лиц - от сорока тысяч до ста тысяч рублей; на индивидуальных предпринимателей - от ста тысяч до трехсот тысяч рублей; на юридических лиц - от трехсот тысяч до пятисот тысяч рублей.

3. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных -

влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до трех тысяч рублей; на должностных лиц - от шести тысяч до двенадцати тысяч рублей; на индивидуальных предпринимателей - от десяти тысяч до двадцати тысяч рублей; на юридических лиц - от тридцати тысяч до шестидесяти тысяч рублей.

4. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных, -

влечет наложение административного штрафа на граждан в размере от двух тысяч до четырех тысяч рублей; на должностных лиц - от восьми тысяч до двенадцати тысяч рублей; на индивидуальных предпринимателей - от двадцати тысяч до тридцати тысяч рублей; на юридических лиц - от сорока тысяч до восьмидесяти тысяч рублей.

5. Невыполнение оператором в сроки, установленные законодательством Российской Федерации в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, -

влечет наложение административного штрафа на граждан в размере от двух тысяч до четырех тысяч рублей; на должностных лиц - от восьми тысяч до двадцати тысяч рублей; на индивидуальных предпринимателей - от двадцати тысяч до сорока тысяч рублей; на юридических лиц - от пятидесяти тысяч до девяноста тысяч рублей.

5.1. Повторное совершение административного правонарушения, предусмотренного частью 5 настоящей статьи, -

влечет наложение административного штрафа на граждан в размере от двадцати тысяч до тридцати тысяч рублей; на должностных лиц - от тридцати тысяч до пятидесяти тысяч рублей; на индивидуальных предпринимателей - от пятидесяти тысяч до ста тысяч рублей; на юридических лиц - от трехсот тысяч до пятисот тысяч рублей.

6. Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством Российской Федерации в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния -

влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до четырех тысяч рублей; на должностных лиц - от восьми тысяч до двадцати тысяч рублей; на индивидуальных предпринимателей - от двадцати тысяч до сорока тысяч рублей; на юридических лиц - от пятидесяти тысяч до ста тысяч рублей.

7. Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных -

влечет наложение административного штрафа на должностных лиц в размере от шести тысяч до двенадцати тысяч рублей.

8. Невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, -

влечет наложение административного штрафа на граждан в размере от тридцати тысяч до пятидесяти тысяч рублей; на должностных лиц - от ста тысяч до двухсот тысяч рублей; на юридических лиц - от одного миллиона до

шести миллионов рублей.

9. Повторное совершение административного правонарушения, предусмотренного частью 8 настоящей статьи, -

влечет наложение административного штрафа на граждан в размере от пятидесяти тысяч до ста тысяч рублей; на должностных лиц - от пятисот тысяч до восьмисот тысяч рублей; на юридических лиц - от шести миллионов до восемнадцати миллионов рублей.

Положение разработано ООО « Джи-Эс-Ти» в соответствии с контрактом от 11.07.2022 г.№ 11/07

Приложение № 1

Перечень сведений, относящихся к персональным данным работников ГБУК «Самарская областная библиотека для слепых»

- паспортные данные;
- анкетные данные, заполненные работником при поступлении на работу или в процессе работы (в том числе - автобиография);
- сведения об образовании, повышении квалификации, переквалификации и т.п. (на основании документов, подтверждающих образование, квалификацию);
- сведения об обязательном пенсионном страховании (на основании страхового свидетельства государственного пенсионного страхования);
- сведения о присвоении идентификационного номера налогоплательщика (на основании свидетельства о присвоении идентификационного номера налогоплательщика);
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о семейном положении работника, перемене им фамилии, наличии детей, иждивенцев;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- сведения о заработной плате работника;
- сведения о социальных льготах;
- занимаемая должность;
- наличие судимостей;
- адрес регистрации и места жительства;
- контактный телефон;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- трудовые книжки сотрудников;
- основания к приказам по личному составу;
- медицинские заключения, предъявляемые работником по прохождению обязательных предварительных и периодических медицинских осмотров;
- копии отчетов, направляемых в государственные органы статистики, налоговые органы, вышестоящие органы управления и другие учреждения;

- фотографии и иные сведения, относящиеся к персональным данным работника;

- финансовое положение (доходы, владение недвижимым имуществом, денежные вклады и др.);

- деловые и иные личные качества, которые носят оценочный характер;

- биометрические данные (внешность, голос);

- специальные данные (раса, национальность, политические взгляды, вероисповедание);

- состояние здоровья;

- прочие сведения, которые могут идентифицировать человека.

Приложение № 2

Директору ГБУК «Самарская областная библиотека для слепых»
От _____
_____
зарегистрированного по адресу: _____
_____
_____
Паспорт _____ № _____
_____
_____

СОГЛАСИЕ
работника на обработку его персональных данных

Я, _____
_____
_____
_____
_____
(Ф.И.О., паспортные данные, в т.ч. дата выдачи, выдавший орган)

руководствуясь ст. 10.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в целях:

обеспечения соблюдения законов и иных нормативных правовых актов; трудовых отношений и иных непосредственно связанных с ними отношений, в том числе размещения информации обо мне на официальном сайте, в средствах информации (открытых источниках), использования моих контактных данных даю согласие на распространение подлежащих обработке персональных данных ГБУК «Самарская областная библиотека для слепых» в следующем порядке:

- фамилия, имя, отчество;
- пол, возраст;

- дата и место рождения;

- паспортные данные;

- адрес регистрации по месту жительства и адрес фактического проживания;

- номер телефона (домашний, мобильный);

- данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;

- семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым и налоговым законодательством;

- отношение к воинской обязанности;

- сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;

- номер СНИЛС, ИНН;

- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в ГБУК «Самарская областная библиотека для слепых»;

- сведения о доходах в ГБУК «Самарская областная библиотека для слепых»

