

О внесении изменения в постановление Правительства Республики Казахстан от 17 апреля 2004 года № 430

Утративший силу

Постановление Правительства Республики Казахстан от 22 октября 2008 года № 978. Утратило силу постановлением Правительства Республики Казахстан от 28 сентября 2018 года № 605 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования)

Сноска. Утратило силу постановлением Правительства РК от 28.09.2018 № 605 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Правительство Республики Казахстан **ПОСТАНОВЛЯЕТ:**

1. Внести в постановление Правительства Республики Казахстан от 17 апреля 2004 года № 430 "Об утверждении Правил электронного документооборота государственных органов Республики Казахстан" (САПП Республики Казахстан, 2004 г., № 17, ст. 220) следующее изменение:

Правила электронного документооборота государственных органов Республики Казахстан, утвержденные указанным постановлением, изложить в новой редакции согласно приложению к настоящему постановлению.

2. Настоящее постановление вводится в действие со дня подписания.

Премьер-Министр
Республики Казахстан

К. Масимов

Приложение
к постановлению Правительства
Республики Казахстан
от 22 октября 2008 года № 978
Утверждены
постановлением Правительства
Республики Казахстан
от 17 апреля 2004 года № 430

Правила

электронного документооборота государственных органов Республики Казахстан

1. Общие положения

1. Настоящие Правила электронного документооборота государственных органов Республики Казахстан (далее - Правила) разработаны в соответствии со

статьей 4 Закона Республики Казахстан от 7 января 2003 года "Об электронном документе и электронной цифровой подписи".

Правила определяют порядок и условия организации электронного документооборота государственных органов Республики Казахстан.

Действие Правил не распространяется на электронные документы, содержащие сведения, составляющие государственные секреты Республики Казахстан.

Работы по созданию закрытых (секретных) ключей электронной цифровой подписи (порядок выработки, регистрации, выдачи, хранения, уничтожения) (далее - ЭЦП) для государственных органов и порядок обеспечения сохранности электронных документов и закрытых (секретных) ключей ЭЦП, содержащих сведения, составляющие государственные секреты, определяются нормативными правовыми актами в области защиты государственных секретов.

2. В Правилах используются следующие основные понятия:

1) бумажная копия электронного документа - документ, полученный посредством распечатки электронного подлинника, имеющий одинаковое наименование с электронным документом и заверенный лицом, обладающим полномочиями на заверение данного документа;

2) единая система электронного документооборота государственных органов (далее - ЕСЭДО) - система обмена электронными документами между государственными органами Республики Казахстан и должностными лицами соответствующего государственного органа, а также процессов создания, использования, передачи и хранения электронной организационно-распорядительной документации государственных органов Республики Казахстан;

3) ключевой носитель - носитель информации, содержащий закрытый ключ ЭЦП;

4) нормативно-справочная информация - информация (классификаторы, справочники, перечни и другие), основанная на нормативных документах и используемая для определения различных характеристик документа;

5) подлинник бумажного документа - документ, составленный в соответствии с требованиями Государственных стандартов Республики Казахстан, и не имеющий электронного исходного подлинника;

6) подлинник электронного документа - документ, подписанный ЭЦП, созданный изначально в формате электронного документа и не имеющий бумажного исходного подлинника;

7) положительный результат проверки подлинности ЭЦП подтверждение подлинности ЭЦП участником системы электронного документооборота государственных органов с использованием средств ЭЦП;

8) средство криптографической защиты информации (далее - СКЗИ) - средство, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение и управление ключами;

9) удостоверяющий центр - юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства;

10) участник единой системы электронного документооборота государственных органов (далее - участник ЕСЭДО) - государственный орган или должностное лицо, участвующее в процессах сбора, обработки, хранения и распространения электронных документов;

11) Центр ЕСЭДО - подсистема ЕСЭДО, обеспечивающая регистрацию участников ЕСЭДО, синхронизацию нормативно-справочной информации и обмен электронными документами между участниками ЕСЭДО;

12) электронная регистрационная контрольная карточка (далее - ЭРКК) - электронный документ с учетными данными о документе по установленной форме, фиксирующая его реквизиты;

13) электронная копия бумажного документа - электронный документ, полностью воспроизводящий информацию подлинного бумажного документа, в электронно-цифровой форме с ЭЦП заверителя;

14) электронный дубликат бумажного документа - документ, произведенный и обработанный вместе с идентичным бумажным документом, имеющим те же реквизиты, структуру и содержание, и подписанный ЭЦП тем же лицом, которое подписало подлинник в виде бумажного документа;

15) формат электронного документа - структура содержательной части электронного сообщения, на основе которого сформирован электронный документ.

