Принято
Общим собранием трудового коллектива
МАУДО «Детская школа искусств»
Протокол № 1 от «18» 01 2023г.

Утверждаю
Директор МАУДО
«Детская школа искусств»
_____ Н.С. Борознова
Приказ № 6 от «18» 01 2023г.

Согласовано:
Председатель профкома
_____ Э.З. Федорова

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников
муниципального автономного учреждения дополнительного образования города Набережные Челны «Детская школа искусств»

1. Общие положения

1.1. Настоящее Положение определяет порядок организации и проведения работ по защите конфиденциальной информации в Муниципальном автономном учреждении дополнительного образования города Набережные Челны «Детская школа искусств» (далее – ДШИ).

1.2. Под информацией ограниченного доступа понимаются сведения, доступ к которым ограничен нормативно-правовыми актами, в частности Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (ред. от 13.07.2015).

1.3. Персональные данные (далее – Д) относятся к информации ограниченного доступа (далее – информация), так как попадают под действие Федерального закона Российской Федерации от 27.07.2006 №152 «О персональных данных» (с изменениями на 02.07.2021).

1.4. Целью разработки Положения – определение порядка обработки персональных данных работников ДШИ, персональные данные которых подлежат обработке, на основании полномочий оператора (ДШИ); обеспечение защиты прав и свобод человека и гражданина, в т.ч. работника ДШИ, при обработке его персональных данных. в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.5. Настоящее Положение разработано на основании ст. 24 Конституции РФ, главы 14 Трудового Кодекса РФ, Закона «Об информации, информатизации и защите информации» № 149-ФЗ от 27.07.2006 г. (ред. от 29.12.2022), Федерального закона РФ «О персональных данных» №152-ФЗ от 27.07.2006 г. (с изменениями на 02.07.2021), Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства РФ от 15.09.2008 №687, Положением об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства РФ от 01.11.2012г. №1119, Кодекса об административных нарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса, а также иными нормативно-правовыми актами в сфере защиты персональных данных.

1.6. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75-летнего срока хранения, если иное не определено законом.

1.7. Положение предназначено для практического использования должностным лицам ответственным за защиту информации.

1.8. Настоящее Положение утверждается и вводится в действие приказом директора ДШИ и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

1.9. Персональная ответственность за организацию и выполнение мероприятий по защите информации возлагается на сотрудника ДШИ, назначенного приказом.

1.10. Ответственность за обеспечение защиты информации возлагается непосредственно на пользователя информации в соответствии с «Инструкцией пользователя информационной системы персональных данных», утвержденной директором ДШИ.

1.11. Проведение работ по защите информации в ИС с помощью встроенных средств безопасности, сертифицированных лицензионных операционных систем и антивирусного программного обеспечения, выполнения требований настоящего Положения, возлагается на ответственного за защиту информации в ДШИ (далее – ответственный).

1.12. Лица, виновные в нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством.

1.13. Положение вступает в действие с момента его утверждения директором ДШИ и действует бессрочно, до замены его новым Положением.

2. Основные термины

2.1. В соответствии с действующим законодательством в настоящем положении применяются следующие термины:

2.1.1. *персональные данные* – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями;

2.1.2. *персональные данные, разрешенные субъектом персональных данных для распространения*, – персональные данные, доступ неограниченного круга лиц которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных для распространения в порядке, предусмотренном ФЗ «О персональных данных»;

2.1.3. *оператор* – юридическое 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;

2.1.4. *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, уничтожение персональных данных;

2.1.5. *автоматизированная обработка персональных данных* – обработка персональных данных с помощью средств вычислительной техники;

2.1.6. *распространение персональных данных* – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

2.1.7. *предоставление персональных данных* – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

2.1.8. *блокирование персональных данных* – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи (за исключением случаев, если обработка необходима для уточнения персональных данных);

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

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

2.1.11. *информационная система персональных данных* – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технологических средств.