- биометрические данные (внешность, голос);

- специальные данные (раса, национальность, политические взгляды, вероисповедание);

- состояние здоровья;

- сведения о деловых и иных личных качествах, носящих оценочный характер.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

« ___ » _____ 20___ г. _____

(подпись)

Приложение № 3

Директору ГБУК «Самарская областная библиотека для слепых»
От _____
_____
зарегистрированного по адресу: _____
_____
_____
Паспорт _____ № _____
_____
_____

СОГЛАСИЕ
работника на передачу его персональных данных,
третьим лицам

Я,
_____,
(фамилия, имя, отчество полностью)
в соответствии со статьей 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- начисления заработной платы, предоставления налоговых вычетов;
- исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений

персонифицированного учета в Пенсионный фонд РФ, сведений о налогах на доходы физлиц в ФНС России, сведений в ФСС РФ;

- предоставления сведений в кредитные организации для оформления банковской карты и перечисления на нее заработной платы и других выплат;

- предоставления сведений третьим лицам для выполнения конкретных функций, связанных с выполнением моих должностных обязанностей;

- предоставления данных для формирования справочных материалов для внутреннего информационного обеспечения деятельности организации;

- обеспечения пропускного и внутриобъектового режимов в организации;

- обеспечения моей безопасности;

- обеспечения сохранности имущества работодателя

даю согласие ГБУК «Самарская областная библиотека для слепых», расположенному по адресу: г. Самара, ул. Никитинская, д. 21, на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно обработку, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение следующих персональных данных в документальной и/или электронной форме:

- фамилия, имя, отчество;

- пол, возраст;

- дата и место рождения;

- паспортные данные;

- адрес регистрации по месту жительства и адрес фактического проживания;

- номер телефона (домашний, мобильный);

- данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;

- семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым и налоговым законодательством;

- отношение к воинской обязанности;

- сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;

- номер СНИЛС, ИНН;

- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в ГБУК «Самарская областная библиотека для слепых»;

- сведения о доходах в ГБУК «Самарская областная библиотека для

слепых»

- биометрические данные (внешность, голос);

- специальные данные (раса, национальность, политические взгляды, вероисповедание);

- состояние здоровья;

- сведения о деловых и иных личных качествах, носящих оценочный характер.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

« ___ » _____ 20___ г. _____

(подпись)

Приложение № 4

_____
_____

УВЕДОМЛЕНИЕ
о получении персональных данных у третьих лиц

Уважаемый,
_____!

В связи с _____
у ГБУК «Самарская областная библиотека для слепых» возникла необходимость получения следующей информации, составляющей Ваши персональные данные:
_____
_____
_____.

Просим Вас предоставить указанные сведения в течение семи рабочих дней с момента получения настоящего уведомления.

В случае невозможности предоставить указанные сведения просим Вас в указанный срок дать письменное согласие на получение ГБУК «Самарская областная библиотека для слепых» необходимой информации из следующих источников: _____
_____
следующими способами: _____
_____.

По результатам обработки указанной информации планируется принятие следующих решений, которые будут доведены до Вашего сведения: _____
_____
_____.

Вы имеете право заявить свои письменные возражения против принятых решений в _____ срок.

В случае Вашего отказа могут возникнуть следующие последствия:

_____
_____
_____.

Информируем Вас о Вашем праве в любое время отозвать свое письменное согласие на обработку персональных данных.

Уведомление получил(а)

« ___ » _____ 2022 г. _____

Приложение № 5

ИНСТРУКЦИЯ
по антивирусной защите в информационных системах

1 Общие положения

1.1 Настоящая Инструкция предназначена для всех сотрудников ГБУК «Самарская областная библиотека для слепых», имеющих доступ к информационным системам (ИС) ГБУК «Самарская областная библиотека для слепых».

1.2 Инструкция устанавливает требования и ответственность при организации защиты информации от воздействия вредоносных компьютерных вирусов.

1.3 Инструкция регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля при работе в ИС ГБУК «Самарская областная библиотека для слепых».

2 Обеспечение антивирусной защиты

2.1 Порядок организации антивирусной защиты.

2.1.1 Для организации антивирусной защиты ИС ГБУК «Самарская областная библиотека для слепых» допускаются к использованию только сертифицированные ФСТЭК России лицензионные антивирусные средства общего применения.

2.1.2 Антивирусное средство защиты должно быть установлено на все средства вычислительной техники (СВТ), входящие в ИС ГБУК «Самарская областная библиотека для слепых».

2.1.3 В ИС ГБУК «Самарская областная библиотека для слепых» права по управлению (администрированию) средствами антивирусной защиты предоставлены только администратору информационной безопасности.

2.1.4 Разработка и осуществление мероприятий по проведению антивирусного контроля осуществляется ответственным за защиту информации с привлечением администратора информационной безопасности и/или специалистов лицензированной организации.

2.1.5 Должностные лица не должны допускать использования в ИС ГБУК «Самарская областная библиотека для слепых» программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

2.1.6 В ИС ГБУК «Самарская областная библиотека для слепых» обеспечивается централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты,

установленными на компонентах информационной системы (автоматизированных рабочих местах).

2.1.7 В ИС ГБУК «Самарская областная библиотека для слепых» обеспечивается централизованное управление обновлением базы данных вредоносных компьютерных программ (вирусов).

2.1.8 Расширенный антивирусный контроль проводится администратором информационной безопасности не реже одного раза в месяц и при необходимости, в случае подозрений в заражении вирусной программой.

2.1.9 При загрузке, открытии или исполнении объектов (файлов) из внешних источников средствами антивирусной защиты проводится автоматическая проверка объектов (файлов).

2.1.10 В виртуальной инфраструктуре обеспечивается реализация и управление антивирусной защитой:

2.1.10.1 проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;

2.1.10.2 проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

2.2 Порядок проведения антивирусного контроля.

