МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «КАРАЧАЕВО-ЧЕРКЕССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ У.Д. АЛИЕВА»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00F43710DABB127C0D3F04420D17B4CDD9
Владелец: ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "КАРАЧАЕВО-ЧЕРКЕССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ У.Д. АЛИЕВА"
Действителен: с 22.01.2024 до 16.04.2025

УТВЕРЖДАЮ
И.о. ректора _____ Узденов Т.А.
«30» 12 2022 г.

ПОЛОЖЕНИЕ
ОБ ИСПОЛЬЗОВАНИИ/ПРИМЕНЕНИИ ЭЛЕКТРОННОЙ ПОДПИСИ В ФЕДЕРАЛЬНОМ ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ «КАРАЧАЕВО-ЧЕРКЕССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ У.Д. АЛИЕВА»

Карачаевск – 2022

1. Общие положения

1.1 Положение об использовании электронной подписи в федеральном государственном бюджетном образовательном учреждении высшего образования «Карачаево-Черкесский государственный университет имени У.Д. Алиева» (далее - Положение) определяет порядок и условия работы сотрудников с электронными документами в системах с применением электронно-цифровой подписи, а также непосредственно связанными с их трудовой деятельностью.

1.2 Положение разработано в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Уставом федеральном государственном бюджетном образовательном учреждении высшего образования «Карачаево-Черкесский государственный университет имени У.Д. Алиева» (далее - КЧГУ, Университет) и локальными нормативными актами Университета.

1.3 Наличие электронной подписи обеспечивает внутренним электронным документам:

- подлинность - подтверждение авторства документа;
- целостность - документ не может быть изменен после подписания;
- не отрицание авторства (неотрекаемость) - пользователь не может отказаться от своей подписи.

1.4 Информация в электронной форме, подписанная электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью пользователя.

1.5 Изготовление (генерацию), выдачу и регистрацию электронных подписей осуществляют сотрудники управления информатизации.

1.6 Использование электронной подписи для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну, не допускается.

2. Термины и определения

2.1 ЭИС - электронная информационная среда, включающая в себя электронные информационные ресурсы, электронные ресурсы, совокупность информационных технологий обеспечивающих электронное взаимодействие и обмен с использованием электронной цифровой подписи.

2.2 Пользователь ЭИС - сотрудник Университета, использующий средства электронной подписи в соответствии с данным Положением и соответствующими инструкциями.

2.3 Права доступа - совокупность правил, регламентирующих порядок и условия доступа субъекта к объектам ЭИС на основе избирательного принципа контроля доступа.

2.4 Администратор ЭИС - сотрудник Университета, обеспечивающий установку, настройку, резервное копирование и другие функции по администрированию ЭИС для ее безотказной работы.

2.5 Средства электронной подписи - шифровальные

(криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи

2.6 Сертификат ключа проверки электронной подписи (сертификат) - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

2.7 Внутренний удостоверяющий центр (ВУЦ) - подразделение, осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей для использования в ЭИС.

2.8 Электронный документ - документ, хранящийся в ЭИС, в котором информация представлена в электронно-цифровой форме.

2.9 Электронная подпись (ЭП) - 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.

2.10 Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.

2.11 Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

2.12 Владелец сертификата ключа подписи - пользователь ЭИС, на имя которого удостоверяющим центром выдан сертификат ключа проверки электронной подписи, и которое владеет соответствующим ключом электронной подписи, позволяющим создавать свою электронную подпись в электронных документах (подписывать электронные документы).

2.13 Аккредитованные удостоверяющие центры - удостоверяющие центры, получившие аккредитацию, а также удостоверяющий центр федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, удостоверяющий центр федерального органа исполнительной власти, уполномоченного на правоприменительные функции по обеспечению исполнения федерального бюджета, казначейскому обслуживанию исполнения бюджетов бюджетной системы Российской Федерации, и удостоверяющий центр Центрального банка Российской Федерации.

2.14 Квалифицированный сертификат - сертификат, созданный с использованием средств аккредитованного удостоверяющего центра.

2.15 Неквалифицированный сертификат - сертификат, созданный с использованием средств ВУЦ.

2.16 Квалифицированная электронная подпись (КЭП) – электронная подпись, полученная в результате криптографического преобразования информации с использованием ключа электронной подписи квалифицированного сертификата.

