МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

НАЧАЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА «ОТКРЫТИЕ»

г. Хабаровск

ПРИНЯТО
Общим собранием
работников учреждения
«30» 08 2014 г
протокол № 1

УТВЕРЖДЕНО
и введено в действие
приказом «01» 09 2014 года
№ 104
Директор Л.В.Змеева

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите персональных данных в МАОУ НОШ «Открытие»

1. Общие положения

1. Настоящее Положение разработано в соответствии с:
   1.1. Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781;
   1.2. Положением о методах и способах защиты информации в информационных системах персональных данных, утвержденным приказом Федеральной службы по техническому и экспортному контролю от 05 февраля 2010 года № 58.
   1.3. Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»
2. Настоящее Положение является развитием комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся у работодателя, посредством планомерных действий по совершенствованию организации труда в МАОУ НОШ «Открытие».

2. Понятие и состав персональных данных

Под персональными данными сотрудников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией. К персональным данным относятся:

- все биографические сведения сотрудника;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- состав семьи;
- размер заработной платы;
- содержание трудового договора;

- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т2) и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкета;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии;
- и т.п.

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

Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который вступил (стал сотрудником) или изъявил желание вступить в трудовые отношения с работодателем.

Субъект персональных данных самостоятельно решает вопрос передачи работодателю своих персональных данных.

Держателем персональных данных является работодатель, которому сотрудник добровольно передает во владение свои персональные данные. Работодатель выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством. Права и обязанности работодателя в трудовых отношениях осуществляются физическим лицом, уполномоченным работодателем. Указанные права и обязанности он может делегировать нижестоящим руководителям – своим заместителям, руководителям структурных подразделений, работа которых требует знания персональных данных работников или связана с обработкой этих данных.

Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

3. Принципы обработки персональных данных

Обработка персональных данных включает в себя их получение, хранение, , передачу, а также распространение, защиту, уничтожение. Получение, хранение, передача или любое другое использование персональных данных сотрудника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества. Все персональные данные сотрудника получаются у него самого. Если персональные данные сотрудника возможно получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие.

Работодатель должен сообщить сотруднику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа сотрудника дать письменное согласие на их получение.

Не допускается получение и обработка персональных данных сотрудника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности.

Пакет анкетно - биографических и характеризующих материалов (далее «Личное дело») сотрудника формируется в «Личное дело» после издания приказа о его приеме на работу. «Личное дело» обязательно содержит личную карточку формы Т2, а также может содержать документы, содержащие персональные данные сотрудника, в порядке, отражающем процесс приема на работу: заявление сотрудника о приеме на работу; анкета; характеристика-рекомендация; результат медицинского обследования на предмет годности к осуществлению трудовых обязанностей; копия приказа о приеме на работу; расписка сотрудника об ознакомлении с документами организации, устанавливающими порядок обработки персональных данных работников, а также об его правах и обязанностях в этой области; расписка сотрудника об ознакомлении его с локальными нормативными актами организации, правилами внутреннего трудового распорядка и т.д.

Все документы хранятся в файлах, файлы содержатся в папках в алфавитном порядке фамилий сотрудников. Анкета является документом «Личного дела», представляющим собой перечень вопросов о биографических данных сотрудника, его образовании, выполняемой работе с начала трудовой деятельности, семейном положении, месте прописки или проживания и т.п. Анкета заполняется сотрудником самостоятельно при оформлении приема на работу. При заполнении анкеты сотрудник должен заполнять все ее графы, на все вопросы давать полные ответы, не допускать исправлений или зачеркивания, прочерков, помарок, в строгом соответствии с записями, которые содержатся в его личных документах. В графах "Состав семьи" перечисляются все члены семьи сотрудника с указанием степени родства (мать, отец, муж, жена, сын, дочь). Указываются фамилия, имя, отчество и дата рождения каждого члена семьи.

При заполнении анкеты и личной карточки Т2 используются следующие документы:

• паспорт;
• трудовая книжка;
• военный билет;
• документы об образовании.

«Личное дело» пополняется на протяжении всей трудовой деятельности сотрудника в данной организации. Изменения, вносимые в карточку Т2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

Сотрудник отдела кадров, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу сотрудника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами.

При обработке персональных данных сотрудников работодатель в лице директора школы вправе определять способы обработки, документирования, хранения и защиты персональных данных сотрудников МАОУ НОШ «Открытие» на базе современных информационных технологий.

