ДЕПАРТАМЕНТ КУЛЬТУРЫ ГОРОДА МОСКВЫ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ КУЛЬТУРЫ ГОРОДА МОСКВЫ "МУЗЕЙ М.А.БУЛГАКОВА"

П Р И К А З

26 декабря 2018г. № 98-09

Об утверждении Положения о защите персональных данных работников ГБУК г. Москвы "Музей М.А. Булгакова"

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных" и на основании главы 14 Трудового кодекса Российской Федерации **приказываю:**

1. Утвердить Положение о защите персональных данных работников ГБУК г. Москвы "Музей М.А. Булгакова" приложение 1 к настоящему приказу.
2. Ввести в действие **с 01.01.2019** Положение о защите персональных данных работников ГБУК г. Москвы "Музей М. А. Булгакова" (далее – Положение)
3. **Бухгалтеру И.Ф.Федотовой:**

- ознакомить всех работников с Положением согласно приложению 2 к настоящему приказу.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор **П.В.Мансилья-Круз**

Приложение 1
К приказу Государственного
бюджетного учреждения культуры
города Москвы "Музей М.А. Булгаков"
от "26" декабря 2018 г. № 98-од

ПОЛОЖЕНИЕ
о защите персональных данных работников Государственного бюджетного учреждения культуры города Москвы "Музей М.А. Булгакова"

Москва
2018 год

1. Общие положения

1.1. ГБУК г. Москвы "Музей М.А. Булгакова", являясь работодателем (оператором), осуществляет работу с персональными данными работников Учреждения (субъекта персональных данных), руководствуясь соответствующими нормами Конституции Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", а также общепризнанными принципами и нормами международного права и международных договоров Российской Федерации, которые в соответствии с частью четвертой статьи 15 Конституции Российской Федерации являются составной частью российской правовой системы.

Так, в соответствии с частью первой статьи 23 Конституции Российской Федерации каждый гражданин имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

1.2. Целью разработанного Положения о защите персональных данных работников Государственного бюджетного учреждения культуры города Москвы "Музей М.А. Булгакова" (далее – Положение) является защита персональных данных от несанкционированного доступа третьих лиц и организация приема, хранения, обработки и передачи персональных данных работников в соответствии с установленными законодательными требованиями.

1.3. Сбор, хранение, использование и распространение информации о частной жизни работника без письменного его согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации.

Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении архивного срока хранения документов, если иное не определено законодательством Российской Федерации.

1.4. Порядок утверждения данного Положения, ввода его в действие и внесения изменений:

- утверждается и вводится в действие приказом директора ГБУК г. Москвы "Музей М.А. Булгакова".

2. Понятие и состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

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

- **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими

лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

- **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

- **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- **конфиденциальность персональных данных** - обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия работника или наличия иного законного основания.

- **общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование о соблюдении конфиденциальности;

- **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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

- **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- **трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу

власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.2. Состав персональных данных – документы, из которых могут быть получены работодателем персональные данные работника:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета;
- документ об образовании, о квалификации или о наличии специальных знаний или специальной подготовки.

2.3. Дополнительные документы (справка о доходах с предыдущего места работы, справка из органов государственной налоговой службы о предоставлении сведений об имущественном положении, справку о наличии (отсутствии) судимости, медицинское заключение о состоянии здоровья и др.).

2.3.1. Автобиографические данные:

- сведения о стаже работы;
- сведения о составе семьи;
- сведения о социальных льготах;
- адрес места жительства;
- домашний, контактный телефон;
- сведения о состоянии в браке;
- сведения о знании иностранных языков;
- место работы или учебы членов семьи и родственников.

2.3.2. Сведения о фактах, событиях и обстоятельствах жизни работника, позволяющих идентифицировать его личность.

2.3.3. Сведения о заработной плате.

2.3.4. Дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям.

2.3.5. Основания к приказам по личному составу.

2.3.6. Подлинники и копии приказов по личному составу.