2.17 Неквалифицированная электронная подпись (НЭП) - электронная

подпись, полученная в результате криптографического преобразования информации с использованием ключа электронной подписи неквалифицированного сертификата.

3. Порядок использования электронной подписи

3.1 Жизненный цикл электронного документа в ЭИС включает: создание и прочие действия по его обработке, отражение в учете, а также хранение. ЭИС обеспечивает регистрацию действий пользователей с электронным документом (логирование) в течение жизненного цикла.

3.2 Все владельцы КЭП и НЭП признают равнозначность своей электронной подписи собственноручной подписи на бумажном носителе, что подтверждается согласием (Приложение №3).

3.3 Полномочия владельца ЭП, подписавшего электронный документ, автоматически подтверждаются в момент подписания электронного документа в ЭИС по положительному результату следующих проверок:

- соответствующий пользователь авторизован в ЭИС,
- соответствующий ключ электронной подписи включен в реестр выданных ключей электронной подписи,
- соответствующий ключ электронной подписи отсутствует в реестре отозванных ключей электронной подписи.

3.4 Время формирования электронной подписи фиксируется средствами ЭИС по местному времени.

3.5 Электронные документы подписанные КЭП или НЭП, признаются в КЧГУ равными по юридической силе документам на бумажных носителях, заверенным собственноручной подписью.

3.6 Пользователи признают, что визуализация штампа КЭП или НЭП при демонстрации электронного документа в интерфейсе ЭИС, является неоспоримым подтверждением факта подписания документа соответствующим владельцем ЭП (подлинность и неотрекаемость).

3.7 При работе с ЭЦП пользователи должны руководствоваться «Инструкция по работе с электронно-цифровой подписью» (Приложение №1), а также «Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи» (Приложение №2)

3.8 Хранение электронных документов осуществляется путем записи сведений об электронных документах в архив электронных документов, который является частью ЭИС.

3.9 Университет обеспечивает техническими и организационными мерами защиту от несанкционированного доступа и преднамеренного уничтожения и/или искажения сведений об электронных документах в архиве электронных документов, а также гарантирует подтверждение авторства документа, подписанного КЭП или НЭП автора, в том числе путем утверждения поименного ограниченного списка лиц, имеющих расширенные (административные) права доступа к архиву электронных документов ЭИС.

3.10 Документы хранятся в ЭИС в том формате, в котором они были созданы. Срок хранения электронных документов и сведений об электронных документах определяется локальными нормативными актами Университета.

3.11 Копия электронного документа может быть изготовлена

(распечатана) на бумажном носителе средствами ЭИС и заверена собственноручной подписью владельца КЭП или НЭП или лица, имеющего расширенные (административные) права доступа к архиву электронных документов. Копия электронного документа на бумажном носителе содержит визуализацию штампа (штампов) КЭП или НЭП, подтверждающую, что оригинал электронного документа подписан КЭП или НЭП. Аутентичность электронного документа и его копии на бумажном носителе обеспечивается средствами ЭИС.

4. Права, обязанности и ответственность владельца электронной подписи

4.1 Владелец ЭП имеет право:

- обращаться для аннулирования (отзыва), приостановки (возобновления) действия принадлежащего ему ключа электронной подписи;
- в случае необходимости замены, восстановления ключа электронной подписи обратиться с соответствующей просьбой и получить новый ключ электронной подписи.

4.2 Владелец КЭП или НЭП обязан:

- вести обработку внутренних электронных документов в ЭИС в соответствии со своими должностными обязанностями;
- принимать все возможные меры для предотвращения несанкционированного использования своего ключа электронной подписи;
- ни при каких условиях не передавать ключ электронной подписи другим лицам;
- при компрометации своего ключа электронной подписи незамедлительно обратиться для приостановки действия принадлежащего ему ключа электронной подписи.

4.3 Владелец ЭП несет личную ответственность за сохранность своего ключа электронной подписи и его защиту от несанкционированного использования.

5. Технология применения средств ЭП в ЭИС

5.1 Для применения ЭП в ЭИС владельцу ЭП необходимо авторизоваться использованием имени пользователя и пароля.

5.2 Информация обо всех выданных пользователю ключах электронной подписи, датах получения и прекращения их действия (изъятия) хранится в ЭИС.