2.2.1 Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется администратором информационной безопасности на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена антивирусная проверка администратором информационной безопасности.

2.2.2 При загрузке компьютера средствами антивирусной защиты проводится антивирусный контроль в автоматическом режиме.

2.2.3 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 ИС ГБУК «Самарская областная библиотека для слепых» самостоятельно или вместе с администратором информационной безопасности проводит внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса.

2.2.4 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИС ГБУК «Самарская областная библиотека для слепых» обязаны:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и администратора информационной безопасности, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на съемном носителе информации администратору информационной безопасности для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при наличии);
- по факту обнаружения зараженных вирусом файлов составить служебную записку администратору информационной безопасности, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

2.3 Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

2.3.1 Администратор информационной безопасности обеспечивает получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

2.3.2 Контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов) обеспечивается путем автоматического получения или предварительно скачиваемых обновлений из официальных источников, например, с сервера обновлений производителя антивирусного средства.

3 Ответственность при организации антивирусной защиты

3.1 Ответственность за организацию антивирусной защиты ИС ГБУК «Самарская областная библиотека для слепых» в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.

3.2 Ответственность за соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности, администратора ИС ГБУК «Самарская областная библиотека для слепых», администратора виртуальной инфраструктуры и пользователей, эксплуатирующих ИС ГБУК «Самарская областная библиотека для слепых».

Приложение № 6

ИНСТРУКЦИЯ
по организации парольной защиты в информационной системе

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в ИС ГБУК «Самарская областная библиотека для слепых», а также контроль над действиями пользователя при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на администратора безопасности ИС.

2. Личный пароль должен выбираться и генерироваться пользователем ИС самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее восьми символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (ЭВМ, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владелец пароля должен быть ознакомлен под роспись с перечисленными выше требованиями и предупрежден об ответственности за использование пароля, не соответствующего данным требованиям, а также за разглашение парольной информации.

3. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 3 месяца.

4. Внеплановая смена личного пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться Администратором информационной безопасности ИС немедленно после окончания последнего сеанса работы данного пользователя с системой на основании письменного указания начальника отдела.

5. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) Администратора информационной безопасности ИС.

6. В случае компрометации личного пароля пользователя ИС должны быть немедленно предприняты меры в соответствии с п.5 или п.6 настоящей

Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в сейфе начальника подразделения.

8. Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администратора информационной безопасности ИС.

Приложение № 7

ИНСТРУКЦИЯ
по резервному копированию в информационных системах

1. Общие положения

1.1. Целью настоящей Инструкции по резервному копированию в информационных системах (далее - ИС) ГБУК «Самарская областная библиотека для слепых» (далее – Инструкция) является превентивная защита элементов ИС ГБУК «Самарская областная библиотека для слепых» от потери защищаемых информационных ресурсов.

1.2. Настоящая Инструкция регламентирует порядок использования систем резервного копирования, архивирования и восстановления информации.

1.3. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в год.

1.4. Защита резервируемой информации в ИС ГБУК «Самарская областная библиотека для слепых» обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в проектной и организационно-распорядительной документации по защите информации в ГБУК «Самарская областная библиотека для слепых».

1.5. В ИС ГБУК «Самарская областная библиотека для слепых» обеспечивается регистрация событий, связанных с резервным копированием информации на резервные машинные носители информации и восстановлением информации с резервных машинных носителей информации.

1.6. Администратор резервного копирования осуществляет не реже одного раза в три месяца проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий.

1.7. Резервное копирование и хранение данных должно осуществлять на периодической основе:

− для обрабатываемой информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну – не реже раза в неделю;

− для технологической информации – не реже раза в месяц;

− эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС ГБУК «Самарская областная библиотека для слепых» – не реже раза в месяц, и

каждый раз при внесении изменений в эталонные копии (выход новых версий);

- для записей регистрации (аудита) – не реже одного раза в неделю.

2. Методы резервного копирования

При выполнении операции Incremental Backup производится резервное копирование файлов, изменившихся со времени последнего выполнения операции Incremental Backup или Full Backup.

При выполнении операции Full Backup производится полное резервное копирование информационного ресурса.

3. Порядок хранения носителей резервных копий

3.1. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

3.2. Хранение (размещение) резервных копий информации должно осуществляться на отдельных (размещенных вне информационной системы) средствах хранения резервных копий и в помещениях, специально предназначенных для хранения резервных копий информации, которые исключают воздействие внешних факторов на хранимую информацию.

3.3. Носители должны храниться не менее года для возможности восстановления данных.

4. Порядок восстановления информации

4.1 Восстановление информации из резервных копий производится администратором резервного копирования на основании согласованной заявки.

4.2 Место расположения восстанавливаемой информации определяется администратором резервного копирования и согласовывается с сотрудником ГБУК «Самарская областная библиотека для слепых», подавшим заявку, в рабочем порядке.

4.3 Восстановление информации с резервных машинных носителей информации (резервных копий) предусматривает определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования ИС ГБУК «Самарская областная библиотека для слепых» и доступности информации:

- для обрабатываемых персональных данных – не более 6 часов;
- для технологической информации – не более 24 часов;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС ГБУК «Самарская областная библиотека для слепых» – не более 24 часов;
- для записей регистрации (аудита) – не более 48 часов.

Приложение № 8

ПРАВИЛА
обращения с машинными носителями информации в информационных системах

1. Общие положения

1.1.Настоящие правила рассматривают вопросы защиты машинных носителей информации в информационных системах ГБУК «Самарская областная библиотека для слепых» (далее – ИС) от несанкционированного доступа к ним, уничтожения, а также неразрешенного раскрытия, модификации, удаления информации на них.

1.2.В качестве машинных носителей информации в настоящей инструкции рассматриваются:

− машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках),

− съемные машинные носители информации (перечислить тип),

− портативные вычислительные устройства, имеющие встроенные носители информации.

