	Министерство образования и молодежной политики Свердловской области
	Государственное автономное профессиональное образовательное учреждение Свердловской области
	«Екатеринбургский техникум химического машиностроения»
	Инструкция по восстановлению связи в ИС

Рассмотрено
на заседании Совета
ГАПОУ СО «ЕТХМ»
Протокол № 3,
от « 31 » января 2020 г.

УТВЕРЖДЕНО
Приказом директора
ГАПОУ СО «ЕТХМ»
№ 24 - о/д от « 03 » февраля 2020 г.

ИНСТРУКЦИЯ
ПО ВОССТАНОВЛЕНИЮ СВЯЗИ В СЛУЧАЕ КОМПРОМЕТАЦИИ ДЕЙСТВУЮЩИХ КЛЮЧЕЙ К КРИПТОСРЕДСТВАМ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГОСУДАРСТВЕННОГО АВТОНОМНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ «ЕКАТЕРИНБУРГСКИЙ ТЕХНИКУМ ХИМИЧЕСКОГО МАШИНОСТРОЕНИЯ»

Екатеринбург
2020 г.

Введено в действие с 03.02.2020 г.

1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

1) утрата (хищение) носителей ключевой информации (далее - НКИ), в том числе - с последующим их обнаружением;

2) увольнение (переназначение) работников, имевших доступ к ключевой информации;

3) передача секретных ключей по линии связи в открытом виде;

4) нарушение правил хранения криптоключей;

5) вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

6) отрицательный результат при проверке наложенной электронной подписи;

7) несанкционированное или безучётное копирование ключевой информации;

8) все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

2. События 1-5 п.1 должны трактоваться как безусловная компрометация действующих ключей. Остальные события требуют специального расследования в каждом конкретном случае.

3. При наступлении любого из перечисленных выше событий владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) Ответственному за эксплуатацию криптографических средств защиты информации лично, по телефону, электронной почте или другим доступным способом. В любом случае владелец ключа обязан убедиться, что его сообщение получено и прочтено адресатом.

4. При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей в течение трёх рабочих дней.

5. Для восстановления конфиденциальной связи после компрометации действующих ключей Пользователь получает новые ключи в течение рабочего дня на основании предоставленного Заявления.

Разработал:
Заместитель директора по УПР Н.В. Катанэ