предназначена для разграничения полномочий между руководителями и специалистами организации;

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

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между персоналом;
- рациональное размещение рабочих мест персонала, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание 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;
- 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 только генеральному директору работниками отдела кадров и в исключительных случаях, по письменному разрешению генерального директора, руководителю структурного подразделения (например, при подготовке материалов для аттестации работников);

5.5.3. Для обеспечения внутренней защиты персональных данных при работе с базами данных необходимо соблюдать ряд мер:

- возможность использования базы данных и доступ к ее ресурсам должны иметь только зарегистрированные пользователи, согласно Регламенту управления пользователями в домене и Регламенту управления пользователями в 1С Предприятие 8;
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (Информационная Система Персональных Данных) (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей);
- защита от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;

5.5.4. Защита персональных данных на электронных носителях.

Все папки, содержащие персональные данные, должны быть защищены паролем в соответствии с Парольной политикой, действующей в Обществе.

5.6. Внешняя защита.

5.6.1. 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.;

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Общества, посетители, работники других