УТВЕРЖДЕНО
приказом и.о.директора
ГБОУ СОШ №1 "ОЦ"
с. Большая Глушица
от 24.04.2023 г. № 142- ОД
и.о. директора школы
_____ О.А. Соколова

C=RU, O="ГБОУ СОШ №1 ""ОЦ"" им. В.И.Фокина с. Большая Глушица", CN=И.о. директора школы Соколова Ольга Александровна, E=shool1_bgl@samara.edu.ru
00c0213d575efc3575
2023.05.02 01:55:08+04'00'

Инструкция
о порядке действий при компрометации криптоключей
ГБОУ СОШ №1 «ОЦ» им. В.И. Фокина с. Большая Глушица

1. Общие положения

Под компрометацией криптоключей понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессами.
К компрометации ключей относятся следующие события:
- утрата носителей ключа;
- утрата иных носителей ключа с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
- доступ посторонних лиц к ключевой информации;
- другие события утери доверия к ключевой информации;

О нарушении, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи средствами криптографической защиты информации (далее – СКЗИ) обязаны сообщить руководству.
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 случае недостачи,

непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.
Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет обладатель скомпрометированной конфиденциальной информации.
Порядок работы пользователей СКЗИ устанавливается инструкцией пользователю СКЗИ, утвержденную приказом директора ГБОУ СОШ №1 «ОЦ» им. В.И. Фокина с. Большая Глушица.
На случай компрометации ключевых документов совместно с ними выдается «Карточка оповещения о компрометации», в которой указывается порядок действий пользователя, номера телефонов и другие способы связи, пароль, означающий факт компрометации криптоключей конкретного пользователя.
Действующие и резервные ключевые документы, предназначенные для применения в случае компрометации действующих криптоключей, должны хранится в внутреннем отсеке сейфа в различных конвертах.

2. Порядок действий пользователя при компрометации ключей.

Первые пять события должны трактоваться как безусловная компрометация действующих ключей; при наличии остальных событий требуется специальное расследование в каждом конкретном случае.
При наступления любого из перечисленных выше событий пользователь должен немедленно прекратить связь с другими пользователя и сообщить о факте компрометации (или предполагаемом факте компрометации) ответственному за использование средств криптографической защиты информации в информационных системах (далее – ответственны).
Расследование факта компрометации (или предполагаемой компрометации) должно проводиться на месте происшествия постоянно действующей в ГБОУ СОШ №1 «ОЦ» им. В.И. Фокина с. Большая Глушица комиссией по уничтожению ключевых документов и средств криптографической информации, обрабатываемых в ОУ, а также допуску пользователей к самостоятельной работе при помощи СКЗИ в ОУ.
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 уничтожения.
Для восстановления конфиденциальной связи после компрометации ключей пользователь обращается ответственному с целью регистрации вновь изготовленных (или резервных) ключей. Регистрация новых ключей шифрования и электронной цифровой подписи осуществляется тем же порядком, как и при плановой смене ключей.

Приложение

ЛИСТ ОЗНАКОМЛЕНИ
с инструкцией о порядке действий при компрометации криптоключей

№ п/п	Дата	должность	Фамилия, имя, отчество	Подпись