Приложение №4
к приказу по учреждению
№83 от 30.03.2022 г.

ИНСТРУКЦИЯ
по эксплуатации средств защиты информации в АУК «ДК «Нефтяник» города Радужный

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет порядок учета, хранения и использования средств защиты информации, а также порядок их изготовления, уничтожения и действий сотрудников АУК «ДК «Нефтяник» города Радужный (далее Учреждение) при компрометации, или поломке, в целях обеспечения безопасности эксплуатации средств защиты информации.

1.2. Все действия работы со средствами защиты информации осуществляются в соответствии с эксплуатационной документацией.

1.3. Учреждение использует сертифицированные ФСБ России средства защиты информации, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.

1.4. Для организации и обеспечения работ по техническому обслуживанию средств защиты информации, приказом учреждения назначается администратор безопасности информационных систем.

1.5. Администратор безопасности информационных систем осуществляет:

− поэкземплярный учет, эксплуатационной и технической документации к ним;

− контроль над соблюдением условий использования средств защиты информации в соответствии с эксплуатационной и технической документацией и настоящей Инструкцией;

− расследование и составление заключений по фактам нарушения условий использования средств защиты информации, которые могут привести к снижению требуемого уровня безопасности информации;

− разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

1.6. Пользователь средств защиты информации обязан:

− не разглашать конфиденциальную информацию, к которой допущен, границы ее защиты, в том числе сведения о криптографических ключах;

− соблюдать требования к обеспечению безопасности конфиденциальной информации при использовании средств защиты информации;

− сдать средства защиты информации, эксплуатационную и техническую документацию к ним, криптографические ключи в

соответствии с порядком, установленным настоящей Инструкцией, при прекращении использования средств защиты информации;

– незамедлительно уведомлять администратора безопасности информационных систем о фактах утраты или недостачи СКЗИ, криптографических ключей, ключей от помещений, ключевых носителей хранилищ и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

1.7. Обучение пользователей правилам работы со средствами защиты информации осуществляет администратор безопасности информационных систем. Администратор безопасности информационных систем должен иметь соответствующий документ о квалификации в области эксплуатации. Непосредственно к работе со средствами защиты информации пользователи допускаются после обучения.

1.8. Текущий контроль, обеспечения функционирования и безопасности средств защиты информации возлагается на администратора безопасности информационных систем.

1.9. Администратор безопасности информационных систем и пользователи должны быть ознакомлены с настоящей Инструкцией под роспись.

2. УЧЕТ И ХРАНЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Средства защиты информации, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.

2.2. Установка средств криптографической защиты информации, ввод в эксплуатацию и закрепление их за ответственными лицами оформляется Актом установки средств криптографической защиты информации, ввода в эксплуатацию и закрепления их за ответственными лицами.

2.3. Дистрибутивы средств защиты информации на носителях, эксплуатационная и техническая документация к ним, инструкции хранятся у администратора безопасности информационных систем. Криптографические ключи, электронно-цифровая подпись и ключевые носители хранятся у пользователей средств защиты информации. Хранение осуществляется в закрываемых на замок металлических хранилищах пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение или в опечатанном пенале (тубусе).

2.4. Пользователи средств защиты информации могут осуществлять хранение рабочих и резервных криптографических ключей, ЭЦП и ключевых носителей предназначенных для применения в случае неработоспособности рабочих криптографических ключей, ЭЦП и ключевых носителей. Резервные криптографические ключи, ЭЦП и ключевые носители могут также находится на хранении у ответственного за эксплуатацию.

2.5. Ключевые носители совместно с журналом должны храниться ответственным за обработку и безопасность ПДн в сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и журнал совместно с другими документами, при этом ключевые носители и журнал должны быть помещены в отдельную папку.

2.6. При необходимости криптографические ключи, ЭЦП и ключевые носители сдаются на временное хранение ответственному за эксплуатацию.

3. ИСПОЛЬЗОВАНИЕ СКЗИ И КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ, ЭЦП И КЛЮЧЕВЫХ НОСИТЕЛЕЙ

3.1. Средства защиты информации используются для обеспечения конфиденциальности и целостности электронных документов и т.п.

3.2. При выявлении сбоев или отказов пользователь обязан сообщить о факте их возникновения администратору безопасности информационных систем.