1.3.Под использованием машинных носителей информации в ИС ГБУК «Самарская областная библиотека для слепых» понимается их подключение к инфраструктуре ИС ГБУК «Самарская областная библиотека для слепых» с целью обработки, приема/передачи информации между информационной системой и носителями информации.

1.4.Данные правила обязательны для применения во всех подразделениях ГБУК «Самарская областная библиотека для слепых», в которых обрабатывается информация ограниченного доступа (в том числе персональные данные), не содержащая сведения, составляющие государственную тайну.

2. Использование машинных носителей информации

2.1.В ИС ГБУК «Самарская областная библиотека для слепых» допускается использование только учтенных машинных носителей информации, которые являются собственностью ГБУК «Самарская областная библиотека для слепых» и подвергаются регулярной ревизии и контролю.

2.2.Машинные носители информации предоставляются сотрудникам ГБУК «Самарская областная библиотека для слепых» по инициативе начальника структурного подразделения в случаях:

− необходимости выполнения вновь принятым сотрудником своих должностных обязанностей;

− возникновения у сотрудника Краткое наименование организации производственной необходимости.

2.3.При использовании сотрудниками машинных носителей информации необходимо:

2.3.1. Использовать машинные носители информации исключительно для выполнения своих служебных обязанностей.

2.3.2. Ставить в известность Ответственного за защиту информации в ГБУК «Самарская областная библиотека для слепых» о любых фактах нарушения требований настоящих правил.

2.3.3. Бережно относиться к машинным носителям информации.

2.3.4. Обеспечивать физическую безопасность машинных носителей информации.

2.3.5. Извещать Ответственного за защиту информации о фактах утраты (кражи) машинных носителей информации.

2.3.6. Перед началом работы с машинными носителями информации пользователь обязан проверять их на наличие вредоносных программ (вирусов) с помощью штатных антивирусных программ. В случае обнаружения вирусов, пользователь обязан действовать в соответствии с «Инструкцией по антивирусной защите».

2.4.При использовании машинных носителей информации запрещено:

2.4.1. Использовать машинные носители информации в личных целях.

2.4.2. Передавать носители информации другим лицам (за исключением администратора информационной безопасности).

2.4.3. Оставлять машинные носители информации без присмотра или передавать на хранение другим лицам;

2.4.4. Выносить машинные носители информации из служебных помещений для работы с ними на дому и т. д.

2.5.Ответственность за подключение машинных носителей информации, не учтенных соответствующим образом, не прошедших проверку, несет пользователь, подключивший данное устройство.

3. Хранение и учёт машинных носителей информации

3.1.Все находящиеся на хранении и в обращении машинные носители информации в ГБУК «Самарская областная библиотека для слепых» подлежат обязательному учёту. На каждый машинный носитель должна наноситься маркировка, позволяющая его идентифицировать.

3.2.Регистрацию машинных носителей информации осуществляет Ответственный за защиту информации в Журнале регистрации, учета и выдачи машинных носителей информации (далее – Журнал регистрации) путем занесения регистрационного или иного номера с указанием пользователя или

группы пользователей, которым разрешен доступ к машинным носителям информации.

3.3.Учет выдачи машинных носителей информации ведется Ответственным за обработку и защиту информации в Журнале регистрации, в котором указывается маркировка носителя, дата, время, фамилия, имя и отчество должностного лица, получившего средство, его роспись.

3.4.Сотрудники ГБУК «Самарская областная библиотека для слепых» получают учтенный машинный носитель от Ответственного за обработку и защиту информации для выполнения работ на конкретный срок. При получении делаются соответствующие записи в Журнале регистрации. По окончании работ пользователь сдает машинный носитель для хранения Ответственному за защиту информации, о чем делается соответствующая запись в журнале регистрации.

3.5.При поступлении нового машинного носителя информации, который будет использоваться в ИС ГБУК «Самарская областная библиотека для слепых», Ответственный за защиту информации регистрирует его в Журнале регистрации. Перед использованием новый машинный носитель информации в обязательном порядке должен пройти антивирусную проверку (при наличии технической возможности).

3.6.При передаче средств вычислительной техники (далее – СВТ) ИС ГБУК «Самарская областная библиотека для слепых» сторонним организациям для проведения ремонтно-восстановительных или иных работ, не съемные машинные носители (накопители на жестких дисках) изымаются из состава СВТ.

3.7.В случае возврата машинного носителя информации в Журнале регистрации Ответственным за защиту информации проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

3.8.В случае увольнения или перевода сотрудника в другое структурное подразделение предоставленные машинные носители информации изымаются.

3.9.Хранить машинные носители информации нужно вдали от источников электромагнитного излучения и тепла.

4. Ликвидация машинных носителей информации и уничтожение (стирание) информации на машинных носителях

4.1.В случае утраты или уничтожения машинных носителей информации немедленно ставятся в известность начальник соответствующего структурного подразделения и Ответственный и защиту информации. На утраченные носители составляется акт (приложение 1). Соответствующие отметки вносятся в Журнал регистрации.

4.2.Машинные носители информации, пришедшие в негодность или отслужившие установленный срок, должны быть уничтожены без возможности восстановления с составлением Акта уничтожения машинных носителей информации (по прилагаемой форме) и последующей регистрацией в Журнале регистрации. Уничтожение машинных носителей осуществляется комиссией.

4.3.В Краткое наименование организации обеспечивается уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации:

4.3.1. Уничтожение (стирание) информации на машинных носителях исключает возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

4.3.2. В ИС ГБУК «Самарская областная библиотека для слепых» используются следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:

перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием.

4.4.Ответственный за обработку и защиту информации обеспечивает регистрацию и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации путем составления соответствующих актов, и занесением в Журнал регистрации.