5.3 При прекращении у сотрудника должностных обязанностей по обработке внутренних электронных документов с использованием КЭП или НЭП или при увольнении сотрудника его ключ вносится в реестр отозванных ключей электронной подписи. С момента внесения ключа в реестр отозванных ключей, все последующие электронные документы, подписанные этой НЭП, не считаются подписанными надлежащим образом, т.е. подписью, равнозначной собственноручной.

6. Заключительные положения

6.1 Настоящее Положение вступает в силу с даты утверждения его ректором Университета.

6.2 Документы, созданные в ЭИС и подписанные КЭП или НЭП в соответствии с настоящим Положением, признаются юридически значимыми с даты утверждения Положения.

6.3 Изменения и дополнения в настоящее Положение вносятся на основании решения ректора или на основании предписаний вышестоящих органов и утверждаются ректором Университета.

Согласовано:

начальник юридического отдела Е.Г. Косова

начальник кадрового управления С.-Б.М. Эрикенов

начальник центра информационных технологий Б.Б. Гогуев

Приложение 1

В целях исполнения Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 6.04.2011 № 63-ФЗ «Об электронной подписи», руководствуясь Уставом Университета, Положением об использовании/применении электронной подписи в КЧГУ, другими нормативными правовыми актами Российской Федерации, регулирующими отношения в области обеспечения информационной безопасности и конфиденциальной информации применяется следующая инструкция.

Инструкция
по работе с электронно-цифровой подписью

1. Термины и определения

Электронная цифровая подпись (ЭЦП) - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации и позволяющий идентифицировать владельца ключа, а также установить отсутствие искажения информации в электронном документе.

Средства криптографической защиты информации (далее - СКЗИ) и квалифицированная электронная цифровая подпись предназначены для подписания электронных документов ЭЦП с целью подтверждения подлинности информации, ее авторства и шифрования при передаче по открытым каналам связи для обеспечения конфиденциальности.

Закрытый ключ подписи - уникальная последовательность символов, известная владельцу сертификата и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств ЭЦП.

Открытый ключ подписи - уникальная последовательность символов, соответствующая закрытому ключу подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения подлинности ЭЦП в электронном документе.

Сертификат ключа подписи (сертификат) - документ на бумажном носителе или электронный документ, который включает в себя открытый ключ ЭЦП и который выдается удостоверяющим центром для подтверждения подлинности ЭЦП и идентификации владельца сертификата.

Носитель ключевой информации (ключевой носитель) - материальный носитель информации, содержащий закрытый ключ подписи или шифрования.

Шифрование - способ защиты информации от несанкционированного доступа за счет ее обратимого преобразования с использованием одного или нескольких ключей.

2. Общие положениями

2.1. Настоящая Инструкция предназначена для пользователей,

использующих средства электронной цифровой подписи (ЭЦП).

2.2. Инструкция содержит основные правила обращения с системами электронного документооборота и ключами ЭЦП, выполнение которых необходимо для обеспечения защиты информации при обмене электронными документами.

2.3. Лица, допущенные к работам с ключами ЭЦП, несут персональную ответственность за безопасность (сохранение в тайне) закрытых ключей подписи и обязаны обеспечивать их сохранность, неразглашение и нераспространение, несут персональную ответственность за нарушение требований настоящей Инструкции, неправомочным использованием ЭЦП и средств ЭЦП, компрометацией используемых ключей ЭЦП, нарушений положений Регламента оказания услуг Удостоверяющего центра.

3. Порядок генерации ЭЦП

3.1. Порядок генерации ЭЦП регламентируется соответствующим Регламентом Удостоверяющего центра.

3.2. Владельцы ЭЦП и ответственные исполнители ЭЦП назначаются распоряжением главы района.

3.3. Пользователь, обладающий правом ЭЦП (ответственный исполнитель ЭЦП), самостоятельно создаёт запрос на личный открытый ключ подписи, а также запрос на получение сертификата открытого ключа (в электронном виде и на бумажном носителе) для последующего получения его в аккредитованном удостоверяющем центре.

3.4. Закрытые ключи изготавливаются в 2-х экземплярах: резервная и рабочая копии. В повседневной работе используется рабочая копия ключевого носителя. Срок действия ключей - 1 год с момента выдачи сертификата.

3.5. Хранить ЭЦП на носителях, используемых (флэшки, жесткие диски) совместно с рабочими файлами запрещается.

