УТВЕРЖДАЮ
Директор ОБПОУ «КГТТС»
_____ Е.Н.Брежнев
Приказ № 455/о от 30.12.2016

ИНСТРУКЦИЯ
по восстановлению связи в случае компрометации действующих ключей к СКЗИ ОБПОУ «КГТТС»

1.1 Под компрометацией индивидуального ключа понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность конфиденциальной информации. К событиям, связанным с компрометацией действующих криптографических ключей, относится:

– утрата (в том числе хищение) ключевых дискет (флэш – накопителей) с последующим их обнаружением;

– увольнение работников, имевших доступ к ключевой информации;

– передача ключевой информации по линии связи в открытом виде (если это не предусмотрено правилами пользования);

– нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;

– возникновение подозрений на утечку информации или ее искажение;

– не расшифровывание входящих или исходящих сообщений;

– отрицательный результат при проверке электронной цифровой подписи документа;

– нарушение целостности упаковки ключевых дискет (флэш - накопителей) и (или) печати на сейфе, где хранились ключевые дискеты (флэш - накопители);

– несанкционированное копирование ключевых дискет (флэш - накопителей);

– случаи, когда нельзя достоверно установить, что произошло с магнитными носителями, содержащими ключевую информацию (в том числе, случаи, когда магнитный носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате злоумышленных действий).

Первые пять событий должны трактоваться как безусловная компрометация действующих ключей; при наличии остальных событий требуется специальное расследование в каждом конкретном случае.

1.2 При наступлении любого из перечисленных выше событий пользователь должен немедленно прекратить связь с другими пользователями и сообщить о факте компрометации (или предполагаемом факте компрометации) Администратору безопасности.

1.3 Расследование факта компрометации (или предполагаемой компрометации) должно проводиться на месте происшествия специально назначаемой комиссией во главе с Администратором безопасности.

Результатом рассмотрения является квалификация или не квалификация данного события как компрометация действующих ключей.

При установлении факта компрометации действующих ключей, скомпрометированные секретные ключи шифрования и подписи уничтожаются.

1.4 Для восстановления конфиденциальной связи после компрометации ключей пользователь обращается к Администратору безопасности с целью регистрации вновь изготовленных (или резервных) ключей. Регистрация новых ключей шифрования и электронной подписи осуществляется тем же порядком, как и при плановой смене ключей.