2. Порядок организации ЕСЭДО

3. Для организации электронного документооборота используется ЕСЭДО, обеспечивающая выполнение следующих функций:

- 1) авторизацию доступа пользователей и разграничение прав доступа;
- 2) формирование (составление) электронного сообщения в формате, установленном для данного электронного документа;
- 3) формирование и проверку ЭЦП электронного документа;
- 4) коллективную работу с электронными документами;
- 5) контроль исполнения электронных документов;
- 6) поиск электронного документа;

7) отправку и подтверждение получения электронных документов в пределах государственного органа и между государственными органами;

8) учет электронных документов (регистрацию входящих и исходящих электронных документов);

9) хранение электронных документов;

10) передачу электронного документа в архив электронных документов государственного органа;

11) гарантированное уничтожение электронных документов, регистрационных свидетельств и соответствующих ключей ЭЦП и электронных баз данных ЕСЭДО.

4. Электронный документ состоит из двух частей: содержательной и реквизитной.

Содержательная часть документа может состоять из одного или нескольких файлов в следующих форматах:

1) PDF, TIFF, JPEG - графический формат;

2) RTF, DOC - текстовый формат;

3) XLS - табличный формат;

4) PPT - презентации;

5) RAR, ZIP - архивированный формат.

При формировании (составлении) электронных документов используются следующие обязательные реквизиты:

1) официальное наименование организации;

2) наименование вида документа;

3) дата документа;

4) регистрационный номер документа;

5) индекс номенклатуры дел;

6) место составления или издания документа;

7) текст;

8) название и версия программного обеспечения, при помощи которого создан документ;

9) электронная цифровая подпись.

Использование дополнительных реквизитов определяется в зависимости от вида документа в соответствии с требованиями Государственных стандартов Республики Казахстан.

5. Участники ЕСЭДО используют единую нормативно-справочную информацию. Регулирование и изменение нормативно-справочной информации, касающейся организационно-распорядительной документации, осуществляет уполномоченный государственный орган управления архивами и документацией.

6. Первичная обработка электронного документа в ЕСЭДО включает:

- 1) проверку всех реквизитов электронного документа;
- 2) проверку подлинности всех ЭЦП электронного документа;
- 3) проверку действительности регистрационного свидетельства ЭЦП и открытого ключа ЭЦП;
- 4) проверку полномочий статуса всех лиц, проставивших ЭЦП в электронном документе.

7. При получении положительного результата первичной обработки электронного документа, он подлежит дальнейшей обработке. В случае отрицательного результата первичной обработки, электронный документ считается неполученным, о чем получатель электронного документа направляет соответствующее уведомление - "не принято" с указанием причины неполучения документа.

8. Перед отправкой электронного документа проверяется правильность его оформления (наличие реквизитов электронного документа) и адреса, в том числе проверка подлинности ЭЦП и регистрационных свидетельств.

9. Электронный документ считается исходящим от отправителя в случае установления принадлежности электронного документа отправителю и неискаженности его содержания путем получения положительного результата проверки ЭЦП получателем.

10. Подтверждение получения электронного документа производится путем направления подтверждения о его получении отправителю, которое также является электронным документом.

11. Дата доставки и регистрации электронного документа государственным органом-получателем подтверждается ЕСЭДО путем передачи в государственный орган - отправитель уведомлений (электронного документа или иного сообщения) содержащего:

- 1) дату, время доставки электронного документа;
- 2) регистрационный номер, присвоенный в системе получателя электронного документа.

12. Электронный документ считается не доставленным получателю до тех пор, пока отправитель не получил соответствующего уведомления.

13. Если уведомление не получено отправителем в течение одного дня после отправки электронного документа, то отправитель может уведомить получателя о неподтверждении получения электронного документа при помощи иных средств связи.

14. ЕСЭДО обеспечивает доставку электронных документов объемом, не превышающим 10 Мб.

15. Ведение учета и контроля исполнения электронных документов в ЕСЭДО осуществляется службой документационного обеспечения государственного органа с использованием ЭРКК.

