1. *Храните важную информацию на двух или более ресурсах. При этом можно пользоваться бэкапом (автоматическим копированием данных, например, с жесткого диска в облачное хранилище);*
2. *Обеспечьте безопасность резервных копий данных – зашифруйте жесткие диски или другие устройства резервного копирования. Следует убедиться, что на новом месте файл открывается без ошибок, при необходимости сохранить заново и опять проверить;*
3. *Если вы используете облако, то важно быть уверенным, что данные не украдут. Используйте только надежные службы облачного хранилища, которые без ограничений используются на территории Российской Федерации;*
4. *Убедитесь, что все подключенные к облаку учетные записи защищены надежными паролями.* *Установите и применяйте правило ограничения параметров общего доступа в облаке;*
5. *Если вы используете для хранения жесткий диск, то необходимо установить и регулярно обновлять антивирусную программу. Многие компьютерные вирусы направлены на незаметное воровство информации, однако они могут и целенаправленно повреждать программы и документы;*
6. *При использовании внешних носителей, помните: перед тем как вытащить устройство из разъема, нужно нажать «Извлечь» в меню, вызываемом правой кнопкой мыши. По этой команде ОС Windows убеждается, что информация сохранена полностью.;*
7. *Используйте качественные носители, они прослужат дольше. Выбирайте флэш-накопители с защитным колпачком. В этом случае разъем защищен от механических повреждений, пыли и влаги;*

*Берегите и защищайте свои электронные данные!*



***Памятка для пользователей о том, где безопасно хранить электронные данные***

