ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Владелец: **Латиева Эльвира Измаиловна**

Приложение
к приказу муниципального
общеобразовательного бюджетного
учреждения гимназии № 1 г. Сочи
имени Филатовой Риммы Алексеевны
от " 01" сентября 2021 года № 390

ИНСТРУКЦИЯ
о порядке оповещения пользователей средств криптографической защиты информации в муниципальном общеобразовательном бюджетном учреждении гимназии № 1 г. Сочи имени Филатовой Риммы Алексеевны о предполагаемой компрометации криптоключей и их замене

Под компрометацией криптоключей в настоящей инструкции понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным процессам и (или) посторонним лицам.

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

1) потеря ключевых носителей с рабочими и (или) резервными криптографическими ключами;

2) потеря ключевых носителей с рабочими и (или) резервными криптографическими ключами с последующим их обнаружением;

3) случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника);

4) временный доступ посторонних лиц к ключевым носителям;

5) увольнение работников, имевших доступ к рабочим и (или) резервным криптографическим ключам;

6) возникновение подозрений относительно утечки информации или её искажения;

7) нарушение целостности печатей на сейфах (металлических шкафах)/хранилищах с ключевыми носителями с рабочими и (или) резервными криптографическими ключами, если используется процедура опечатывания сейфов/хранилищ;

8) утрата ключей от сейфов/хранилищ в момент нахождения в них ключевых носителей с рабочими и (или) резервными криптографическими ключами;

9) другие события утери доверия к ключевой документации.

2. В случае возникновения обстоятельств, указанных в пункте 1 настоящей инструкции, пользователь средств криптографической защиты информации (далее – СКЗИ) обязан незамедлительно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей, по телефону информировать ответственного

пользователя СКЗИ о факте компрометации используемых закрытых криптографических ключей.

3. Решение о компрометации криптографических ключей принимает руководитель образовательной организации на основании письменного уведомления о компрометации, подписанного ответственным пользователем СКЗИ, с приложением, при необходимости, письменного объяснения пользователя СКЗИ по факту компрометации его криптографических ключей.

4. Уведомление должно содержать:

1) идентификационные параметры скомпрометированного криптографического ключа;

2) фамилию, имя, отчество пользователя СКЗИ, который владел скомпрометированным криптографическим ключом;

3) сведения об обстоятельствах компрометации криптографического ключа;

4) время и обстоятельства выявления факта компрометации криптографического ключа.

5. Ответственный пользователь СКЗИ после получения информации о компрометации криптографического ключа пользователя СКЗИ, убеждается в достоверности полученной информации, в согласованное с руководителем организации время выводит из действия ключевую информацию, соответствующую скомпрометированному закрытому криптографическому ключу (прекращает обмен электронными документами с использованием сертификата ключа подписи, соответствующего скомпрометированному закрытому криптографическому ключу) и проводит работу по отзыву сертификата ключа подписи пользователя СКЗИ.

6. Пользователь СКЗИ может одновременно иметь несколько закрытых криптографических ключей и соответствующих им сертификатов ключей подписи, часть из которых использовать в качестве рабочих, а часть – в качестве резервных, на случай компрометации рабочих закрытых криптографических ключей. Это обеспечивает осуществление непрерывного электронного документооборота пользователя СКЗИ за счёт оперативного перехода на использование резервных криптографических ключей, в случае компрометации рабочих криптографических ключей.

7. Осуществление электронного документооборота и использование СКЗИ может быть возобновлено только после ввода в действие другого криптографического ключа взамен скомпрометированного.

8. Скомпрометированные ключи подлежат уничтожению в соответствии с порядком, установленным в пункте 47 «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом Федерального агентства

правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) от 13 июня 2001 года № 152.

9. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в спецпомещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю СКЗИ. Ответственный пользователь СКЗИ должен оценить возможность компрометации хранящихся криптографических ключей, составить акт и принять, при необходимости, меры к локализации последствий компрометации криптографических ключей и к их замене.

10. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ в спецпомещениях, должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптографических ключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

11. Осмотр ключевых носителей многократного использования посторонними лицами, не следует рассматривать, как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения, принимаются срочные меры к их розыску.

12. На время отсутствия пользователей СКЗИ, указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае, по согласованию с ответственным пользователем СКЗИ, необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в отсутствие пользователей СКЗИ.

Директор муниципального
общеобразовательного бюджетного
учреждения гимназии № 1 г. Сочи
имени Филатовой Риммы Алексеевны,
ответственный пользователь СКЗИ Э.И. Латиева