3. Понятие и состав персональных данных

3.1.В состав персональных данных работника (сотрудника ДШИ) входят документы, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, состоянии здоровья, а также о предыдущих местах их работы.

3.2.Комплекс документов, сопровождающий процесс оформления трудовых отношений работника в ДШИ при его приеме, переводе и увольнении.

3.3.Информация, представляемая работником при поступлении на работу в

ДШИ, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

– заявление о приёме на работу;

– паспорт или иной документ, удостоверяющий личность;

– трудовая книжка (либо сведения о трудовой деятельности, в случае перехода на электронную трудовую книжку);

– номер страхового свидетельства государственного пенсионного страхования (СНИЛС);

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

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

– сведения о повышении квалификации;

– свидетельство о присвоении ИНН;

– адрес регистрации;

– адрес проживания;

– номер телефона;

– дата и место рождения;

– сведения о детях и семейном положении;

– фото;

– справка об отсутствии судимости;

– сведения о наградах (поощрениях), почетных званиях;

– e-mail и любая другая информация прямо или косвенно относящаяся к работнику.

3.4. В дальнейшем в отделе кадров в личную карточку Т-2 вносятся данные из п. 3.3. настоящего Положения, а также:

– сведения о социальных гарантиях;

– сведения об отпусках и т.д.

3.5. В отделе кадров Организации создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

3.5.1. Документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию; проведению собеседований с кандидатом на должность; копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; копии отчетов, направляемых в государственные и муниципальные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

4. Обработка персональных данных

4.1. Под обработкой персональных данных работника понимается получение, хранение, комбинирование, передача или любое другое использование

персональных данных работника.

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

4.2.1. Персональные данные работника используются для целей, связанных с выполнением работником трудовых функций. Работодатель для этой цели запрашивает у работника общие персональные данные: фамилию, имя, отчество, дату, месяц и год рождения, место рождения, адрес, семейное положение, образование, профессию; специальные категории персональных данных: состояние здоровья, сведения о судимости, биометрические персональные данные: фото в бумажном и электронном виде.

4.2.2. Работодатель не принимает, не снимает и не хранит копии личных документов работников. Документы, которые работник предъявляет работодателю для хранения в оригинале (справки, медицинские заключения и т.д.) хранятся в личном деле работника в течение 50 лет после расторжения с работником трудового договора.

4.2.3. После истечения срока нормативного хранения документов, которые содержат персональные данные работника, документы подлежат уничтожению. Для этого работодатель создает экспертную комиссию и проводит экспертизу ценности документов. В ходе проведения экспертизы комиссия отбирает дела с истекшими сроками хранения и по итогам отбора составляет акт о выделении к уничтожению дел, не подлежащих хранению. После чего документы измельчаются в шредере. Персональные данные работников в электронном виде стираются с информационных носителей, либо физически уничтожаются сами носители, на которых хранится информация.

4.2.4. При определении объема и содержания, обрабатываемых персональных данных работника, работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.

4.2.5. Все персональные данные работника ДШИ следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо работодателя должно сообщить работнику ДШИ 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.

4.2.6. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях, и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны работодателем только с его письменного согласия.

Обработка указанных персональных данных работников работодателем возможна только с их согласия либо без их согласия в следующих случаях:

– персональные данные относятся к состоянию здоровья работника и их

обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;

– по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

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

4.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники:

– директор;

– специалист по кадрам;

– заместители директора по учебно-воспитательной работе и заместитель по хозяйственной работе (только к персоналу своего структурного подразделения);

– главный бухгалтер и бухгалтер 1 категории.

4.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

4.4.1. 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 карается в соответствии с законодательством.

4.5. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.

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

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

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

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

– разрешать доступ к персональным данным работников только специально полномоченным лицам, определенным приказом по организации, при этом казанные 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 ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

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

4.5.3. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы ДШИ работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.

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

4.6.1. Трудовые книжки хранятся в сейфе в приемной.

