ДОКУМЕНТ ПОДПИСАН ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Документ отправлен на официальный сайт: sosh2.obmirbn.ru
Уполномоченное лицо – руководитель образовательного учреждения:
МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "НИЖНЕГОРСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №2" НИЖНЕГОРСКОГО РАЙОНА РЕСПУБЛИКИ КРЫМ
Действителен с: с 05.08.2026, 14:17
Действителен до: до 29.10.2027, 14:17
Ключ подписи: 00EA8A9CBA0690E6D6C9ABFEDBD28FE47

Муниципальное бюджетное общеобразовательное учреждение «Нижнегорская средняя общеобразовательная школа №2» Нижнегорского района Республики Крым

УТВЕРЖДЕНА
приказом МБОУ «Нижнегорская СОШ №2
от 16.10.2026№ 501

ИНСТРУКЦИЯ
по восстановлению связи в случае компрометации действующих ключей к СКЗИ в информационной системе персональных данных

1. Общие положения

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:

1) утрата (в том числе хищение) ключевых дискет (флэш-накопителей) с последующим их обнаружением;
2) увольнение работников, имевших доступ к ключевой информации;
3) передача ключевой информации по линии связи в открытом виде (если это не предусмотрено правилами пользования);
4) нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;
5) возникновение подозрений на утечку информации или её искажение;
6) не расшифровывание входящих или исходящих сообщений;
7) отрицательный результат при проверке электронной цифровой подписи документа;
8) нарушение целостности упаковки ключевых дискет (флэш-накопителей) и (или) печати на сейфе, где хранились ключевые дискеты (флэш-накопители);
9) несанкционированное копирование ключевых дискет (флэш-накопителей);
10) 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 произошёл 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.

2. Порядок действий при компрометации ключей

2.1. При наступлении любого из перечисленных в п. 1.1 событий пользователь должен немедленно прекратить связь с другими пользователями и сообщить о факте компрометации (или предполагаемом факте компрометации) Администратору ИБ ИСПДн.

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

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

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

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

3. Ответственность за нарушение требований

3.1. Пользователи криптосредств несут персональную ответственность за сохранность полученных криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов, за соблюдение положений настоящей Инструкции.

3.2. Администратор ИБ ИСПДн несёт ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки ПДн с использованием криптосредств лицензионным требованиям и условиям эксплуатационной и технической документации к криптосредствам, а также настоящей Инструкции.