Сотрудник обязан:

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

Сотрудник имеет право на:

- полную информацию о своих персональных данных и обработке этих данных;

-свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника. Доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;
-требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия.

4. Доступ к персональным данным

Персональные данные добровольно передаются сотрудником непосредственно держателю этих данных и потребителям внутри МАОУ НОШ «Открытие» исключительно для обработки и использования в работе.

1. Внешний доступ.

К числу массовых потребителей персональных данных вне МАОУ НОШ «Открытие» 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.

2. Внутренний доступ.

Внутри МАОУ НОШ «Открытие» к разряду потребителей персональных данных относятся сотрудники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- все сотрудники отдела кадров;
- все сотрудники бухгалтерии;
- руководители структурных подразделений.

В кадровом секторе хранятся личные карточки сотрудников, работающих в настоящее время. Для этого используются специально оборудованные шкафы или сейфы, которые запираются. Личные карточки располагаются в алфавитном порядке. После увольнения документы по личному составу передаются на хранение.

5. Передача персональных данных

При передаче персональных данных сотрудника работодатель должен соблюдать следующие требования:

1. Передача внешнему потребителю.

- 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.

- При передаче персональных данных сотрудника потребителям (в том числе и в коммерческих целях) за пределы МАОУ НОШ «Открытие» работодатель не должен сообщать эти данные третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника.

- Ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения директора школы и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений.

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

- Сведения передаются в письменной форме.

- По возможности персональные данные обезличиваются.

2. Передача внутреннему потребителю.

- Работодатель вправе разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, перечисленным в п.2 гл.4.

- Потребители персональных данных должны подписать согласие о неразглашении персональных данных сотрудников.

6. Защита персональных данных

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 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.

1. «Внутренняя защита».

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами компании. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудниками требований нормативно – методических документов по защите информации;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только директору школы, и в исключительных случаях, по письменному разрешению директора школы, руководителю структурного подразделения;

- персональные компьютеры, на которых содержатся персональные данные, должны быть защищены паролями доступа.

2. «Внешняя защита».

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 МАОУ НОШ «Открытие», посетители, сотрудники 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.

Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим;
- порядок охраны территории, зданий, помещений;
- требования к защите информации при интервьюировании и собеседованиях.

7. Порядок определения защищаемой информации

Для определения защищаемой информации, а также информационных систем для ее обработки в учреждении создается комиссия.

Определение защищаемой информации проводится по результатам анализа всей имеющейся информации по каждому направлению деятельности учреждения.

Результаты работы комиссии отражаются в актах.

Для планирования, координации и проведения работ по защите информации ограниченного распространения в учреждении назначается ответственный по защите информации.

8. Порядок при проведении работ по созданию ИСПДн

Деятельность по созданию ИСПДн осуществляется в соответствии с требованиями федеральных и краевых нормативных правовых актов, внутренних документов МАОУ НОШ в области защиты информации. Координацию работ по созданию ИСПДн осуществляет ответсвенный по защите персональных данных.

В случае возникновения необходимости создания ИСПДн ответственный по защите информации информирует об этом директора школы для совместного принятия решения о последующем порядке действий.

Предложения о создании ИСПДн выносятся ответственным по защите информации на рассмотрение директору школы.

Ответственный по защите информации приступает к работе по созданию ИСПДн после издания директором МАОУ НОШ «Открытие» приказа о создании комиссии по определениюи классификации информационных систем персональных данных.

9. Порядок разработки, ввода в действие и эксплуатации ИСПДн

Предпроектная стадия.

1. Предпроектное обследование автоматизированных систем (далее - АС) проводится ответственным по защите информации совместно с созданной комиссией по определениюи классификации информационных систем персональных данных, которые участвуют в определении (уточнении):
   1.1. угроз безопасности информации применительно к конкретным условиям функционирования;

1.2. конфигурации, топологии АС и систем связи в целом, а также их отдельных компонентов;
1.3. физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня;
1.4. режима обработки информации в АС в целом и в ее отдельных компонентах;
1.5. средств вычислительной техники и связи, технических и программных средств, предназначенных для обработки защищаемой информации.