4.6.3. Личные дела, личные карточки по форме Т-2, документы, содержащие персональные данные, необходимые для осуществления выплат заработной платы работникам и других выплат, и отчислений (в Пенсионный фонд, в Фонд социального страхования) хранятся в приемной.

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

4.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

4.9. 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. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

5. Доступ к персональным данным

5.1.Внутренний доступ (доступ внутри школы).

5.1.1. Право доступа к персональным данным сотрудника имеют:

– директор;

– заместители директора по учебно-воспитательной работе;

– заместитель директора по хозяйственной работе (доступ к личным данным только сотрудников своего подразделения);

– специалист по кадрам;

– сам работник, носитель данных;

– главный бухгалтер и бухгалтер 1 категории.

5.2.Работник ДШИ имеет право:

5.2.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные работника.

5.2.2. Требовать от Работодателя уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для Работодателя персональных данных.

5.2.3. Получать от Работодателя:

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

5.2.4. Требовать извещения Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.2.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Работодателя при обработке и защите его персональных данных.

5.3. Копировать и делать выписки персональных данных работника разрешается исключительно в служебных целях с письменного разрешения специалиста по кадрам или директора.

5.4. Передача информации третьей стороне возможна только при письменном согласии работников.

5.5. Внешний доступ.

5.5.1. К числу массовых потребителей персональных данных вне ДШИ можно отнести государственные и негосударственные функциональные структуры:

– налоговые инспекции; правоохранительные органы; органы статистики;

– страховые агентства;

– военкоматы;

– органы социального страхования;

– пенсионные фонды;

– подразделения муниципальных органов управления администрации города Набережные Челны;

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

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

5.5.4. Другие организации.

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

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

В случае развода бывшая супруга (супруг) имеют право обратиться в ДШИ с письменным запросом о размере заработной платы сотрудника без его согласия. (УК РФ).

6. Защита персональных данных

6.1. Целью технической защиты информации в ДШИ является предотвращение несанкционированного доступа к информации при её обработке в информационных системах, связанные с действиями нарушителей, включая пользователей информационных систем, реализующих угрозы непосредственно в информационных системах, а также нарушителей, не имеющих доступ к информационным системам, реализующих угрозы из сетей международного информационного обмена с целью её разрушения, искажения, уничтожения, блокировки и несанкционированного копирования.

6.2. Целями организационных мероприятий по защите информации в ДШИ являются:

– исключение непреднамеренных действий сотрудников ДШИ, приводящих к утечке, искажению, разрушению информации, в том числе ошибки эксплуатации автоматизированной системы;

– сведение к минимуму возможности нарушения политик безопасности с помощью любых средств, не связанных непосредственно с использованием автоматизированной системы (физический вынос информации на электронном носителе).

6.3. Директор ДШИ самостоятельно определяет состав, перечень мер необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных п.1.4. настоящего Положения.

К таким мерам могут, в частности, относиться:

– назначение ответственного за организацию защиты информации;

– издание комплекта документов, определяющих политику в отношении обработки ПД в ДШИ, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации;

– использование средств антивирусной защиты;

– предотвращение организационными мерами НСД к обрабатываемой информации;

– организация процесса резервного копирования и архивирования как неотъемлемой части

– политики защиты информации;

– осуществление учета машинных носителей информации и их хранение в надежно запираемых шкафах.

6.4. В целях защиты персональных данных на бумажных носителях работодатель:

– назначает ответственных за обработку персональных данных;

– хранит документы, содержащие персональные данные работников в шкафах,

запирающихся на ключ;

– хранит трудовые книжки работников в сейфе в приёмной.

6.5. В целях обеспечения конфиденциальности документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только специалистом по кадрам и бухгалтерией.

6.6. Работники, допущенные к персональным данным работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных работников не допускаются.

7. Особенности обработки информации, содержащей персональные данные

7.1. ДШИ не имеет права получать и обрабатывать данные субъекта ПД о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

7.2. Обработка указанных данных возможна без его согласия в соответствии со ст. 6 Федеральным законом от 27.07.2006 № 152 «О персональных данных» (с изменениями на 02.07.2021).

