|  |  |
| --- | --- |
|  |  |

**Инструкция по обращению с ЭЦП**

1. Проверка целостности ПО СКЗИ, системного, сетевого и прикладного ПО, в среде которого работают СКЗИ, должна выполняться пользователем после загрузки операционной системы при помощи ПО контроля целостности входящего в состав ПО СКЗИ.

2. При эксплуатации СКЗИ не допускается:

- подключать к ПЭВМ дополнительные устройства и соединители без соответствующего предписания на возможность их совместного использования;

- работать на компьютере, если во время его начальной загрузки не проходит встроенный тест, предусмотренный в ПЭВМ;

- оставлять без контроля вычислительные средства, входящие в состав СКЗИ, при включенном питании и загруженном программном обеспечении СКЗИ. При кратковременном перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана производится с использованием пароля доступа;

- вносить какие-либо изменения в программное обеспечение;

- несанкционированно устанавливать создавать и выполнять на ПЭВМ посторонние программы;

- осуществлять несанкционированное вскрытие системных блоков ПЭВМ.

3. Ключевые носители являются основным элементом, обеспечивающим стойкость конфиденциальной связи, поэтому при обращении с ключами Пользователь должен принять все необходимые меры, направленные на исключение несанкционированного доступа к ним.

4. Пользователь обязан:

- хранить ключевые носители в опечатываемом сейфе;

- не оставлять ключевые носители без присмотра в ПЭВМ или на столе;

- получать/сдавать рабочие ключевые носители под роспись с указанием в журнале времени получения и сдачи;

- обращаться с письменным заявлением к Оператору системы для восстановления ключевых носителей с резервных копий, с указанием причин, повлекших необходимость восстановления.

5. Хранение конфиденциальных документов, носителей ключевой информации, нормативной и эксплуатационной документации разрешается только в металлических шкафах (хранилищах сейфах). При вынужденных перерывах в работе ключевые носители и другие конфиденциальные документы должны быть помещены в сейф, а сейф опечатан личной печатью.

6. Допускается хранение носителей шифровальных ключей в одном хранилище с другими документами в условиях, исключающих их непреднамеренное уничтожение или иное применение, не предусмотренное правилами пользования СКЗИ.

7. Для защиты ключевой информации от механических, электромагнитных и других факторов воздействия, приводящих к разрушению информации, либо ее искажению, целесообразно хранить дискеты в футлярах из экранирующего материала.

8. В случае отсутствия у Пользователя индивидуального хранилища, носители шифровальных ключей по окончании рабочего дня должны сдаваться им лицу, ответственному за их хранение.

9. При работе с ключевыми носителями запрещается:

- снимать несанкционированные копии с шифровальных ключей;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам к ним не допущенным;

- выводить секретные ключи на дисплей принтер или другие внешние устройства отображения информации;

- вставлять ключевой носитель в USB гнездо ПЭВМ (или другое устройство считывания) в режимах, не предусмотренных штатным режимом, а также в USB гнездо других ПЭВМ;

- записывать на ключевой носитель постороннюю информацию.

10. После плановой смены ключей или компрометации ключей пользователи СКЗИ уничтожают выведенные из действия секретные ключи шифрования и ЭЦП со всех магнитных носителей не позднее чем через одни сутки после момента вывода ключей из действия.

11. Об уничтожении ключей делается соответствующая запись в Журнале учета ключевых документов.

|  |  |
| --- | --- |
|  |  |