5. Ответственность

5.1.Ответственность за выполнение правил эксплуатации машинных носителей информации при выполнении непосредственных работ со средствами несут пользователи ИС ГБУК «Самарская областная библиотека для слепых».

5.2.Контроль выполнения установленных правил эксплуатации и регистрацию и учет машинных носителей информации осуществляет ответственный за защиту информации.

Приложение № 9

ИНСТРУКЦИЯ
пользователя информационных систем

1 Общие положения

1.1 Инструкция пользователя информационных систем ГБУК «Самарская областная библиотека для слепых» (далее – ИС) (далее – Инструкция) определяет функциональные обязанности, права и ответственность пользователей ИС ГБУК «Самарская областная библиотека для слепых», в которых обрабатывается информация согласно утвержденному Перечню информационных систем и информации, обрабатываемой в ГБУК «Самарская областная библиотека для слепых».

1.2 Настоящая Инструкция подготовлена в соответствии с требованиями нормативно-методических документов ФСТЭК России и ФСБ России по защите информации ограниченного доступа (в том числе персональных данных), не содержащей сведений, составляющих государственную тайну (далее – Информация), обрабатываемой с использованием средств автоматизации.

1.3 В настоящей Инструкции используются следующие понятия и определения:

1.3.1 Автоматизированное рабочее место (АРМ) – объект вычислительной техники, созданный на базе автономных средств вычислительной техники с необходимым для решения конкретных задач периферийным оборудованием.

1.3.2 Компрометация пароля – утрата доверия к тому, что используемый пароль обеспечивает безопасность персональных данных. К событиям, приводящим к компрометации пароля, относятся следующие события (включая, но не ограничиваясь) – несанкционированное сообщение пароля другому лицу; утеря бумажного или машинного носителя информации, на котором был записан пароль; запись пароля на бумажном, машинном, ином носителе информации, доступ к которому не контролируется.

1.3.3 Конфиденциальность информации – обязательное для соблюдения лицом, получившим доступ к информации, требование не допускать ее распространение без наличия иного законного основания.

1.3.4 Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных

средств.

1.3.5 Несанкционированный доступ к информации – доступ к информации с нарушением установленных прав доступа, приводящий к нарушению конфиденциальности персональных данных, к утечке, искажению, подделке, уничтожению, блокированию доступа к информации.

1.3.6 Средство защиты информации (СЗИ) – программные, программно-аппаратные, аппаратные средства, предназначенные и используемые для защиты информации в информационных системах.

1.3.7 Пользователь информационной системы – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования.

1.3.8 Утеря пароля – события, приводящие к невозможности восстановления пароля в памяти лица, владеющего данным паролем.

1.3.9 Электронная вычислительная машина (ЭВМ) – персональный компьютер, предназначенный для автоматизации деятельности пользователей и входящий в состав информационной системы. В состав ЭВМ входят: системный блок, монитор, клавиатура, мышь, внешние устройства (локальный принтер, сканер и т.д.), программное обеспечение.

2 Обязанности пользователя

2.1 Пользователь ИС ГБУК «Самарская областная библиотека для слепых»обязан:

2.1.1 Знать и выполнять требования:

- настоящей инструкции;
- внутренних распорядительных документов по режиму обработки Информации, учету, хранению и пересылке носителей информации, обеспечению безопасности Информации;
- нормативных правовых актов действующего законодательства в области защиты Информации.

2.1.2 Хранить в тайне Информацию, ставшую ему известной во время работы или иным путем, и пресекать действия других лиц, которые могут привести к разглашению Информации. О таких фактах, а также о других причинах или условиях возможной утечки Информации немедленно информировать Ответственного за защиту информации, Администратора информационной безопасности (далее – ИБ).

2.1.3 При определении информации, подлежащей защите, использовать «Перечень информационных систем и информации ограниченного доступа», утвержденный ….

2.1.4 Знать и выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на

персональных компьютерах в соответствии с инструкциями, требованиями, регламентирующими функционирование установленных средств защиты.

2.1.5 Хранить в тайне свой пароль доступа в ИС ГБУК «Самарская областная библиотека для слепых», а также информацию о системе защиты, установленной в ИС ГБУК «Самарская областная библиотека для слепых».

2.1.6 Немедленно ставить в известность Администратора ИБ:

- в случае утери носителя с Информацией и/или при подозрении компрометации личных ключей и паролей;
- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа к ИС ГБУК «Самарская областная библиотека для слепых»;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИС ГБУК «Самарская областная библиотека для слепых».

2.1.7 В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в ИС ГБУК «Самарская областная библиотека для слепых» программно-аппаратных средств защиты информации ставить в известность Администратора ИС.

2.1.8 Принимать меры по реагированию, в случае возникновения нештатных и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций. Оперативно докладывать Администратору ИС и Администратору ИБ о случаях возникновения нештатных и аварийных ситуаций. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ИС. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

2.2 Для получения консультаций по вопросам информационной безопасности и по использованию СЗИ Пользователь обращается к администратору ИБ.

2.3 В случае увольнения Пользователь обязан вернуть все документы и материалы, относящиеся к ИС. В том числе: отчеты, инструкции, служебную переписку, списки сотрудника, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к ИС ГБУК «Самарская областная библиотека для слепых», полученные в течение срока работы.

2.4 Уборка помещений должна производиться под контролем Пользователя, имеющего доступ в помещение и постоянно в нем работающего.

2.5 Вынос технических средств ИС ГБУК «Самарская областная библиотека для слепых», на которых проводилась обработка Информации, за пределы контролируемой зоны с целью их ремонта, замены и т. п. без согласования с Администратором ИБ и Ответственным за защиту информации запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

2.6 АРМ, используемые для работы с Информацией, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра монитора (экрана).