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

– фамилию, имя, отчество, адрес субъекта ПД, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта ПД;

– цель обработки ПД;

– перечень ПД, на обработку которых дается согласие субъекта персональных данных;

– перечень действий с ПД, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПД;

– срок, в течение которого действует согласие субъекта ПД, а также способ его отзыва, если иное не установлено федеральным законом;

– подпись субъекта персональных данных.

7.4. Согласие на обработку ПД может быть отозвано субъектом ПД по письменному запросу на имя директора ДШИ.

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

7.6. Субъекты ПД не должны отказываться от своих прав на сохранение и

защиту тайны.

7.7. Субъект ПД имеет право на получение следующей информации:

– сведения о лицах, которые имеют доступ к ПД или которым может быть предоставлен такой доступ;

– перечень обрабатываемых ПД и источник их получения;

– сроки обработки ПД, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта ПД может повлечь за собой обработка его ПД.

7.8. Субъект ПД вправе требовать от оператора уточнения своих ПД, их блокирования или уничтожения в случае, если ПД являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

7.9. Сведения о ПД должны быть предоставлены субъекту ПД оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам ПД.

7.10. Доступ к своим ПД предоставляется субъекту ПД или его законному представителю оператором при получении письменного запроса субъекта ПД или его законного представителя. Письменный запрос должен быть адресован на имя зам.директора ДШИ или уполномоченного руководителем лицо.

7.11. Субъект в праве обжаловать в судебном порядке неправомерные действия или бездействия должностных лиц ДШИ при обработке и защите его ПД.

7.12. 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.

7.13. 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.

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

7.15. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

7.16. «Внутренняя защита».

7.16.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для

разграничения полномочий между руководителями и специалистами организации.

7.16.2. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно - методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места. Личные дела могут выдаваться на рабочие места только директору, работникам службы управления персоналом и в исключительных случаях, по письменному разрешению директора, - заместителям директора (например, при подготовке материалов для аттестации работника).

7.17. «Внешняя защита».

7.17.1. 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.

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

7.17.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряда мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- учет и порядок выдачи удостоверений;
- технические средства охраны, сигнализации;

- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

7.18. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

7.19. По возможности персональные данные обезличиваются.

7.20. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

8. Права и обязанности должностных лиц

8.1.Директор ДШИ организует работу по построению системы защиты информационных систем. В частности:

8.1.1. Назначает ответственного за организацию защиты информации из числа сотрудников ДШИ.

8.1.2. Утверждает состав комиссии по организации работ по защите информации.

8.1.3. Утверждает комплект документов, определяющих политику в отношении обработки ПД в учреждении, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации.

8.1.4. Утверждает меры и состав средств СЗИ, предложенных для обеспечения безопасности ПД при их обработке в ИСПД. При этом оценивает соотношение вреда, который может быть причинен субъектам ПД и принимаемых мер по защите ИСПД.

8.2. Директор ДШИ:

- составляет Перечень сведений конфиденциального характера в ДШИ;
- контролирует работу ответственного по организации и проведению работ по защите информации в ДШИ;
- предотвращает организационными мерами НСД к обрабатываемой в ИС информации;
- контролирует порядок подготовки, учета и хранения документов конфиденциального характера;
- контролирует порядок передачи информации другим органам и организациям, а также между структурными подразделениями своей организации;
- организуют выполнение мероприятий по защите информации при использовании технических средств;
- участвует в определении мест установки и количества СОУТ, необходимых для обработки информации, а также пользователей этих ИС;
- участвует в определении правил разграничения доступа к информации в ИС, используемых в ДШИ.