3.6. Не позднее, чем за 30 рабочих дней до окончания срока действия закрытого ключа, его пользователь обязан выполнить мероприятия по формированию новых закрытых ключей, соответствующего запроса на издание сертификата и оформить заявку на получение нового сертификата.

4. Порядок хранения и использования ЭЦП

4.1. Для хранения ключевых носителей в помещении должно использоваться хранилище (сейф, шкаф, секция).

4.2. Хранение ключевых носителей допускается в одном хранилище с другими документами и ключевыми носителями, при этом отдельно от них и в упаковке, исключающей возможность негласного доступа к ним. Для этого ключевые носители помещаются в специальный контейнер, опечатываемый личной печатью ответственного исполнителя или владельца ЭЦП. Перед вскрытием контейнера необходимо проверить целостность печати и ее принадлежность. В нерабочее время опечатанный контейнер с ключевыми носителями должен находиться в хранилище.

4.3. Транспортирование ключевых носителей должно осуществляться способом, исключающим их утрату, подмену или порчу.

4.4. Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства ЭЦП.

4.5. Запрещается оставлять без контроля вычислительные средства, на которых эксплуатируется ЭЦП после ввода ключевой информации. При уходе пользователя с рабочего места компьютер должен быть заблокирован, а средства ЭЦП убраны в хранилище.

4.6. ЭЦП не подлежит передаче третьим лицам.

4.7. При физической порче рабочей копии ключевого носителя, пользователь уведомляет об этом руководителя подразделения.

4.8. Не допускается:

- осуществлять несанкционированное копирование ключевых носителей;
- разглашать и передавать содержимое ключевых носителей и передачу самих носителей лицам, к ним не допущенным;
- использовать ключевые носители в режимах, не предусмотренных правилами пользования ЭЦП, либо использовать ключевые носители на посторонних ПЭВМ;
- записывать на ключевые носители постороннюю информацию.

5. Порядок уничтожения ключей на ключевых носителях

5.1. Ключи могут быть выведены из действия и уничтожены в следующих случаях:

- плановая смена ключей;
- изменение реквизитов ответственного исполнителя (владельца) ЭЦП;
- компрометация ключей;
- выход из строя (износ, порча) ключевых носителей;
- прекращение полномочий пользователя ЭЦП.

5.2. Уничтожение ключей может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) ключей без повреждения ключевого носителя по рекомендациям изготовителя ключей.

5.3. Ключи должны быть уничтожены не позднее 10 суток после вывода их из действия.

5.4. Удаление ключей после прекращения действий возлагается на пользователя ЭЦП.

6. Действия при компрометации ключей

6.1. Компрометация ключа - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

- потеря ключевых носителей, в том числе с последующим обнаружением;
- возникновение подозрений на утечку информации или ее искажение;
- нарушение печати на контейнере с ключевыми носителями;

- утрата ключей от помещения и сейфов в момент нахождения в них носителя с ключами ЭЦП, в том числе с последующим обнаружением.
- нарушение правил хранения и уничтожения;

6.2. Пользователь самостоятельно определяет факт компрометации закрытого ключа.

6.3. При компрометации ключа пользователь немедленно прекращает обмен электронными документами с другими пользователями и извещает о факте компрометации руководителю подразделения, затем подает в Удостоверяющий центр письменное заявления об аннулировании скомпрометированных ключей. Возобновление работы с ЭЦП возможно только после замены скомпрометированных ключей.

6.4. По факту компрометации ключей должно быть проведено служебное расследование с оформлением уведомления о компрометации.

6.5. Выведенные из действия скомпрометированные ключи уничтожаются.

Приложение 2

Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

1. Общие положения

Настоящее руководство составлено в соответствии с требованиями Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и является средством официального информирования лиц, владеющих квалифицированной электронной подписью, об условиях, рисках и порядке использования квалифицированной электронной подписи и средств электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи.

