|  |  |  |
| --- | --- | --- |
| **МуниципальнэIуэхущIапIэ**  **Къэбэрдей-БалъкъэрРеспубликэм**  **и Эльбрус муниципальнэкуейм щIэныгъэмкIэ и управленэ** | GERB_ | **Муниципал учреждение**  **Къабарты-Малкъар Республиканы**  **Эльбрус муниципал районну билим**  **бериу управлениясы** |

**МУНИЦИПАЛЬНОЕ УЧРЕЖДЕНИЕ**

**«УПРАВЛЕНИЕ ОБРАЗОВАНИЯ»**

**ЭЛЬБРУССКОГО МУНИЦИПАЛЬНОГО РАЙОНА**

**КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ**

361624, Кабардино-Балкарская Республика, город Тырныауз, проспект Эльбрусский, №-39

Тел.4-39-25, e-mail:ob[relbrus@yandex.ru](mailto:relbrus@yandex.ru)

**ПРИКАЗ**

**01.10.2020 г. г.п. Тырныауз № 132**

**О допуске пользователей к работе со средствами**

**криптографической защиты информации**

Во исполнение приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»,

**ПРИКАЗЫВАЮ:**

1. Допустить к работе со средствами криптографической защиты информации лиц, указанных в перечне пользователей средств криптографической защиты информации, согласно Приложению 1.
2. Утвердить инструкцию пользователя средств криптографической защиты информации в Организации, согласно Приложению 2.
3. Контроль за исполнением настоящего приказа оставляю за собой.
4. Приказ вступает в силу со дня его подписания.

**Начальник управления образования Н.М.Атакуева**

ПРИЛОЖЕНИЕ 1

УТВЕРЖДЕНО  
приказом   
от 01.10.2020 г. № 132

**Перечень пользователей средств криптографической защиты информации**

| **№** | **Наименование подразделения** | **Ф.И.О.** | **Должность** | **Наименование средств криптографической защиты информации** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

ПРИЛОЖЕНИЕ 2

УТВЕРЖДЕНО  
приказом   
от 01.10.2020 г. № 132

**Инструкция** **пользователя**

**средств криптографической защиты информации в Организации**

# Общие положения

* 1. Настоящая Инструкция определяет:

- порядок обращения со средствами криптографической защиты информации (далее – СКЗИ) и криптографическими ключами; - основные обязанности, права и ответственность пользователя СКЗИ (далее – Пользователя); - действия при компрометации ключей и восстановлении конфиденциальной связи; - специальные требования по обработке информации с использованием СКЗИ;

* 1. Деятельность Пользователя контролируется его непосредственным руководителем.

# Основные обязанности Пользователя

* 1. Пользователь обязан:

- соблюдать требования по обеспечению безопасности функционирования СКЗИ; - обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей; - сдать ответственному лицу за СКЗИ носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ; - сдать ответственному лицу за СКЗИ носители ключевой информации (далее – НКИ) по окончании срока действия сертификата ключа, а также в случае компрометации ключа; - немедленно уведомлять ответственное лицо за СКЗИ о компрометации криптографических ключей; - немедленно уведомлять ответственное лицо за СКЗИ о фактах утраты или недостачи СКЗИ, НКИ; - выполнять все требования настоящей Инструкции, правила, изложенные в эксплуатационной документации на СКЗИ, а также другие документы, регламентирующие порядок работы с СКЗИ; - в пределах своей компетенции предоставлять информацию комиссии, проводящей служебные расследования по фактам компрометации, а также выявлению причин нарушения требований безопасности функционирования СКЗИ.

# Права Пользователя

* 1. Пользователь имеет право: - вносить предложения Руководству по совершенствованию СКЗИ;

- повышать уровень квалификации по использованию СКЗИ

# Порядок обращения со средствами криптографической защиты информации

* 1. Монтаж и установка СКЗИ осуществляется ответственным лицом за СКЗИ.
  2. Служебные помещения, в которых размещаются СКЗИ, должны отвечать всем требованиям по оборудованию и охране, предъявляемым к помещениям, выделенным для работы с конфиденциальной информацией. Для хранения носителей ключевой информации помещения обеспечиваются сейфами (металлическими шкафами), оборудуются охранной сигнализацией и по убытии сотрудников закрываются, опечатываются личными печатями ответственных лиц и сдаются под охрану.
  3. Дубликаты ключей от сейфов (а также значения кодов – при наличии кодовых замков) пользователей должны храниться в сейфе руководителя подразделения в упаковках, опечатанных личными печатями пользователей. Несанкционированное изготовление дубликатов ключей ЗАПРЕЩЕНО. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменён.
  4. К эксплуатации СКЗИ допускаются лица, прошедшие соответствующую подготовку и изучившие правила пользования данным СКЗИ.
  5. Все программное обеспечение ПЭВМ, предназначенной для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую СКЗИ, не допускается.

