

**Частное общеобразовательное учреждение
Гимназия № 212 «Екатеринбург – Париж»**

СОГЛАСОВАНО
С УПРАВЛЯЮЩИМ СОВЕТОМ
ГИМНАЗИИ,
ПРОТОКОЛ ОТ 20.03. 2015 Г.,
№ 4



УТВЕРЖДАЮ:
ДИРЕКТОР ГИМНАЗИИ

(И.Л. ЯЧМЕНЕВА)

2015 Г.

**ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ**

1. Общие положения

1.1. Настоящее положение устанавливает порядок приема, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения, учета документов, содержащих сведения, отнесенные к персональным данным работников Частного общеобразовательного учреждения Гимназия № 212 «Екатеринбург - Париж» с использованием средств автоматизации или без использования таких средств.

1.2. Основные понятия:

1) персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), являющемуся работником Частного общеобразовательного учреждения Гимназия № 212 «Екатеринбург - Париж», в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

2) обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

3) 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;

4) использование персональных данных — действия (операции) с персональными данными, совершаемые работодателем в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работника или других лиц, либо иным образом затрагивающих права и свободы работника или других лиц;

5) блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

6) уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

7) обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

8) информационная система персональных данных — система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также

информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

9) конфиденциальность персональных данных — обязательное для соблюдения работодателем или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия работника или наличия иного законного основания;

10) общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами РФ не распространяется требование соблюдения конфиденциальности.

11) работники — лица, имеющие трудовые отношения с Частным общеобразовательным учреждением Гимназия № 212 «Екатеринбург - Париж», либо кандидаты на вакантную должность, вступившие с организацией в отношения по поводу приема на работу.

12) оператор — лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

1.3. Положение о защите персональных данных и изменения к нему утверждаются генеральным директором. Все работники организации должны быть ознакомлены под роспись с данным положением и изменениями к нему.

2. Понятие и состав персональных данных

Под персональными данными работников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, его родственников, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность и личность его родственников. Персональные данные работника являются конфиденциальной информацией. К персональным данным относятся следующие сведения и документы:

- все биографические сведения о работнике;
- образование;
- специальность,
- занимаемая должность;
- наличие судимостей;
- место жительства (пребывания);
- домашний телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора;
- содержание налоговых деклараций;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т-2) и трудовые книжки сотрудников;
- приказы и 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;
- анкеты, заполняемые работниками;
- копии документов об образовании;
- результаты медицинского обследования.

3. Принципы обработки персональных данных

3.1. Обработка персональных данных должна осуществляться на основе принципов:

- 1) законности целей и способов обработки персональных данных и добросовестности;
- 2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям работодателя;
- 3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- 4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- 5) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

3.2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3.3. Работник является собственником своих персональных данных и самостоятельно решает вопрос передачи работодателю своих персональных данных.

3.4. Держателем персональных данных является работодатель, которому работник добровольно передает во владение свои персональные данные. Работодатель выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

3.5. Право доступа к персональным данным работника имеют следующие лица, уполномоченные работодателем:

1. Директор гимназии;
2. Первый заместитель директора;
3. Заместитель директора по учебной работе;
4. Заместитель директора по воспитательной работе;
5. Заместитель директора по административно- хозяйственной работе;
6. Главный бухгалтер;
7. Специалист по кадрам;
8. Секретарь - делопроизводитель;
9. Врач – педиатр;
10. Руководитель библиотечно – информационного центра.

3.6. 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.

3.7. Получение, хранение, комбинирование, передача или любое другое использование персональных данных работника 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 работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

4. Получение, обработка и хранение персональных данных

4.1. Работодатель получает сведения о персональных данных работника из следующих документов:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка;
- страховое свидетельство государственного пенсионного страхования;

- документы воинского учета;
- документ об образовании, о квалификации или наличии специальных знаний;
- анкета, заполняемая работником при приеме на работу и в иные документы и сведения, предоставляемые работником при приеме на работу и в процессе работы.

4.2. Все персональные данные работника получаются у него самого.

Сотрудник, ответственный за документационное обеспечение кадровой деятельности, принимает от работника документы, проверяет их полноту и правильность указываемых сведений.

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 источникам и способам получения персональных данных и последствиях отказа работника дать письменное согласие на их получение.

4.3. Условием обработки персональных данных работника является его согласие. Работник принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе, за исключением случаев, предусмотренных п. 4.4 настоящего положения. Согласие на обработку персональных данных может быть отозвано работником.

4.4. Согласие работника на обработку его персональных данных не требуется в следующих случаях:

- 1) обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

- 2) обработка персональных данных осуществляется в целях исполнения трудового или иного договора или соглашения между работником и работодателем;
- 3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- 4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия при данных обстоятельствах невозможно;

- 5) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов пользователей услугами связи;
- 6) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами.

4.5. Письменное согласие работника на обработку его персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес работника, номер основного документа и удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
 - наименование и адрес работодателя;
 - цель обработки персональных данных;
 - перечень персональных данных, на обработку которых дается согласие работника;
 - перечень действий с персональными данными, на совершение которых дается согласие; общее описание используемых работодателем способов обработки персональных данных;
 - срок, в течение которого действует согласие, а также порядок его отзыва.
- Для обработки персональных данных, содержащихся в письменной форме субъекта на обработку его персональных данных, дополнительное согласие не требуется. В случае смерти работника согласие на обработку его персональных данных при необходимости дает в письменной форме один из его наследников, если такое согласие не было дано работником при его жизни.

4.6. Не допускается получение и обработка персональных данных работника о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных п. 4.7 настоящего положения.

4.7. Обработка указанных в п. 4.6. настоящего положения персональных данных допускается в случаях, если:

- 1) работник дал согласие в письменной форме на обработку своих персональных данных;
- 2) персональные данные являются общедоступными;
- 3) 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 в данный момент невозможно;
- 4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- 5) обработка персональных данных необходима в связи с осуществлением правосудия;
- 6) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

4.8. Обработка персональных данных о судимости может осуществляться в соответствии с федеральными законами.

4.9. Обработка персональных данных, перечисленных в п. 4.6. настоящего положения должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

4.10. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия работника в письменной форме, за исключением случаев, предусмотренных п. 4.11 настоящего положения.

4.11. Обработка биометрических персональных данных может осуществляться без согласия работника в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, уголовно-исполнительным законодательством Российской Федерации.

4.12. Документы, содержащие персональные данные работника составляют его личное дело. Личное дело в обязательном порядке включает личную карточку формы Т-2. Личное дело хранится уполномоченным лицом на бумажных носителях, а помимо этого может храниться в виде электронных документов. Личное дело пополняется на протяжении всей трудовой деятельности работника. Письменные доказательства получения работодателем согласия работника на обработку его персональных данных хранятся в личном деле работника.

4.13. При обработке персональных данных работников генеральный директор вправе определять способы обработки, документирования, хранения и защиты персональных данных на базе современных информационных технологий.

5. Конфиденциальность персональных данных

5.1. Работодателем и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, предусмотренных п. 5.2 настоящего положения.

5.2. Обеспечение конфиденциальности персональных данных не требуется:

- 1) в случае обезличивания персональных данных;
- 2) в отношении общедоступных персональных данных.

6. Общедоступные источники персональных данных

6.1. В целях информационного обеспечения деятельности структурных подразделений и сотрудников Частного общеобразовательного учреждения Гимназия № 212 «Екатеринбург - Париж» внутри организации могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги и др.). В общедоступные источники персональных данных с письменного согласия работника могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные работником.

6.2. Сведения о работнике могут быть в любое время исключены из общедоступных источников персональных данных по его требованию либо по решению руководителя организации, либо суда или иных уполномоченных государственных органов.

7. Права и обязанности сторон в области защиты персональных данных

7.1. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен трудовым законодательством, включая сведения об образовании, специальных знаниях, стаже работы, отношении к воинской обязанности, гражданстве, месте жительства и др.
- своевременно сообщать работодателю об изменении своих персональных данных.

7.2. Работник имеет право:

- получать полную информацию о своих персональных данных;
- иметь свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных действующим законодательством;
- иметь доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;
- получать сведения об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему работнику;
- требовать от работодателя уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- получать информацию, касающуюся обработки его персональных данных, в том числе содержащую: подтверждение факта обработки персональных данных оператором, а также цель такой обработки; способы обработки персональных данных, применяемые оператором; 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 него может повлечь за собой обработка его персональных данных;
- 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.