При применении квалифицированной электронной подписи в информационных системах владельцу сертификата необходимо выполнять требования:

- Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. №152, в части обращения со средствами криптографической защиты информации;
- Инструкция по работе с электронно-цифровой подписью (Приложение №1);
- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. № 66, в части эксплуатации средств криптографической защиты информации;
- эксплуатационной документации к средствам электронной подписи;
- приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

1. Требования по размещению

При размещении средств вычислительной техники с установленными на них средствами квалифицированной электронной подписи:

- должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства квалифицированной электронной подписи, посторонним лицам, не имеющим допуск к работе в

этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты и передаваемую информацию;

- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

2. Требования по установке средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

2.1. При использовании средств квалифицированной электронной подписи должны выполняться следующие меры по защите информации от несанкционированного доступа:

2.1.1. Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- личный пароль пользователь не имеет права никому сообщать;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

2.1.2. При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

- не использовать нестандартные, измененные или отладочные версии операционных систем;
- исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;
- исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;
- на средствах вычислительной техники с установленными средствами квалифицированной электронной подписи должна быть установлена только одна операционная система;
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);
- режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;

- всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;

- необходимо предусмотреть меры, максимально ограничивающие доступ к:

- системному реестру;
- файлам и каталогам;
- временным файлам;
- журналам системы;
- файлам подкачки;
- кэшируемой информации (пароли и т.п.);
- отладочной информации.

2.1.3. На средствах вычислительной техники необходимо:

- организовать удаление (по окончании сеанса работы средств квалифицированной электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

- исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;

- регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

2.1.4. В случае подключения технических средств с установленными средствами квалифицированной электронной подписи к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

2.1.5. Необходимо организовать и использовать:

- систему аудита, организовать регулярный анализ результатов аудита;
- комплекс мероприятий по антивирусной защите.

2.2. Запрещается:

- осуществлять несанкционированное копирование ключевых носителей;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации;

- использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;

- вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;

- записывать на ключевые носители постороннюю информацию;

- оставлять средства вычислительной техники с установленными

средствами квалифицированной электронной подписи без контроля после ввода ключевой информации;

- использовать ключ электронной подписи и соответствующий сертификат ключа проверки электронной подписи, Заявление на изменение статуса которого подано в территориальный орган Федерального казначейства, в течение времени, исчисляемого с момента подачи Заявления на изменение статуса сертификата по момент официального информирования об изменении статуса сертификата, либо об отказе в изменении статуса;

- использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;

- удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки электронной подписи.

3. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи

3.1. Меры защиты ключей квалифицированной электронной подписи.

Ключи квалифицированной электронной подписи при их создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним.

Ключевые носители должны иметь маркировку с учетным номером, присвоенным Заявителем.

Ключи квалифицированной электронной подписи на ключевом носителе могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной электронной подписи.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи.

3.2. Обращение с ключевой информацией и ключевыми носителями.

Недопустимо пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме открытых ключей).

Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной электронной подписи, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

Носитель ключевой информации должен быть вставлен в считывающее

устройство только на время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

3.3. Обеспечение безопасности АРМ с установленными средствами квалифицированной электронной подписи.

С целью контроля исходящего и входящего подозрительного трафика, технические средства с установленными средствами квалифицированной электронной подписи должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. На технических средствах, используемых для работы в информационных системах:

- на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 3;
- должно быть установлено только лицензионное программное обеспечение;
- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;
- должны быть отключены все неиспользуемые службы и процессы операционной системы (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);
- должны регулярно устанавливаться обновления операционной системы;
- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами квалифицированной электронной подписи и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в соответствующей информационной системе;
- должна быть активирована регистрация событий информационной безопасности;
- должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной электронной подписи, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред организации, в том числе средства квалифицированной электронной подписи, журналы работы систем обмена электронными документами и так далее.

Приложение 3

СОГЛАСИЕ

Я, _____настоящим
Фамилия Имя Отчество полностью
подтверждаю, что ознакомлен с Положением об использовании электронной подписи в федеральном государственном бюджетном образовательном учреждении высшего образования «Карачаево-Черкесский государственный университет имени У.Д. Алиева», признаю равнозначность своей Неквалифицированной электронной подписи (далее - НЭП) собственноручной подписи на бумажном носителе и даю согласие на использование НЭП в _____
в соответствии с Положением об использовании электронной подписи в федеральном государственном бюджетном образовательном учреждении высшего образования «Карачаево-Черкесский государственный университет имени У.Д. Алиева» с «_____»_____20__г.

« ___» _____20 __г. _____
Подпись
____ _____ ____ _____

Лист регистрации изменений

Раздел (подраздел), в который вносятся изменения	Основания для изменений	Краткая характеристика вносимых изменений	Дата и номер протокола Ученого совета

Лист ознакомления

№ п/п	Должность	ФИО	Подпись	Дата