# Использование электронной подписи

* 1. 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.
  2. Сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной подписью Удостоверяющего центра, которые включают в себя открытый ключ электронной подписи и которые выдаются Удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной подписи и идентификации владельца сертификата ключа подписи.
  3. Владелец сертификата ключа подписи – физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы).
  4. Подтверждение подлинности электронной подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной подписи с использованием сертификата ключа подписи принадлежности электронной подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной подписью электронном документе.
  5. Электронная подпись в электронном документе равнозначна собственноручной подписи владельца ключа в документе на бумажном носителе при одновременном соблюдении следующих условий:
* сертификат ключа подписи, относящийся к этой электронной подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
* подтверждена подлинность электронной подписи в электронном документе;
* электронная подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

# Порядок обращения с ключами ЭП

* 1. Криптографический ключ владельца ключа применяется для подписания (проверки электронной подписи) электронных документов до окончания срока его действия или наступления события, трактуемого как компрометация криптоключей.
  2. Владелец электронной подписи (ЭП) – пользователь СКЗИ, получивший установленным порядком право использовать персональный ключ ЭП для удостоверения содержания электронных документов и (или) аутентификации в единой системе идентификации и аутентификации .
  3. Доверенное лицо Владельца ЭП – пользователь СКЗИ, получивший установленным порядком право использовать ключ Владельца ЭП для удостоверения содержания электронных документов и (или) аутентификации.
  4. Назначение владельцев ЭП и доверенных лиц осуществляется на основании приказа о назначении пользователей СКЗИ.
  5. НКИ являются объектами особой важности, т.к. они содержат информацию, предназначенную для гарантированной идентификации Владельца ключа, защиты электронного документа от подделки, компрометации.
  6. Владельцы ключей несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту НКИ от несанкционированного использования.
  7. Для хранения носителей ключевой информации Пользователь должен быть обеспечен сейфом. В случае отсутствия индивидуального сейфа по окончании рабочего дня Пользователь обязан сдавать НКИ лицу, ответственному за хранение.
  8. Категорически запрещается:

- хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность; - во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ); - хранить на НКИ какую-либо информацию, кроме ключевой; - использовать в помещениях, где применяются СКЗИ, личные технические средства, позволяющие осуществлять копирование ключевой информации.Не позднее 10 дней до окончания срока действия сертификата криптоключей Пользователь предоставляет ответственному лицу за СКЗИ заявление на изготовление нового ключа.

* 1. После ввода в действие нового ключа Пользователь обязан предоставить ответственному лицу за СКЗИ ключ, выведенный из действия для уничтожения ключевой информации с носителя.
  2. Использование криптоключей, выведенных из действия, запрещается.

# Действия при компрометации действующих ключей и восстановлении конфиденциальной связи

* 1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

- утрата (хищение) НКИ, в том числе – с последующим их обнаружением; - увольнение (переназначение) сотрудников, имевших доступ к ключевой информации; - передача секретных ключей по линии связи в открытом виде; - нарушение правил хранения криптоключей; - вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки); - отрицательный результат при проверке наложенной ЭП; - все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

* 1. При наступлении любого из перечисленных выше событий владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) ответственному лицу за СКЗИ лично, по телефону, электронной почте или другим доступным способом. В любом случае владелец ключа обязан убедиться, что его сообщение получено и прочтено адресатом.
  2. При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей и сдачу их ответственному лицу за СКЗИ в течение 3 рабочих дней.
  3. Для восстановления конфиденциальной связи после компрометации действующих ключей Пользователь получает у ответственного лица за СКЗИ новые ключи ЭП на основании предоставленного Заявления.

# Ответственность Пользователя

* 1. Владелец ключа несет персональную ответственность за конфиденциальность личных ключевых носителей.
  2. В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Пользователь ключа может быть привлечен к дисциплинарной и/или административной ответственности в соответствии с действующим Законодательством Российской Федерации.

ЛИСТ ОЗНАКОМЛЕНИЯ

с приказом от 01.10.2020 г. № 132

«О допуске пользователей к работе со средствами криптографической защиты информации»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ пп** | **Ф.И.О.**  **работника** | **Должность**  **работника** | **Дата** | **Подпись об ознакомлении** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |