

УТВЕРЖДЕНО
Решением Совета директоров
ООО «Спектр Инвест»
(Протокол № 2/СД/2011 от 30 сентября 2011 г.)

РЕГЛАМЕНТ
использования электронной цифровой подписи в
Системе электронного документооборота
ООО «Спектр Инвест»

Москва
2011 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Регламент является документом, регламентирующим порядок применения электронной цифровой подписи в Системе электронного документооборота при осуществлении взаимодействия Общества с ограниченной ответственностью «Спектр Инвест» (далее – Общество) и иных Участников Системы электронного документооборота.

Настоящий Регламент определяет правовые условия, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Владелец сертификата ключа подписи – физическое лицо, являющееся пользователем Системы электронного документооборота, на имя которого Удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах.

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

Система электронного документооборота (Система ЭДО) – организационно-техническая автоматизированная информационная система электронного документооборота, представляющая собой совокупность программного, аппаратного и информационного обеспечения ее участников. Система электронного документооборота является автоматизированной информационной системой, действующей по правилам, устанавливаемым Обществом.

Открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе.

Оператор Системы электронного документооборота – лицо, обеспечивающее функционирование и использование Системы электронного документооборота. Оператором Системы электронного документооборота является Общество.

Подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат проверки средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Пользователь Системы электронного документооборота – физическое лицо, в том числе являющееся уполномоченным представителем участника Системы электронного документооборота и наделенное полномочиями по совершению действий в рамках Системы электронного документооборота.

Пользователь сертификата ключа подписи – физическое лицо, являющееся пользователем Электронной системы документооборота и использующее сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Сертификат ключа подписи – электронный документ с электронной цифровой подписью уполномоченного лица Удостоверяющего центра, который включает в себя

открытый ключ электронной цифровой подписи и который выдается Удостоверяющим центром Пользователям Системы электронного документооборота для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Средство электронной цифровой подписи - программное средство, обеспечивающие реализацию следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Удостоверяющий центр (УЦ) – организация, обеспечивающая согласно Федеральному закону от 10.01.2002 года № ФЗ-1 «Об электронной цифровой подписи» выполнение функций удостоверяющего центра.

Уполномоченное лицо Удостоверяющего центра - физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению от лица Удостоверяющего центра сертификатов ключей подписей и списков отозванных сертификатов.

Участник Системы электронного документооборота – лицо, правомерно использующее Систему электронного документооборота.

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

Электронный документ – электронное сообщение, соответствующее формату электронных документов MSOffice, подписанное электронной цифровой подписью и способное быть преобразованным средствами Системы ЭДО в форму, пригодную для однозначного восприятия его содержания.

3. ДЕЙСТВИЕ РЕГЛАМЕНТА

3.1. Настоящий Регламент утверждается решением компетентного органа Общества.

3.2. Настоящий Регламент прекращает свое действие на основании решения соответствующего компетентного органа Общества. Прекращение действия настоящего Регламента не влияет на юридическую силу и действительность электронных документов, созданных Участниками Системы ЭДО до прекращения действия настоящего Регламента.

3.3. Действие настоящего Регламента распространяется на Участника Системы ЭДО с момента получения сейф-пакета, предусмотренного п. 13.2 настоящего Регламента.

4. СУБЪЕКТЫ РЕГЛАМЕНТА

Субъектами настоящего Регламента являются участники Системы ЭДО, выступающие непосредственно или в лице своих полномочных представителей - пользователей Системы ЭДО: владельцев сертификатов ключей подписей и пользователей сертификатов ключей подписей.

5. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

5.1. Условиями допуска Участника к осуществлению электронного документооборота являются:

- присоединение к настоящему Регламенту, путем представления Заявления на формирование ключей электронной подписи (Приложение 1);
- установка необходимого программного обеспечения (ПО);
- выполнение Удостоверяющим центром процедуры формирования ключей подписи;
- изготовление Удостоверяющим центром сертификата ключа для Участника.