2.7 Пользователю категорически запрещается:

- передавать кому бы то ни было, устно или письменно, Информацию, а также личные ключи и атрибуты доступа к ресурсам ИС ГБУК «Самарская областная библиотека для слепых», открыто осуществлять ввод персонального пароля в присутствии других лиц;
- использовать Информацию при подготовке открытых публикаций, докладов, научных работ и т.д.;
- выполнять работы с документами, содержащими Информацию, на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения Ответственного за защиту информации;
- оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие Информацию, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами, содержащими Информацию;
- использовать компоненты программного и аппаратного обеспечения ИС ГБУК «Самарская областная библиотека для слепых» в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства (в том числе отключать (блокировать) СЗИ);
- осуществлять обработку Информации в присутствии посторонних (не допущенных к данной информации) лиц;
- подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства;
- записывать и хранить Информацию на неучтенных носителях

информации;

- оставлять включенной без присмотра свое АРМ, не активизировав средства защиты информации от НСД (временную блокировку экрана);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность Администратора ИБ.
- обсуждать с посторонними лицами процедуры доступа к ИС ГБУК «Самарская областная библиотека для слепых» и обрабатываемую Информацию.

2.8 Без согласования с Администратором ИБ Пользователю запрещается:

- производить установку программных средств;
- самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение;
- изменять установленный алгоритм функционирования аттестованной ИС ГБУК «Самарская областная библиотека для слепых»;
- запускать на рабочем месте файлы, не связанные с исполнением Пользователем служебных обязанностей;
- открывать общий доступ к папкам на своей рабочей станции;
- привлекать посторонних лиц для производства ремонта или настройки АРМ ИС Краткое наименование организации.

3 Права пользователя

3.1 Пользователь имеет право:

3.1.1 Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.2 Получать доступ к информации, материалам, техническим средствам, помещениям, необходимых для надлежащего исполнения своих обязанностей.

4 Ответственность пользователя

4.1 Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также нормативных документов в области защиты информации.

4.2 Пользователь несет ответственность за нарушения в работе аттестованной ИС ГБУК «Самарская областная библиотека для слепых», вызванные его неправомерными действиями или неправильным использованием предоставленных прав, предусмотренных настоящей инструкцией.

4.3 Пользователь отвечает за правильность включения и выключения

АРМ ИС ГБУК «Самарская областная библиотека для слепых» и всех действий при работе с ним.

4.4 За разглашение Информации, а также за нарушение порядка работы с документами или машинными носителями информации, сотрудники могут быть привлечены к дисциплинарной или иной предусмотренной законодательством ответственности.

Приложение № 10

ИНСТРУКЦИЯ АДМИНИСТРАТОРА
информационной безопасности информационных систем

1. Общие положения

1.1.Инструкция Администратора информационной безопасности информационных систем ГБУК «Самарская областная библиотека для слепых» (далее – ИС) (далее – Инструкция) определяет функции, права и обязанности Администратора информационной безопасности (далее – Администратор ИБ) по вопросам обеспечения информационной безопасности при подготовке и исполнении документов в ИС ГБУК «Самарская областная библиотека для слепых».

1.2.Администратор ИБ назначается из числа сотрудников ГБУК «Самарская областная библиотека для слепых» приказом директора и обеспечивает правильность использования и нормальное функционирование установленной системы защиты ИС ГБУК «Самарская областная библиотека для слепых».

1.3.Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и не исключает обязательного выполнения их требований.

1.4.Администратор ИБ обладает правами доступа к любым программно-аппаратным средствам защиты информации (далее – СЗИ) на технических средствах пользователей. Он несет ответственность за реализацию принятой политики безопасности.

2. Должностные обязанности

2.1.Администратор ИБ обязан:

2.1.1. Осуществлять учет и периодический контроль за составом и полномочиями пользователей ИС ГБУК «Самарская областная библиотека для слепых».

2.1.2. Осуществлять оперативный контроль за работой пользователей ИС ГБУК «Самарская областная библиотека для слепых», анализировать содержимое системных журналов средств вычислительной техники (далее – СВТ) и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование системных журналов СВТ и надлежащий режим хранения данных архивов.

2.1.3. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых в ИС ГБУК

«Самарская областная библиотека для слепых» СЗИ.

2.1.4. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных СВТ, обеспечивать и контролировать установку и настройку СЗИ.

2.1.5. Не реже одного раза в месяц проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование).

2.1.6. Управлять учётными записями пользователей, реализовывать правила разграничения доступа, а также осуществлять контроль соблюдения этих правил.

2.1.7. Управлять идентификаторами (осуществлять создание, присвоение и уничтожение идентификаторов пользователей и устройств) и средствами аутентификации (аутентификационной информацией) внутренних пользователей в ИС Краткое наименование организации, обеспечивать соблюдение правил идентификации и аутентификации пользователей и устройств.

2.1.8. Осуществлять контроль за хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации.

2.1.9. Осуществлять контроль не реже одного раза в три месяца установленного (инсталлированного) в ИС ГБУК «Самарская областная библиотека для слепых» программного обеспечения.

2.1.10. Настраивать параметры журналов регистрации событий безопасности.

2.1.11. Проводить мониторинг и анализ результатов регистрации событий безопасности и реагирование на них не реже одного раза в неделю.

2.1.12. Управлять средствами антивирусной защиты.

2.1.13. Осуществлять контроль уровня защищенности информации, обрабатываемой в ИС ГБУК «Самарская областная библиотека для слепых».

2.1.14. Осуществлять контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков.

2.1.15. Обеспечивать сохранность СЗИ, эксплуатационной и технической документации к СЗИ, а также порядок обращения с СЗИ в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации, обрабатываемой с использованием средств автоматизации.

2.1.16. Проводить не реже одного раза в 6 месяцев контроль правил генерации и смены паролей пользователей, заведения и удаления учетных

записей пользователей, реализации правил разграничения доступом, полномочий пользователей.