16. Учет электронных документов осуществляется путем ведения ЭРКК. Сроки хранения ЭРКК соответствуют срокам хранения электронных документов. ЭРКК хранятся совместно с электронными документами, соответствующими регистрационными свидетельствами ЭЦП, уведомлениями - квитанциями о доставке этих электронных документов.

17. Участники ЕСЭДО обеспечивают защиту от несанкционированного доступа и непреднамеренного уничтожения и (или) искажения учетных данных, содержащихся в базах данных электронного документооборота ЕСЭДО, а также обеспечивают создание резервных копий электронных документов соответствующих государственных органов.

18. В архивах электронных документов должны храниться электронный документ с ЭРКК и уведомление о доставке электронного документа.

19. Сроки хранения электронных документов в государственных органах устанавливаются уполномоченным государственным органом управления архивами и документацией.

20. Электронные документы хранятся в том формате (касается вложенных файлов), в котором они были сформированы, отправлены или получены, с сохранением ЭЦП.

21. Хранение электронных документов сопровождается хранением соответствующих электронных баз данных, открытых ключей ЭЦП (регистрационных свидетельств ЭЦП) и программ, обеспечивающих ведение учета и проверку ЭЦП электронных документов.

22. Для открытых ключей ЭЦП в государственных органах и удостоверяющем центре хранятся оформленные в установленном порядке документы (регистрационные свидетельства), подтверждающие принадлежность этих ключей конкретному участнику ЕСЭДО.

Для каждого открытого ключа хранится информация о начале и завершении его действия. При этом доступ к массивам открытых ключей находящихся на оперативном (ведомственном) архивном хранении должен быть ограничен.

Сохранность, надлежащее использование и защита от несанкционированного доступа к носителям ключевой информации, а также хранящихся в них закрытых (секретных) ключей ЭЦП возлагается на их владельцев.

23. При хранении электронных документов обеспечивается привязка (синхронизация) электронных документов и соответствующих открытых ключей ЭЦП.

Архивы электронных документов подлежат защите от несанкционированного доступа и непреднамеренного уничтожения и (или) искажения.

Защиту архива электронных документов осуществляют участники ЕСЭДО в порядке, установленном нормативными правовыми актами уполномоченного государственного органа в сфере по обеспечению информационной безопасности

3. Порядок использования и соотношения электронных и бумажных документов в ЕСЭДО

24. Электронный документ не имеет копий в электронном виде.

25. В номенклатуре дел фиксируется форма представленного документа: электронная или бумажная.

26. Электронные документы со сроками хранения свыше 10 лет имеют бумажные копии электронного документа.

27. Электронные копии бумажных документов создаются в случаях, когда работа с заверенными электронными копиями бумажных документов не противоречит действующему законодательству и обеспечивает удобную обработку и использование информации, содержащейся в бумажном документе.

28. Электронная копия заверяется с указанием на то, что исходным документом является бумажный документ и нанесением сведений о подписи. Для заверения электронной копии документа в системе электронного документооборота предусматривается ЭЦП для заверяющего с текстом " * * * Копия бумажного документа введена с подлинника бумажного документа" и полем для указания подписавшего лица на бумажном документе. Взаимное соответствие исходного бумажного документа и его электронной копии обеспечивается лицом, заверившим копию бумажного документа.

29. Полномочиями на заверение электронной копии бумажных документов обладают лица, определенные в информационной системе как ответственные за создание электронных копий бумажных документов, а также данные действия закреплены нормативными правовыми актами участника ЕСЭДО.

30. Бумажная копия электронного документа отображает содержание электронного документа в явном виде, доступном для восприятия без использования дополнительных средств и методов.

31. Бумажная копия электронного документа заверяется с указанием на то, что исходным документом является электронный документ и нанесением сведений о результате проверки ЭЦП. Для заверения копии электронного документа на бумажном носителе и нанесении информации о результате проверки ЭЦП используется штамп с текстом " * * * Копия электронного

документа верна. Определен положительный результат проверки ЭЦП" и полем для подписи заверяющего лица.

При отрицательном результате проверки ЭЦП используется штамп с текстом " ? ? ? Копия электронного документа не верна. Определен отрицательный результат проверки ЭЦП" и полем для подписи заверяющего лица. Взаимное соответствие исходного электронного документа и его бумажной копии обеспечивается лицом, заверившим копию электронного документа на бумажном носителе.

