- ответственность за разглашение конфиденциальной информации и утрату документов, содержащих конфиденциальную информацию.

1.8. Обязанности по конфиденциальному делопроизводству возлагаются на специалиста по обслуживанию вычислительной техники (в части обеспечения работоспособности электронной системы делопроизводства).

1.9. Конфиденциальная информация должны находиться преимущественно в электронном виде и быть защищена электронными средствами защиты.

1.10. Входящие конфиденциальные бумажные документы переводятся в электронный вид, дальнейшая работа с данными документами происходит работниками в электронном виде.

1.11. Работа работников с конфиденциальными бумажными документами допускается в виде исключения с разрешения директора в случае невозможности или нецелесообразности перевода документа в электронный вид.

1.12. После перевода конфиденциального входящего бумажного документа в электронный вид, данный документ, по решению директора уничтожается или, после отработки, определяется в соответствующее дело (архив).

1.13. Обмен конфиденциальными документами внутри ООО осуществляется, преимущественно, в электронном виде с использованием средств электронной защиты.

1.14. Порядок работы с электронными конфиденциальными документами определен в части 2 данной Инструкции.

1.15. Определение вида исходящего конфиденциального документа (электронного или бумажного) возлагается на исполнителя по согласованию с директором.

1.16. Ответственность за организацию работы с конфиденциальной информацией, разработку и осуществление необходимых мер по сохранности конфиденциальной информации возлагается на соответствующих должностных лиц.

2. Порядок работы с конфиденциальной информацией, представленной в электронном виде

2.1. Хранение, работа и архивирование любых электронных конфиденциальных документов (файлов) должно осуществляться с учётом требования ограничения несанкционированного доступа к ним третьих лиц способами, оговоренными настоящим разделом данной Инструкции.

2.2. Все персональные компьютеры, установленные на рабочих местах работников, подключены к защищены.

2.3. Каждый персональный компьютер оснащён стандартным набором программных средств, принятых для эксплуатации. Любые изменения в оснащении персонального компьютера, подключённых к сети, должны быть санкционированы, осуществлены ответственными специалистами.

2.4. Вся конфиденциальная информация, имеющаяся в распоряжении работника, должна храниться и обрабатываться на корпоративном файл-сервере.

2.5. Первичный допуск работника к работе на персональном компьютере, включенного в сеть осуществляется специалистом по обслуживанию вычислительной техники по указанию руководства и включает в себя:

- ознакомление работника с настоящей Инструкцией под роспись;
- инструктаж по порядку работы с программными средствами, принятыми для эксплуатации;
- получение сотрудником персонального пароля;
- получение адреса персонального почтового ящика почты.

2.6. Работник, допущенный к работе с персональным компьютером, получает доступ:

- к персональному разделу на корпоративном файл-сервере («Личная» папка) для хранения и обработки электронных конфиденциальных документов (файлов) с предоставленной в его распоряжение для выполнения поставленных перед ним задач;
- к персональному почтовому ящику корпоративной почты.

2.7. Все электронные конфиденциальные документы (файлы), должны храниться на корпоративном сервере одним из возможных способов:

- в личной папке работника в защищённом на личном ключе виде;
- в личной папке работника в защищённом на личном плюс один или несколько открытых ключей уполномоченных руководства сотрудников виде - в случае необходимости и по указанию руководства.

2.8. Все новые электронные конфиденциальные документы (файлы) должны создаваться только на файл-сервере в личной папке работника.