2.1.17. Своевременно и точно отражать изменения в организационно-распорядительных документах по управлению СЗИ, установленных на СВТ ИС ГБУК «Самарская областная библиотека для слепых».

2.1.18. Осуществлять поэкземплярный учет в соответствующем журнале:

− СЗИ (носителей дистрибутивов, системных блоков с установленными СЗИ);

− эксплуатационной и технической документации к СЗИ.

2.1.19. Осуществлять хранение:

− носителей дистрибутивов СЗИ;

− лицензий и сертификатов на СЗИ.

2.1.20. Не реже одного раза в месяц осуществлять проверки:

− состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва);

− состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).

2.1.21. Проводить первоначальный, плановый и внеплановый инструктаж обслуживающего и эксплуатирующего персонала ИС ГБУК «Самарская областная библиотека для слепых» по вопросам работы с СЗИ.

2.1.22. Отвечать на вопросы обслуживающего и эксплуатирующего персонала ИС ГБУК «Самарская областная библиотека для слепых», связанные с работой СЗИ.

2.1.23. Составлять инструкции по работе с СЗИ.

2.1.24. Докладывать директору ГБУК «Самарская областная библиотека для слепых» об имевших место попытках несанкционированного доступа к информации и техническим средствам ИС.

2.1.25. Участвовать в выявлении инцидентов информационной безопасности и реагировании на них.

В ходе выявления инцидентов и реагирования на них осуществляются:

− обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий,

приводящих к возникновению инцидентов;

− анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

− планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС ГБУК «Самарская областная библиотека для слепых» в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

− планирование и принятие мер по предотвращению повторного возникновения инцидентов.

2.1.26. Управлять системой защиты информации ИС ГБУК «Самарская областная библиотека для слепых».

В ходе управления системой защиты информации ИС ГБУК «Самарская областная библиотека для слепых» осуществляются:

− поддержание системы защиты информации (структуры системы защиты информации ИС ГБУК «Самарская областная библиотека для слепых», состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты;

− управление изменениями системы защиты информации, в том числе определение типов возможных изменений системы защиты информации, санкционирование внесения изменений в системы защиты информации, документирование действий по внесению изменений в системы защиты информации, сохранение данных об изменениях системы защиты информации, контроль действий по внесению изменений в системы защиты информации;

− анализ потенциального воздействия планируемых изменений в системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИС ГБУК «Самарская областная библиотека для слепых»;

− определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИС ГБУК «Самарская областная библиотека для слепых» и их системы защиты информации;

− внесение информации (данных) об изменениях в базовой конфигурации ИС ГБУК «Самарская областная библиотека для слепых»и их системы защиты информации в эксплуатационную документацию на систему защиты информации ИС ГБУК «Самарская областная библиотека для слепых».

2.1.27. В случае возникновения нештатных ситуаций и аварийных ситуаций принимать меры по реагированию в пределах функций и полномочий с целью ликвидации последствий. Оперативно докладывать вышестоящему руководству о случаях возникновения внештатных ситуаций и аварийных ситуаций. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ИС ГБУК «Самарская областная библиотека для слепых». Предпринимаемые меры по возможности согласовывать с вышестоящим руководством.

3. Права

3.1.Администратор ИБ имеет право:

3.1.1. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС ГБУК «Самарская областная библиотека для слепых».

3.1.2. Непосредственно обращаться к пользователям АРМ с требованием прекращения работы в ИС ГБУК «Самарская областная библиотека для слепых» при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

3.1.3. В пределах своей компетенции сообщать своему непосредственному руководителю обо всех недостатках в работе ИС ГБУК «Самарская областная библиотека для слепых» и их системы защиты.

3.1.4. Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.5. Подписывать и визировать документы в пределах своих обязанностей в соответствии с настоящей Инструкцией.

3.1.6. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимый для надлежащего исполнения своих прав и обязанностей (в т.ч. вести мониторинг действий пользователей и обслуживающего персонала ИС Краткое наименование организации).

3.1.7. Вносить свои предложения по совершенствованию мер защиты информации в ИС ГБУК «Самарская областная библиотека для слепых».

4. Ответственность

4.1.Администратор ИБ ИС ГБУК «Самарская областная библиотека для слепых» несет ответственность:

4.1.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством

Российской Федерации.

4.1.2. За правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.1.3. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

Приложение №11

Инструкция
по уничтожению персональных данных в ГБУК "Самарская областная библиотека слепых"

1. Общие положения

1.1. Настоящая инструкция определяет порядок уничтожения и обезличивания информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в **ГБУК "Самарская областная библиотека слепых"** (далее — Оператор).

1.2. Инструкция разработана в соответствии с ч. 7 ст. 5, ч. 4 ст. 21 и п. 9 ч. 1 ст. 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — ФЗ «О персональных данных»), «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ», утвержденными приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 и иными нормативными правовыми актами РФ в области защиты персональных данных.

2. Условия и порядок уничтожения информации, содержащей персональные данные

2.1. Оператор уничтожает информацию, содержащую персональные данные: — по достижении целей обработки или в случае утраты необходимости в достижении этих целей;

— по достижении окончания срока хранения;

— при наступлении иных законных оснований.

2.2. Уничтожение информации, содержащей персональные данные, производится в случае достижения цели обработки в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

2.3. Уничтожение информации, содержащей персональные данные, производится в случае выявления неправомерной обработки в срок, не превышающий десяти дней с момента выявления неправомерной обработки персональных данных.

2.4. Ответственными за уничтожение информации, содержащей персональные данные, назначаются ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в информационной системе Оператора. Ответственные лица подписывают соответствующий «Акт об уничтожении персональных данных».

2.5. К персональным данным, хранимым в электронном виде, относятся файлы, папки, электронные архивы на жестком диске компьютера и съемных машинных носителях (компакт-дисках CD-R/RW или DVD-R/RW, дискетах 3,5, флеш-носителях).

