Приложение № 1
к приказу от 23.10.2020г № 521/3

Инструкция по восстановлению связи в случае компрометации действующих ключей к СКЗИ

1. Общие положения

1. Инструкция по восстановлению связи в случае компрометации действующих ключей к СКЗИ определяет порядок восстановления связи при компрометации действующих ключей к криптосредствам (далее – Инструкция) МБОУ «Березинская СОШ»

2. Настоящая Инструкция разработана в соответствии с Приказом ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении 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».

2. Термины и определения

3. Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

4. Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации). Различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования (магнитная лента, дискета, компакт-диск, Data Key, Smart Card, Touch Memory и т.п.).

5. Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

6. Криптоключ – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

7. Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации.

8. Пользователь криптосредств – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

9. Средства криптографической защиты информации – шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

10. Электронная подпись – 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.

3. События, связанные с компрометацией действующих криптоключей

11. К событиям, связанным с компрометацией действующих криптоключей, относится:

1) утрата (в том числе хищение) ключевых носителей (флэш - накопителей) с последующим их обнаружением;

2) увольнение сотрудников, имевших доступ к ключевой информации;

3) передача ключевой информации по линии связи в открытом виде;

4) нарушение правил хранения и уничтожения (после окончания срока действия) криптоключа;

5) возникновение подозрений на утечку информации или ее искажение;

6) не расшифровывание входящих или исходящих сообщений;

7) отрицательный результат при проверке электронной подписи документа;

8) нарушение целостности упаковки ключевых носителей и (или) печати на сейфе, где хранились ключевые носители;

9) несанкционированное копирование ключевых носителей;

10) случаи, когда нельзя достоверно установить, что произошло с ключевыми 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).

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

4. Действия при компрометации криптоключей

13. При наступлении любого из перечисленных выше событий пользователь должен немедленно прекратить связь с другими пользователями и сообщить о факте компрометации (или предполагаемом факте компрометации) Ответственному пользователю криптосредств.

14. Расследование факта компрометации (или предполагаемой компрометации) должно проводиться на месте происшествия специально назначаемой комиссией во главе с Ответственным пользователем криптосредств. Результатом рассмотрения является квалификация или не квалификация данного события как компрометация действующих криптоключей. При установлении факта компрометации действующих криптоключей, скомпрометированные криптоключи уничтожаются.

15. Для восстановления конфиденциальной связи после компрометации криптоключей пользователь обращается к Ответственному пользователю криптосредств с целью регистрации вновь изготовленных (или резервных) криптоключей. Регистрация новых ключей шифрования и электронных подписей осуществляется тем же порядком, как и при плановой смене ключей.