Сведения о наличии персональных данных должны быть предоставлены работнику в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных. Доступ к своим персональным данным предоставляется работнику или его законному представителю оператором при личном обращении либо при получении запроса. Запрос должен содержать номер основного документа, удостоверяющего личность работника или его законного представителя,

сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись работника или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

7.3. Право работника на доступ к своим персональным данным ограничивается в случае, если:

- 1) обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- 2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
- 3) предоставление персональных данных нарушает конституционные права и свободы других лиц.

7.4. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении работника или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных п. 7.5 настоящего положения.

7.5. Решение, порождающее юридические последствия в отношении работника или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия работника в письменной форме или в случаях, предусмотренных федеральными законами.

7.6. Работодатель обязан разъяснить работнику порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов. Работодатель обязан рассмотреть возражение работника в течение семи рабочих дней со дня его получения и уведомить его о результатах рассмотрения такого возражения.

7.7. Если обязанность предоставления персональных данных работником установлена федеральным законом, работодатель обязан разъяснить работнику юридические последствия отказа предоставить свои персональные данные.

7.8. Если персональные данные были получены не от работника, за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если персональные данные являются общедоступными, работодатель до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:

- 1) наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- 2) цель обработки персональных данных и ее правовое основание;
- 3) предполагаемые пользователи персональных данных;
- 4) права работника в области защиты персональных данных.

7.9. Работодатель обязан безвозмездно предоставить работнику возможность ознакомления с персональными данными, относящимися к соответствующему работнику, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлению работником сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах работодатель обязан уведомить работника и третьих лиц, которым персональные данные этого

работника были переданы.

7.10. В случае выявления недостоверных персональных данных или неправомерных действий с ними работодатель обязан осуществить блокирование персональных данных, относящихся к соответствующему работнику, с момента получения такой информации на период проверки. В случае подтверждения факта недостоверности персональных данных работодатель на основании соответствующих документов обязан уточнить персональные данные и снять их блокирование.

В случае выявления неправомерных действий с персональными данными работодатель в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений работодатель в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных работодатель обязан уведомить работника.

7.11. В случае достижения цели обработки персональных данных работодатель обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом работника.

7.12. В случае отзыва работником согласия на обработку своих персональных данных работодатель обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением сторон. Об уничтожении персональных данных работодатель обязан уведомить работника.

8. Доступ к персональным данным и их передача.

8.1. Внутренний доступ к персональным данным работника имеют сотрудники структурных подразделений организации, которым эти данные необходимы для выполнения должностных обязанностей:

Директор гимназии;
Первый заместитель директора;
Заместитель директора по учебной работе;
Заместитель директора по воспитательной работе;
Заместитель директора по административно- хозяйственной работе;
Главный бухгалтер;
Специалист по кадрам;
Секретарь - делопроизводитель;
Врач – педиатр;
Руководитель библиотечно.- информационного центра.

Для хранения персональных данных используются специально оборудованные шкафы или сейфы, которые запираются на ключ.

После увольнения работника документы, содержащие его персональные данные, хранятся в организации в течение сроков, установленных архивным законодательством.

8.2. Внешний доступ со стороны третьих лиц к персональным данным работника осуществляется только с письменного согласия работника, за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью работника или других лиц, и иных случаев, установленных законодательством.

8.3. Работодатель обязан сообщать персональные данные работника по надлежаще оформленным запросам суда, прокуратуры, правоохранительных органов.

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

8.4.1. 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 работника потребителям в коммерческих целях за пределы организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника.

Ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения генерального директора 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 и должны иметь гриф конфиденциальности.

8.4.2. Передача внутреннему потребителю:

Работодатель вправе разрешать доступ к персональным данным работников только специально уполномоченным лицам.

Потребители персональных данных должны подписать обязательство о неразглашении персональных данных работников.

9. Безопасность персональных данных

9.1. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

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

9.3. Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе управленческой и производственной деятельности организации.

9.3.1. «Внутренняя защита»

Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителем и специалистами компании. Для защиты персональных данных сотрудников работодатель обязан соблюдать следующие правила:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей персональные данные;
- 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 персональных данных;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;

- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты сведений при работе с конфиденциальными документами;
- личные дела работников не могут выдаваться на рабочие места,
- персональные компьютеры, на которых содержатся персональные данные, должны быть защищены паролями доступа.

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

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

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

Нарушение установленного законом порядка сбора, хранения, использования или распространения персональных данных влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.

кор.  (Александров С.А.)