2.6. Съемные машинные носители по истечению сроков обработки и хранения на них персональных данных подлежат уничтожению с целью невозможности восстановления и дальнейшего использования. Это достигается путем деформирования, нарушения единой целостности носителя или его сжигания.

2.7. В случае допустимости повторного использования съемного машинного носителя применяется программное удаление («затирание») содержимого путем его форматирования с последующей записью новой информации на данный носитель.

2.8. Подлежащие уничтожению файлы с персональными данными, расположенные на жестком диске информационной системы персональных данных, удаляются средствами операционной системы компьютера с последующим «очищением корзины».

2.9. Черновики документов, испорченные листы, варианты и не подписанные проекты документов уничтожаются путем их сожжения или измельчения или другим путем, исключающим восстановление текста документов.

3. Условия и порядок обезличивания информации, содержащей персональные данные

3.1. Оператор может обезличивать персональные данные в статистических или иных исследовательских целях, по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

— замена части данных идентификаторами;

— обобщение, изменение или удаление части данных;

— деление данных на части и обработка в разных информационных системах;

— перемешивание данных;

— другие способы.

3.3. В случае достижения целей обработки персональных данных или в случае утраты необходимости в достижении этих целей способом обезличивания является уменьшение перечня обрабатываемых данных.

3.4. Ответственный за организацию обработки персональных данных назначается ответственным за проведение мероприятий по обезличиванию персональных данных.

3.5. Решение о необходимости обезличивания персональных данных и способе обезличивания принимает ответственный за организацию обработки персональных данных.

3.6. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

3.7. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

3.8. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

3.9. В процессе обработки обезличенных данных, при необходимости, может производиться деобезличивание. После обработки персональные данные, полученные в результате такого деобезличивания, уничтожаются.

3.10. Обработка персональных данных до осуществления процедур обезличивания и после выполнения операций деобезличивания должна осуществляться в соответствии с законодательством Российской Федерации с применением мер по обеспечению безопасности персональных данных.

4. Ответственность

4.1. Ответственность за осуществление контроля выполнения требований настоящей инструкции несет ответственный за организацию обработки персональных данных Оператора.

4.2. Ответственность за выполнение настоящей инструкции возлагается на ответственного за организацию обработки персональных данных, ответственного за обеспечение безопасности персональных данных и всех работников Оператора, допущенных к обработке обезличенных персональных данных, в соответствии с действующим законодательством.

Приложение № 12

Директору ГБУК «Самарская областная библиотека для слепых»
От _____
_____
зарегистрированного по адресу:
_____
_____
Паспорт_____№_____
_____

Письменное согласие
субъекта на обработку персональных данных

Я, _____
_____
_____
_____
_____
(Ф.И.О., паспортные данные, в т.ч. дата выдачи, выдавший орган)

руководствуясь ст. 10.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в целях:

обеспечения соблюдения законов и иных нормативных правовых актов; трудовых отношений и иных непосредственно связанных с ними отношений, в том числе размещения информации обо мне на официальном сайте, в средствах информации (открытых источниках), использования моих контактных данных даю согласие на распространение подлежащих обработке персональных данных ГБУК «Самарская областная библиотека для слепых» в следующем порядке:

- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения;
- паспортные данные;
- адрес регистрации по месту жительства и адрес фактического проживания;
- номер телефона (домашний, мобильный);
- данные документов об образовании, квалификации, профессиональной

подготовке, сведения о повышении квалификации;

- семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым и налоговым законодательством;

- отношение к воинской обязанности;

- сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;

- номер СНИЛС, ИНН;

- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в ГБУК «Самарская областная библиотека для слепых»;

- сведения о доходах в ГБУК «Самарская областная библиотека для слепых»

- биометрические данные (внешность, голос);

- специальные данные (раса, национальность, политические взгляды, вероисповедание);

- состояние здоровья;

- сведения о деловых и иных личных качествах, носящих оценочный характер.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

« ___ » _____ 20___ г. _____

(подпись)

Приложение № 13

Директору ГБУК «Самарская областная библиотека для слепых»
От_____
_____
зарегистрированного по адресу:
_____
_____
Паспорт_____ № _____
_____
_____

СОГЛАСИЕ
на обработку персональных данных соискателя

Я, _____,
(фамилия, имя, отчество полностью)
в соответствии со статьей 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- начисления заработной платы, предоставления налоговых вычетов;
- исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений о налогах на доходы физлиц в ФНС России, сведений в ФСС РФ;
- предоставления сведений в кредитные организации для оформления банковской карты и перечисления на нее заработной платы и других выплат;
- предоставления сведений третьим лицам для выполнения конкретных функций, связанных с выполнением моих должностных обязанностей;
- предоставления данных для формирования справочных материалов для

внутреннего информационного обеспечения деятельности организации;

- обеспечения пропускного и внутриобъектового режимов в организации;
- обеспечения моей безопасности;
- обеспечения сохранности имущества работодателя

даю согласие ГБУК «Самарская областная библиотека для слепых», расположенному по адресу: г. Самара, ул. Никитинская, д. 21, на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно обработку, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение следующих персональных данных в документальной и/или электронной форме:

- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения;
- паспортные данные;
- адрес регистрации по месту жительства и адрес фактического проживания;
- номер телефона (домашний, мобильный);
- данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;
- семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым и налоговым законодательством;
- отношение к воинской обязанности;
- сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;
- номер СНИЛС, ИНН;
- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в ГБУК «Самарская областная библиотека для слепых»;
- сведения о доходах в ГБУК «Самарская областная библиотека для слепых»
- биометрические данные (внешность, голос);
- специальные данные (раса, национальность, политические взгляды, вероисповедание);
- состояние здоровья;
- сведения о деловых и иных личных качествах, носящих оценочный характер.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

« ___ » _____ 20___ г. _____

(подпись)