5.2. Для формирования ЭЦП под электронными документами каждый Участник должен иметь ключевой носитель с закрытым ключом и сертификат открытого ключа.

6. ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

6.1. Электронный документ может быть подписан только тем закрытым ключом ЭЦП, для которого Удостоверяющим центром изготовлен сертификат ключа.

6.2. Электронный документ считается исходящим от Участника, если он подписан ЭЦП, владельцем сертификата ключа которой является данный Участник.

6.3. Риск неправомерного подписания электронного документа ЭЦП несет Участник, от имени которого данный документ подписан.

6.4. Электронный документ, подписанный от имени Участника, не влечет правовых последствий, если до момента получения данного документа адресат будет уведомлен о приостановлении действия или аннулировании сертификата ключа соответствующей подписи.

6.5. Замена закрытых ключей электронной подписи не влияет на юридическую силу электронного документа, если он был подписан действующим на дату подписания закрытым ключом ЭЦП в соответствии с настоящим Регламентом.

6.6. Каждый Участник должен иметь свой индивидуальный закрытый ключ ЭЦП для подписания исходящих от него электронных документов.

6.7. Проверка ЭЦП проводится при получении доставленного электронного документа средствами ЭЦП.

6.8. Участником используются ключи, соответствующие сертификаты ключей, полученные в установленном настоящим Регламентом порядке.

7. ТРЕБОВАНИЯ К ЭЛЕКТРОННОМУ ДОКУМЕНТУ

7.1. Электронный документ, сформированный в системе ЭДО, имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия в случае его надлежащего оформления в соответствии с настоящим Регламентом.

7.2. Электронное сообщение приобретает правовой статус электронного документа при его соответствии требованиям, установленным настоящим Регламентом.

7.3. Электронный документ должен быть сформирован в одном из форматов, соответствующих форматам электронных документов MS Office и подписан ЭЦП.

7.4. Все действия с электронными документами, оформленными, переданными и/или полученными в соответствии с настоящим Регламентом, признаются Участниками совершенными в письменной форме и не могут быть оспорены только на том основании, что они совершены в электронном виде.

8. ФОРМИРОВАНИЕ ЭЛЕКТРОННОГО ДОКУМЕНТА

8.1. Формирование электронного документа осуществляется в следующем порядке:

- формирование электронного сообщения в формате, установленном для данного электронного документа;
- подписание сформированного электронного сообщения электронной подписью.

9. ПОДЛИННИК ЭЛЕКТРОННОГО ДОКУМЕНТА

9.1. Электронный документ может иметь неограниченное количество экземпляров. Для создания дополнительного экземпляра существующего электронного документа осуществляется воспроизводство содержания документа вместе с ЭЦП.

9.2. Все экземпляры электронного документа являются подлинниками данного электронного документа.

9.3. Электронный документ не может иметь копий в электронном виде.

9.4. Подлинник электронного документа считается не существующим в случаях если:

- нет ни одного учтенного экземпляра данного электронного документа;
- получение или восстановление экземпляра данного электронного документа невозможно;
- нет способа установить подлинность ЭЦП.

10. КОПИИ ЭЛЕКТРОННОГО ДОКУМЕНТА НА БУМАЖНОМ НОСИТЕЛЕ

10.1. Копии электронного документа могут быть изготовлены (распечатаны) на бумажном носителе и заверены собственноручной подписью уполномоченного лица Общества, и скреплены оттиском печатью Общества.

10.2. Копии электронного документа на бумажном носителе должны содержать обязательную отметку, свидетельствующую о том, что это копия.

10.3. Электронный документ и его копии на бумажном носителе должны быть аутентичными.

10.4. Программные средства, осуществляющие преобразование электронного документа для изготовления (распечатки) в виде бумажного документа, являются неотъемлемой составной частью программного обеспечения, используемого в системе ЭДО.

11. ПРОВЕРКА ПОДЛИННОСТИ ДОСТАВЛЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТА

11.1. Полученный электронный документ проверяется на целостность, т.е. его доставку в неискаженном (по отношению к первоначальному) виде.