8.3. Ответственный:

- разрабатывает организационно-распорядительные документы по вопросам защиты информации при её обработке с помощью ИС;
- контролирует исполнение приказов и распоряжений вышестоящих

организаций по вопросам обеспечения безопасности информации;

- знакомит работников ДШИ, непосредственно осуществляющих обработку ПД, с положениями законодательства Российской Федерации о ПД, в том числе требованиями к защите ПД;

- обеспечивает защиту информации, циркулирующей на объектах информатизации, организовывает работы по декларированию (аттестации) ИС на соответствие нормативным требованиям;

- устанавливает систематический контроль работы СЗИ, применяемых в ИС, а также за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;

- проводит инструктаж пользователей ИС;

- контролирует выполнение администратором ИС обязанностей по обеспечению функционирования СЗИ (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам ИС, антивирусная защита, резервное копирование данных и т.д.)

- контролирует порядок учёта и хранения машинных носителей конфиденциальной информации;

- присутствует (участвует) в работах по внесению изменений в аппаратно-программную конфигурацию ИС;

- определяет порядок и осуществляет контроль ремонта средств вычислительной техники, входящих в состав ИС;

- принимает меры по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших допуск к ИС;

- требует устранения выявленных нарушений и недостатков, давать обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;

- требует от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;

- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в случае выявления попыток НСД к информации или попыток хищения, копирования, изменения незамедлительно принимает меры пресечения и докладывает вышестоящему ДШИ;

- в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

9. Планирование работ по защите информации

9.1. Планирование работ по защите информации проводится на основании:

- рекомендаций актов проверок контрольными органами;
- результатов анализа деятельности в области защиты информации;
- рекомендаций и указаний Роскомнадзора и ФСТЭК России;

10. Контроль состояния защиты информации

10.1. С целью своевременного выявления и предотвращения несанкционированного доступа к информации, хищения технических средств и

носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность систем информатизации, осуществляется контроль состояния и эффективности средств защиты информации.

10.2. Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

10.3. Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты информации, проводится ответственным.

10.4. Плановые и внеплановые проверки за соответствием обработки персональных данных требованиям законодательства могут осуществляться территориальными органами Федеральной службы по надзору в сфере связи и массовых коммуникаций (далее – Роскомнадзор).

10.5. Допуск представителей этих органов для проведения контроля осуществляется в установленном порядке по предъявлению служебных удостоверений и предписаний на право проверки, подписанных руководителем (заместителем) соответствующего органа.

10.6. Ответственный обязан присутствовать при всех проверках по вопросам защиты информации.

10.7. Результаты проверок отражаются в Актах проверок.

10.8. По результатам проверок контролирующими органами ответственный с привлечением заинтересованных должностных лиц в десятидневный срок разрабатывает план устранения выявленных недостатков.

10.9. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

10.10. При обнаружении нарушений директор ДШИ принимает необходимые меры по их устранению в сроки, согласованные с органом или должностным лицом, проводившим проверку.

10.11. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

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

10.13. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

- требовать исключения или исправления неверных, или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны.

10.14. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;
- своевременно сообщать работодателю об изменении своих персональных данных.

10.15. Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

10.16. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

11. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

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

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

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

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

11.5.Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

11.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

11.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо

несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

11.5.3. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

11.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

11.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

12. Уведомление об обработке персональных данных

12.1.Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор РФ) о своем намерении осуществлять обработку персональных данных.

12.2. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения:

– наименование (фамилия, имя, отчество), адрес оператора;

– цель обработки персональных данных;

– категории персональных данных;

– категории субъектов, персональные данные которых обрабатываются;

– правовое основание обработки персональных данных;

– перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

– описание мер по обеспечению безопасности персональных данных при их обработке;

– фамилия, имя, отчество физических лиц, ответственных за организацию обработки персональных данных, номера их контактных телефонов, почтовые адреса и адреса электронной почты;

– дата начала обработки персональных данных;

– срок и условие прекращения обработки персональных данных;

– сведения о месте нахождения базы данных информации, содержащей

персональные данные.

12.3. Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

12.4. В случае изменения сведений, указанных в п.12.2, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.