2.3.7. Состав декларируемых сведений о наличии материальных ценностей.

2.3.8. Содержание декларации, подаваемой в налоговую инспекцию.

3. Сбор, обработка и хранение персональных данных

3.1. Все персональные данные работника следует получить у него самого. Если персональные данные работника, возможно, получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих

получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.2. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях, информацию о национальной принадлежности работника и частной жизни.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

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

3.4. Состав работников, допущенных к обработке, передаче и хранению персональной информации:

3.4.1. Полный доступ к обработке, передаче и хранению персональных данных работника могут иметь следующие работники:

- директор;
- главный бухгалтер;
- специалист по кадрам и делопроизводству;

3.4.2. Ограниченный доступ к обработке, передаче и хранению персональных данных работника могут иметь следующие работники:

Наименование должности	Персональные данные и перечень документов, к которым может быть допущено должностное лицо. А также цели, для которых данное должностное лицо имеет право обрабатывать данные сведения.
- заместитель директора по административно-управленческой работе, - заместитель директора по музейно-образовательной деятельности, - заместитель директора по научно-просветительской деятельности.	- фамилия, имя, отчество, номер мобильного и контактного телефона, адрес электронной почты;

- бухгалтер,	- фамилия, имя, отчество, паспортные данные работника, адрес места постоянной и временной регистрации, адрес места фактической регистрации, номер домашнего, мобильного и контактного телефона, адрес электронной почты, дата и место рождения, ИНН, страховое свидетельство государственного пенсионного страхования, сведения, относящиеся к трудовой деятельности субъекта (трудовая книжка, стаж работы, сведения о заработной плате), сведения о социальных льготах, пенсионном обеспечении, медицинском страховании, данные об инвалидности – ФСС, ПФР, 2-НДФЛ, органы исполнительной власти, для оформления бухгалтерской, налоговой, статистической отчетности; - при автоматизированной обработке персональных данных в 1С УАИС бюджетный учет; - сведения об иждивенцах – для произведения необходимых вычетов из заработной платы, установленных законодательно; - фамилия, имя, отчество, паспортные данные работника, дата и место рождения, адрес места жительства, номер домашнего, мобильного и контактного телефона, адрес электронной почты, ИНН, страховое свидетельство государственного пенсионного страхования – на право предоставления интересов учреждения перед третьими лицами (казначейство, ЕАИСТ2*, ЕИС**), при подготовке документации по запросам прокуратуры, ФАС РФ, Главного контрольного управления г. Москвы, Департамента г. Москвы по конкурентной политике
- юрисконсульт	- фамилия, имя, отчество, паспортные данные работника, адрес места постоянной и временной регистрации – при подготовке и для оформления доверенностей, на право предоставления интересов учреждения перед третьими лицами (суд, почта и пр.); - фамилия, имя, отчество, паспортные данные работника, адрес места жительства, ИНН – при подаче документов на государственную регистрацию в МИ ФНС, портал госуслуг
- администратор; - заведующий отделом; - ученый секретарь.	- фамилия, имя, отчество, паспортные данные работника, адрес места жительства – для заполнения анкет на участие в конкурсах и при подаче заявок на участие в профессиональных конкурсах, - фамилия, имя, отчество, номер домашнего, мобильного и контактного телефона, адрес электронной почты - на право предоставления интересов учреждения перед третьими лицами (Мосгорзазвитие, Департамент культуры г. Москвы);
- старший научный сотрудник;	- фамилия, имя, отчество, номер мобильного и контактного телефона, адрес электронной почты - для проведения мероприятий
- главный хранитель музейных предметов; - хранитель музейных предметов	- фамилия, имя, отчество, номер мобильного и контактного телефона, адрес электронной почты - КАМИС
- главный инженер	- фамилия, имя, отчество, номер страхового свидетельства государственного пенсионного страхования, паспортные данные, медицинские ограничения – для проведения спецоценки условий труда; - паспортные данные, дата рождения - для проведения инструктажей и заполнения журналов

* ЕАИСТ2 - единая автоматизированная информационная система торгов города Москвы (версия 2)

**ЕИС - единая информационная система.

3.4.3. Лицо, ответственное за организацию обработки персональных данных назначается приказом директора.