3.3. Пользователю запрещается:

- осуществлять несанкционированное копирование средств защиты информации; использовать ключевые носители и ЭЦП для работы на других рабочих местах для шифрования и подписи электронных документов;
- разглашать содержимое средств защиты информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;
- вставлять носители криптографических ключей, ЭЦП и ключевые носители в устройства считывания в режимах, не предусмотренных штатным режимом работы средств защиты информации, а также в устройства считывания других ПЭВМ;
- записывать на носители с криптографическими ключами, ЭЦП и ключевыми носителями постороннюю информацию;
- подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные в штатной комплектации;
- работать на ПЭВМ, если во время ее начальной загрузки не проходят встроенные тесты, предусмотренные в ПЭВМ;
- вносить какие-либо изменения в программное обеспечение средств защиты информации.

4. ИЗГОТОВЛЕНИЕ И ПЛАНОВАЯ СМЕНА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И ЭЦП

4.1. Криптографические ключи и ЭЦП изготавливаются на отчуждаемый ключевой носитель в соответствии с эксплуатационно-технической документацией на средства защиты информации и требованиями безопасности, установленными настоящей Инструкцией.

4.2. Переход на новые криптографические ключи пользователь выполняет самостоятельно в соответствии с эксплуатационной документацией на средства защиты информации. Переход на новые криптографические ключи осуществляется в сроки, указанные в сертификате ключа подписи.

4.3. При замене криптографических ключей используют программное обеспечение в соответствии с документами по эксплуатации. Пользователь самостоятельно обязан обновить сертификат ключ подписи. Обновление справочников сертификатов ключей производится путем добавления новых сертификатов ключей подписи из файлов, содержащих сертификаты ключей подписи, предоставляемых ответственным за эксплуатацию. Обновление справочников сертификатов ключей подписи осуществляется в соответствии с эксплуатационной документацией на средства защиты информации.

5. ДЕЙСТВИЯ ПРИ КОМПРОМЕТАЦИИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И ЭЦП

5.1. К обстоятельствам, указывающим на возможную компрометацию криптографических ключей и ЭЦП, но не ограничивающим их, относятся следующие:

- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами или ЭЦП;
- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами или ЭЦП с последующим их обнаружением;
- увольнение сотрудников, имевших доступ к рабочим и/или резервным криптографическим ключам или ЭЦП;
- возникновение подозрений относительно утечки информации или ее искажения;
- нарушение целостности печатей на сейфах (металлических шкафах) с ключевыми носителями с рабочими и/или резервными криптографическими ключами, ЭЦП, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них ключевых носителей с рабочими и/или резервными криптографическими ключами, ЭЦП;
- временный доступ посторонних лиц к ключевым носителям, а также другие события, при которых достоверно не известно, что произошло с ключевыми носителями.

5.2. В случае возникновения обстоятельств, указанных в п. 5.1 настоящей Инструкции, пользователь обязан незамедлительно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей.

5.3. Использование средства защиты информации может быть возобновлено только после ввода в действие другого криптографического ключа, ЭЦП взамен скомпрометированного.

6. УНИЧТОЖЕНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ, ЭЦП И КЛЮЧЕВЫХ НОСИТЕЛЕЙ

6.1.. Неиспользованные или выведенные из действия криптографические ключи, ЭЦП и ключевые носители подлежат уничтожению.

6.2. Уничтожение криптографических ключей, ЭЦП на ключевых носителях производится администратором безопасности информационных систем.

6.3. Криптографические ключи, ЭЦП находящиеся на ключевых носителях, уничтожаются путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на средства защиты информации.

6.4. При уничтожении криптографических ключей, ЭЦП находящихся на ключевых носителях, необходимо:

- установить наличие оригинала и количество копий криптографических ключей, ЭЦП;
- проверить внешним осмотром целостность каждого ключевого носителя;
- установить наличие на оригинале и всех копиях ключевых носителей реквизитов путем сверки с записями в журнале поэкземплярного учета;
- убедиться, что криптографические ключи, ЭЦП находящиеся на ключевых носителях, действительно подлежат уничтожению;
- произвести уничтожение ключевой информации на оригинале и на всех копиях носителей.

6.5. В журнале поэкземплярного учета администратором безопасности информационных систем производится отметка об уничтожении криптографических ключей.

Лист ознакомления с Инструкцией
по эксплуатации средств защиты информации
в АУК «ДУ «Нефтяник» города Радужный

№ п/п	Фамилия, имя, отчество работника	Дата ознакомления с Инструкцией	Подпись работника