АДМИНИСТРАЦИЯ
ПРИСТЕНСКОГО РАЙОНА КУРСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 19.10.2021 № 588-па

Об утверждении Инструкции о порядке действий при компрометации криптоключей в ФГИС «ЕГР ЗАГС», отдела ЗАГС Администрации Пристенского района Курской области

В целях выполнения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» Администрация Пристенского района Курской области ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемую Инструкцию о порядке действий при компрометации криптоключей в ФГИС «ЕГР ЗАГС» отдела ЗАГС Администрации Пристенского района Курской области.

2. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации, управляющего делами Администрации Пристенского района Курской области - Н.М. Миронову.

3. Постановление вступает в силу со дня его подписания.

Глава Пристенского района Курской области **В.В.Петров**

УТВЕРЖДЕНА
постановлением Администрации
Пристенского района Курской области
от 19.10.2021 № 586-па

Инструкция
о порядке действий при компрометации криптоключей в ФГИС «ЕГР ЗАГС», отдела ЗАГС Администрации Пристенского района Курской области

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) процессам.

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 документации.

Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия.

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать руководству органа криптографической защиты информации.

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.

Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет обладатель скомпрометированной конфиденциальной информации.

Порядок оповещения пользователей СКЗИ о предполагаемой компрометации криптоключей и их замене устанавливается руководством органа криптографической защиты информации.

На случай компрометации ключевых документов совместно с ними выдается «Карточка оповещения о компрометации», в которой указывается порядок действий пользователя, номера телефонов органа криптографической защиты информации 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 храниться во внутреннем отсеке сейфа в различных конвертах.

Порядок действий пользователя при компрометации ключей

При компрометации ключа у пользователя он должен немедленно прекратить связь по сети с другими пользователями. Решение о факте или угрозе компрометации своего закрытого ключа пользователь принимает самостоятельно.

Пользователь должен немедленно известить орган криптографической защиты информации о компрометации ключей пользователя.

Информация о компрометации может передаваться в орган криптографической защиты информации по телефону с сообщением заранее условленного пароля, зарегистрированного в «Карточке оповещения о компрометации». Порядок обращения и хранения карточки должен соответствовать порядку обращения и хранения ключевых документов.

При наличии сетевого взаимодействия пользователь может оповестить Центр регистрации путем формирования электронного сообщения о компрометации.

После компрометации ключей пользователю формируется новый закрытый ключ и запрос на сертификат. Уведомление о компрометации секретного ключа ЭП на бумажном носителе, заверенное рукописной подписью владельца сертификата и запрос на сертификат (на машинном носителе) вместе с заверенными рукописной подписью бланками запроса на бумажном носителе доставляется лично пользователем или через специальную почтовую связь в орган криптографической защиты информации.