Приложение №6
к Приказу № 9 от «19» декабря 2019 г.

Инструкция по действиям в случае компрометации ключевой информации

ПРО ООО ВДПО

История внесения изменений			
Порядковый номер	**Описание изменений**	**Автор**	**Дата введения**
1			

Пермь, 2019 г.

Раздел ГОСТ 27001	Контрольный номер документа	Номер версии	Дата утверждения	Срок пересмотра
A.5	ИН-03	1.0		1 год

СОДЕРЖАНИЕ

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
ДИТ	Департамент информационных технологий

2. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящая Инструкция является внутренним нормативным документом, регламентирующим действия работников, участвующих в обработке и защите ПДн ПРО ООО ВДПО при выполнении ими обязанностей по защите ПДн.

3. ПРИЗНАКИ КОМПРОМЕТАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ

Под компрометацией индивидуального криптографического ключа понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам. К событиям, связанным с компрометацией действующих криптографических ключей, относятся следующие признаки:

- утрата носителей ключевой информации (рабочего или резервного);
- утрата носителей ключевой информации (рабочего или резервного) с последующим их обнаружением;
- разглашение, несанкционированное копирование ключевой информации;
- передача секретных ключей по линии связи в открытом виде;
- увольнение сотрудника, имевшего доступ к ключевой информации;
- неконтролируемый доступ посторонних лиц к носителям ключевой информации;
- возникновение обоснованных подозрений на утечку персональных данных или их искажение;
- невозможность расшифровывания входящих сообщений;
- отрицательный результат при проверке электронной подписи документа;
- нарушение целостности упаковки носителей ключевой информации и/или печати на хранилище (сейфе), где хранились носители.
- нарушение правил хранения криптоключей;

- утрата ключей, кодов от мест хранения ключевой информации (сейфов, металлических шкафов), где хранились носители ключевой информации, в том числе с их последующим обнаружением;
- неисправность носителя ключевой информации;
- другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Первые шесть признаков говорят о безусловной компрометации действующих ключей. По остальным признакам проводится расследование в каждом конкретном случае.

4. ДЕЙСТВИЯ ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ

При наступлении любого из перечисленных в предыдущем разделе событий работник обязан немедленно:

- прекратить обработку ПДн;
- прекратить связь с другими пользователями или абонентами;
- сообщить о факте компрометации Администратору безопасности ИСПДн;
- следовать указаниям Администратора безопасности ИСПДн.

5. ДЕЙСТВИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИСПДН

Администратор безопасности ИСПДн при получении сведений о возможной компрометации ключевой информации обязан провести следующие действия:

- Удостоверится в достоверности полученной информации.
- Провести анализ признаков возможной компрометации ключевой информации и принять решение о компрометации ключевой информации.
- В случае принятия решения о состоявшейся компрометации:
- Произвести временную остановку работы СКЗИ, которые участвовали в работе со скомпрометированным ключом, приостановить работу пользователя в ИСПДн, чей ключ был скомпрометирован.
- В случае если скомпрометирован закрытый ключ электронной подписи, немедленно инициировать процедуру отзыва сертификата открытого ключа, принять меры к сохранению скомпрометированного закрытого ключа для дальнейшего возможного разбора конфликтных ситуаций.
- Уведомить Директора ДИТ и следовать его указаниям.
- Провести предварительное расследование инцидента.
- Провести внеплановое тестирование СЗИ и СКЗИ ИСПДн.

- В случае выявления нарушений работы СЗИ, СКЗИ устранить в соответствии с инструкциями к СЗИ и СКЗИ.
- В соответствии с установленным порядком генерации ключевой информации инициировать процедуру генерации новых ключей.
- После генерации новых ключей провести работы по запуску работы СЗИ, СКЗИ, возобновить работу пользователя в ИСПДн.
- Внести соответствующие записи в журнале учета носителей ключевой информации.

6. ДЕЙСТВИЯ ДИРЕКТОРА ДИТ

Директор ДИТ при получении сведений о возможной компрометации ключевой информации обязан провести следующие действия:

- Создать комиссию по расследованию случая компрометации ключевой информации;
- По результатам расследования случая компрометации ключевой информации принять необходимые меры.

7. ОТВЕТСТВЕННОСТЬ

Руководители структурных подразделений ПРО ООО ВДПО несут ответственность за ежегодное доведение до сотрудников настоящей Инструкции (под роспись) и обеспечение соблюдения ее правил в своих подразделениях.

Сотрудники несут персональную ответственность за соблюдение правил настоящей Инструкции в соответствии с положениями внутренней нормативной документации ПРО ООО ВДПО.

Лист изменений

№ версии	Приказ/ дата	Название документа	Лист / Статья	Содержание изменения	Характер изменения	Изменения произвел

Лист ознакомления

№	Дата	Должность/подразделение	Ф.И.О	Подпись