Памятка пользователю СКЗИ

Средства криптографической защиты информации (СКЗИ)

Электронная подпись (ЭП) - это **информация** в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая ***используется для определения лица***, подписывающего информацию.	**Сертификат ключа проверки электронной подписи** - электронный **документ** или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и ***подтверждающий принадлежность ключа проверки*** электронной подписи ***владельцу сертификата ключа*** проверки электронной подписи.
Существует три вида ЭП: 1.**Простая**; 2.**Неквалифицированная**; 3.**Квалифицированная** (удостоверяющими центрами ***ФНС России***).	**Ключ электронной подписи** - уникальная последовательность символов, предназначенная для создания электронной подписи; **Ключ проверки электронной подписи** - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.
Контроль за соблюдением правил пользования СКЗИ и условий их использования осуществляется: ***- ФСБ России;*** ***- обладателем защищаемой информации;*** ***- пользователем защищаемой информации.***	В соответствии с приказом ФАПСИ № 152 от 13.06.2001 к работе с СКЗИ пользователи допускаются***только после соответствующего обучения***.

СЛЕДУЕТ

Корпусы системных блоков, находящихся в эксплуатации, опечатаны специальными стикерами. Регулярный **контроль целостностистикеров**должен осуществляться ***пользователями*** данных рабочих мест.	Ключевые носители необходимо хранить в опечатываемом **сейфе**, либо в опечатываемом **пенале (колбе)**.
При возникшем подозрении в ***компрометации*** ключевых документов или передававшейся с их использованием информации, необходимо **сообщить в УЦ ФНС России**.	По окончании рабочего дня помещение с СКЗИ должны быть **закрыты и сданы под охрану**.

ЗАПРЕЩАЕТСЯ

- Оставлять свое рабочее место без присмотра во время работы с ключами электронной подписи;
- Хранить свои реквизиты доступа (пароли, PIN-коды) на бумажных носителях под клавиатурой, на столе, в незапираемом ящике или мониторе компьютера;
- Передавать носители ЭП третьим лицам, не прошедшим соответствующее обучение и не имеющим доверенности на использование данной ЭП;
- Продолжать работу на АРМ, в случае обнаружения на нем вредоносного программного обеспечения.