Определить следующие обязанности ответственному за организацию обработки персональных данных:

- осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

- доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, требований к защите персональных данных;

- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

На время отсутствия ответственного за организацию обработки персональных данных (отпуск, командировка, болезнь и т.п.) обязанности перекладываются на лицо, назначенное приказом директора в установленном порядке.

3.4.4. Конкретный перечень лиц, получающих доступ к персональным данным и осуществляющих их обработку, утверждается приказом директора.

3.5. Порядок обработки, передачи и хранения персональной информации.

3.5.1. В соответствии со статьей 86 Трудового кодекса Российской Федерации в целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника должны соблюдать следующие общие требования:

- обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

- при определении объема и содержания, обрабатываемых персональных данных работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными федеральными законами;

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

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

- работники не должны отказываться от своих прав на сохранение и защиту тайны.

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

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

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

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

- осуществлять передачу персональных данных работника в пределах одной организации в соответствии с данным локальным нормативным актом работодателя;

- 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 Российской Федерации и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций;

- все меры конфиденциальности при сборе, обработке и хранении персональных данных работника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации;

- не отвечать на вопросы, касающиеся персональных данных работника по телефону или факсу. Передавать по телефону запрошенную третьими лицами информацию только в присутствии работника, либо с его письменного согласия.

3.5.3. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники 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 федеральным законом;

- определение своих представителей для защиты своих персональных данных;

- требование об исключении или исправлении неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса 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 суде любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных;

- работодатель, работники и их представители должны совместно вырабатывать меры защиты персональных данных работника.

3.6. Ответственность за разглашение:

3.6.1. Все лица, непосредственно имеющие отношение к персональной базе данных, должны подписывать обязательство о неразглашении персональной информации работников.

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

3.6.3. Руководитель, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

3.6.4. Каждый работник Учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

3.6.5. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и влечет привлечение к ответственности в соответствии с законодательством.

3.6.6. Ответственность лиц, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, согласно действующему законодательству может быть дисциплинарной, административной, гражданско-правовой или уголовной в соответствии с федеральными законами.

4. Доступ к персональным данным работника

4.1. Внутренний доступ.

4.1.1. Право доступа к персональным данным работника, имеют лица, указанные в п. 3.4. настоящего Положения.

Другие работники Учреждения имеют доступ к персональным данным работника только с письменного согласия самого работника, субъекта данных.

4.1.2. По письменному заявлению работника работодатель обязан не позднее трех рабочих дней со дня подачи этого заявления выдать работнику копии документов, связанных с работой (копии приказа о приеме на работу, приказов о переводах на другую работу, приказ об увольнении с работы; выписки из трудовой книжки; справки о заработной плате, периоде работы у данного работодателя и другое). Копии документов, связанных с работой, должны быть заверены надлежащим образом и представляться работнику безвозмездно.

4.2. Внешний доступ.

4.2.1. К числу лиц, допущенных к персональным данным работника, имеют организации (и, соответственно, должностные лица данных организаций), осуществляющие контрольные и надзорные функции, а также другие лица, установленные федеральными законами, в частности:

- инспекции труда (инспекторы труда правового департамента и департамента охраны труда);
- прокуратура Российской Федерации;
- правоохранительные органы;
- налоговые инспекции;
- военкоматы;
- органы, осуществляющие миграционный учет иностранных граждан;
- органы ФСС Российской Федерации;
- органы Пенсионного фонда Российской Федерации.

4.2.2. Органы и должностные лица, указанные в п. 4.2.1. настоящего Положения, имеют доступ к информации только в сфере своей компетенции, в порядке, установленном законодательством Российской Федерации.

4.2.3 Организации, в которые работник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае письменного разрешения работника.