2. Класс информационных систем персональных данных устанавливается в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСБ России, ФСТЭК России и Мининформсвязи России от 13 февраля 2008г. № 55/86/20 и оформляется актом.
3. При необходимости разработки технического проекта на ИСПДн ответственным по защите информации совместно с комиссией разрабатывается техническое (частное техническое) задание с учетом установленного класса ИСПДн

Стадия проектирования и создания ИСПДн.

1. На основе требований, определенных при предпроектном обследовании, школой осуществляется закупка сертифицированных по требованиям безопасности технических и программных средств защиты, обработки, передачи и хранения информации.
2. На стадии создания ИСПДн ответственным по защите информации совместно комиссией осуществляются организационные и технические мероприятия по защите информации:
   2.1. размещение и монтаж технических средств и систем обработки конфиденциальной информации;
   2.2. организация охраны кабинетов с установленной ИСПДн в целях исключения несанкционированного доступа к техническим средствам обработки, хранения и передачи информации, нарушения их работоспособности, хищения средств и носителей информации;
   2.3. определение лиц, ответственных за эксплуатацию средств защиты информации;
   2.4. обучение лиц, назначенных ответственными за эксплуатацию ИСПДн, специфике работы с учетом требований по безопасности информации и установленного класса;
   2.5. разработка и реализация разрешительной системы доступа пользователей к обрабатываемой в ИСПДн информации;
   2.6. разработка организационно-распорядительной документации по защите информации в ИСПДн.

Стадия ввода в эксплуатацию ИСПДн.

1. Ответственным по защите информации на стадии ввода в эксплуатацию ИСПДн и СЗИ проводится проверка работоспособности средств защиты информации в комплексе с другими техническими и программными средствами в составе ИСПДн и отработка технологического процесса обработки (передачи) информации.
2. Ввод ИСПДн в эксплуатацию осуществляется после проведения его комплексной проверки (аттестационных испытаний) в реальных условиях эксплуатации в целях оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.
3. ИСПДн вводится в эксплуатацию приказом директора школы.
4. Эксплуатация ИСПДн осуществляется в соответствии с условиями и требованиями, определенными внутренними организационно-распорядительными документами учреждения по защите информации и утвержденным техническим паспортом на ИСПДн.
5. Все изменения в информационных технологиях обработки информации в ИСПДн, составе и размещении технических средств и систем, условиях их эксплуатации,

которые могут повлиять на эффективность мер и средств защиты информации в ИСПДн согласуются с ответственным по защите информации.

6. Для своевременного выявления и предотвращения утечки информации по техническим каналам, исключения несанкционированного доступа и предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности технических средств, проводится периодический контроль состояния защиты информации.
7. Контроль осуществляется ответственным по защите информации (не реже одного раза в полгода) и заключается в оценке:
   7.1. работоспособности применяемых средств защиты информации в соответствии с их эксплутационной документацией;
   7.2. выполнения работниками школы, допущенных к работе на СПДн, своих обязанностей в части обеспечения защиты информации.
8. При выявлении в ходе проведения контроля нарушения правил эксплуатации ИСПДн, технологии обработки защищаемой информации и требований по безопасности информации эксплуатация ИСПДн может быть приостановлена решением директора МАОУ НОШ «Открытие» до момента восстановления требуемого уровня безопасности информации.

10. Ответственность должностных лиц структурных подразделений, занятых в создании и эксплуатации ИСПДн

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

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

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

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско–правовую или уголовную ответственность граждан и юридических лиц.

Ответственность за своевременность подачи информации о необходимости создания ИСПДн для обработки защищаемой информации возлагается на ответственного по защите информации.

Ответственность за качество формирования требований по технической защите конфиденциальной информации при создании ИСПДн, а также за полноту и качество разработки системы защиты информации в его составе возлагается на ответственного по защите информации.

Работники школы, допущенные к работе на СПДн несут ответственность за выполнение требований по безопасности информации, соблюдение технологии обработки защищаемой информации, неизменность условий обработки информации (размещение и/или состав технических средств обработки и защиты информации, состав используемого в ИСПДн программного обеспечения) в соответствии с организационно-технической документацией на эксплуатируемую ИСПДн.

При нарушении требований по безопасности информации на директора школы, на ответственного по защите информации и работников школы, допущенных к работе на СПДн налагается дисциплинарная и административная ответственность в соответствии с действующим законодательством Российской Федерации.