32. Бумажная копия электронного документа содержит:

- 1) текст документа;
- 2) распечатку сертификата соответствия ЭЦП;
- 3) обязательную отметку "Копия электронного документа";
- 4) наименование информационной системы, из которой он получен;
- 5) дату создания бумажной копии;

6) штамп с текстом " * * * Копия электронного документа верна. Определен положительный результат проверки ЭЦП" и подпись заверителя или штамп с текстом " ? ? ? Копия электронного документа не верна. Определен отрицательный результат проверки ЭЦП".

Данные, указанные в подпунктах 2) - 6) указываются на каждом листе бумажной копии электронного документа.

4. Порядок использования электронной цифровой подписи в ЕСЭДО

33. Участникам ЕСЭДО обеспечиваются подлинность и целостность электронных документов путем:

1) интегрирования в ЕСЭДО средств криптографической защиты информации (далее - СКЗИ), прошедших процедуру подтверждения соответствия в порядке, установленном законодательством Республики Казахстан по техническому регулированию;

2) разграничением прав доступа к электронным документам.

34. Участникам ЕСЭДО необходимо:

1) хранить в тайне служебную информацию, ставшую им известной в процессе работы с СКЗИ;

2) хранить в тайне содержание закрытых ключей средств ЭЦП (СКЗИ);

3) обеспечивать сохранность носителей ключевой информации и других документов о ключах ЭЦП, выдаваемых с этими носителями информации;

4) осуществлять синхронизацию времени на персональных компьютерах с эталонным временем;

5) не осуществлять эксплуатацию программ на персональных компьютерах (в том числе - вирусы), которые могут нарушить корректное функционирование средств ЭЦП.

35. Для оформления электронных документов в ЕСЭДО могут использоваться только те закрытые (секретные) ключи электронной цифровой подписи, которым соответствуют открытые ключи ЭЦП, имеющие действующие регистрационные свидетельства, выданные удостоверяющим центром.

36. Порядок применения электронной цифровой подписи в ЕСЭДО заключается в следующем:

1) подписание электронного документа осуществляется:

одной или несколькими ЭЦП руководителей;

одной ЭЦП работника службы документационного обеспечения;

2) порядок применения электронной цифровой подписи руководителя:

руководитель подписывает текст документа (вложенный(ые) файлы) до регистрации с применением ЭЦП, которая обеспечивает целостность и неизменность текста документа;

формирование ЭЦП руководителя (первой ЭЦП) осуществляется с использованием СКЗИ, ключевого носителя информации СКЗИ и регистрационного свидетельства, полученного в удостоверяющем центре государственных органов;

3) Порядок применения электронной цифровой подписи службы документационного обеспечения:

для пересылки электронного документа между государственными органами:

электронная цифровая подпись работника службы документационного обеспечения подписывает следующие реквизиты:

уникальный идентификатор, назначенный из ЕСЭДО;

дата документа;

автор документа;

текст;

ЭЦП руководителя;

формирование электронной цифровой подписи службы документационного обеспечения осуществляется с использованием СКЗИ, ключевого носителя и регистрационного свидетельства, полученного в удостоверяющем центре государственных органов.

В случае отправки электронного документа юридическому или физическому лицу на их запрос через веб-портал "электронного правительства" используется электронная цифровая подпись работника службы документационного обеспечения которой подписывают следующие реквизиты:

уникальный идентификатор, назначенный из ЕСЭДО;

дата документа;
автор документа;
заголовок к тексту (краткое содержание);
текст;

ЭЦП руководителя;

формирование ЭЦП службы документационного обеспечения осуществляется с использованием СКЗИ, закрытого ключа и соответствующего регистрационного свидетельства юридического или физического лица.

37. Датой создания электронного документа считается дата формирования и установки электронной цифровой подписи службы документационного обеспечения.

5. Обеспечение информационной безопасности в ЕСЭДО

38. Информационная безопасность ЕСЭДО обеспечивается путем соблюдения организационных правовых мер и использования программно-аппаратного комплекса средств автоматизации, включающего в себя системы электронного документооборота, удостоверяющего центра, транспортной среды и технических средств защиты информации, сертифицированных на соответствие требованиям информационной безопасности в порядке, установленном законодательством Республики Казахстан.

Средства криптографической защиты информации используются в строгом соответствии с их эксплуатационной документацией и правилами использования.

39. Документы, содержащие секретную информацию, не подлежат отправке посредством программного обеспечения ЕСЭДО.