4.2.4. Сведения о работающем или уже уволенном работнике могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника с согласием (разрешением, просьбой предоставить сведения о работнике).

4.2.5. Персональные данные работника могут быть предоставлены

родственникам или членам его семьи только с письменного разрешения самого работника. В случае развода и отсутствия соглашения сторон об уплате алиментов, справка о заработной плате работника может быть предоставлена в суд без его согласия, на основании письменного запроса и определения суда.

5. Защита персональных данных

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

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

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

5.2. Внутренняя защита.

5.2.1. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации.

Для защиты персональных данных работников работодатель принимает следующие меры:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны. Для этого со всеми работниками, допущенными к персональным данным, проводится при допуске и периодически соответствующий инструктаж и обучение;
- наличие необходимых условий, исключающих несанкционированный доступ в помещения для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

- организация порядка уничтожения информации;

- разъяснительная работа с работниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами. Данная обязанность возложена на руководителей структурных подразделений, в подчинении которых находятся работники, допущенные к персональным данным;

- не допускается выдача личных дел работников на рабочие места. Личные дела могут выдаваться на рабочие места только директору и главному бухгалтеру.

5.2.2. Защита персональных данных на бумажных носителях:

- все документы, содержащие персональные данные работников, хранятся в кабинете бухгалтерии, в специально отведенном для этого месте, с применением специального оборудования (металлические несгораемые шкафы, сейфы).

Ключи от специального оборудования в рабочее время хранятся у специалиста по кадрам и делопроизводству, главного бухгалтера, без права передачи третьим лицам, на время их отсутствия ключи хранятся у лица, исполняющего обязанности руководителя подразделения.

5.2.3. Защита персональных данных при автоматизированной обработке персональных данных - обработка персональных данных с помощью средств вычислительной техники:

- информация о персональных данных работников на компьютерах доступна только для строго определенных сотрудников и хранится на персональных компьютерах с доступом через пароль.

5.3. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации.

5.3.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных".

5.3.2. Оператором осуществляется классификация информационных систем персональных данных в соответствии с Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" в зависимости от категории обрабатываемых данных и их количества.

5.3.3. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии:

- утвержденных организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт классификации ИСПДн, инструкции пользователя, администратора

по организации антивирусной защиты, и других нормативных и методических документов;

- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;

- охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

5.3.4. Информационные системы персональных данных:

Наименование системы	Подразделение предприятия	Доступ в интернет	Объем данных	Наименование документа
УАИС Бюджетный учет	Бухгалтерия	Да	от 500-5000	Постановление Правительства Москвы от 19.08.2014 №466-ПП
СБИС	Бухгалтерия	Да, используется Крипто Про	от 500	
Файлы Microsoft Word, Microsoft Excel	Бухгалтерия, кадры.	Не используется	от 1000 – 100000	

5.4. Порядок обработки персональных данных без использования средств автоматизации.

5.4.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

5.4.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

5.4.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории

персональных данных.

5.5. Внешняя защита.

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

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

5.5.2. Для защиты персональных данных работников работодатель соблюдает следующие меры:

- технические средства охраны, сигнализации (ответственность за их бесперебойной работой лежит на главном инженере;
- порядок охраны зданий и помещений (ответственность за охрану лежит на главном инженере);
- требования к защите информации при собеседованиях (контроль за соблюдением данного требования лежит на специалисте по кадрам и делопроизводству).

6. Заключительные положения

6.1. Настоящее Положение о защите персональных данных работников вступает в силу с момента его утверждения приказом директора ГБУК г. Москвы "Музей М.А. Булгакова" и действует до введения нового Положения о защите персональных данных работников.

6.2. Ознакомление работников с условиями настоящего Положения производится под роспись в листе ознакомления (приложение) или при приеме на работу под роспись в трудовом договоре.

6.3. Подпись работника в листе ознакомления с Положением о защите персональных данных работников означает его согласие и обязательство исполнения.