11.2. Полученный электронный документ проверяется на соответствие установленному для него формату.

11.3. Электронный документ подлежит дальнейшей обработке и исполнению только в случае положительного результата проверки целостности электронного документа, его соответствия формату электронного документа MS Office.

11.4. При отрицательном результате проверки целостности электронного документа, в том числе подлинности ЭЦП, документ считается не полученным и не подлежит дальнейшей обработке и исполнению.

12. ОТЗЫВ ЭЛЕКТРОННОГО ДОКУМЕНТА

12.1. В отдельных случаях отправитель имеет право отозвать отправленный документ путем отправки получателю электронного документа об отзыве.

12.2. Электронный документ может быть отозван до момента его исполнения.

13. УДОСТОВЕРЯЮЩИЙ ЦЕНТР И СЕРТИФИКАТЫ ОТКРЫТЫХ КЛЮЧЕЙ

13.1. Удостоверяющим центром, выдающим сертификаты ключей подписей для использования в Системе ЭДО является Удостоверяющий Центр компании «Сигнал-КОМ» - eNotary.

В Системе ЭДО не принимаются и не признаются сертификаты ключей подписей, изданные иными Удостоверяющими центрами.

13.2. Оператор Системы ЭДО передает Участникам Системы ЭДО на основании соответствующего Акта приема-передачи (Приложение 2) сейф-пакет, запечатанный таким образом, что любая попытка его вскрытия не может остаться незамеченной. Сейф-пакет включает в себя:

- сертификаты ключей электронной подписи;
- ключи электронной подписи;
- программное обеспечение, в т.ч. средства криптографической защиты;

Представление Заявления на формирование ключа подписи (Приложение 1) означает согласие и присоединение к настоящему Регламенту.

Расходы, связанные с изготовлением ключей электронной подписи и использование соответствующего программного обеспечения оплачиваются Участником системы ЭДО согласно тарифам, определенным Приложением 3 к настоящему Регламенту.

13.3. Идентификационные данные, включенные в соответствующее поле сертификата ключа подписи однозначно идентифицируют владельца сертификата ключа подписи и соответствуют идентификационным данным владельца сертификата ключа подписи, зарегистрированным в Реестре Удостоверяющего центра.

13.4. Для определения статуса сертификата ключа подписи, получения актуального списка отозванных сертификатов, актуальных сертификатов уполномоченных лиц Удостоверяющего центра используется файл сертификатов Удостоверяющего центра.

14. СРЕДСТВА ПРИМЕНЕНИЯ ЭЦП

14.1. В качестве средства ЭЦП, обеспечивающего реализацию функций создания ЭЦП в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждения с использованием открытого ключа электронной цифровой подписи подлинности ЭЦП в электронном документе, создания закрытых и открытых ключей электронных цифровых подписей, используются программный продукт Signal-COM CSP ЗАО «Сигнал-КОМ».

Пользователи Системы ЭДО должны обеспечить сохранность в тайне закрытых ключей электронных цифровых подписей.

15. ДОКУМЕНТЫ, ПОДПИСЫВАЕМЫЕ ЭЦП

15.1. Перечень электронных документов, которые могут быть подписаны ЭЦП и в которых ЭЦП признается равнозначной собственноручной в случае выполнения всех условий равнозначности определяется следующими документами:

- 1) Регламентом Предоставления ООО «Спектр Инвест» брокерских услуг на рынке ценных бумаг Общества;
- 2) Договором доверительного управления ценными бумагами и средствами инвестирования в ценные бумаги, заключенным Обществом с Участником Системы ЭДО;

3) Отчетом доверительного управляющего в соответствии с Договором доверительного управления ценными бумагами и средствами инвестирования в ценные бумаги;

4) Отчетом брокера в соответствии с Договором о предоставлении брокерских услуг на рынке ценных бумаг.

16. УСЛОВИЯ РАВНОЗНАЧНОСТИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ СОБСТВЕННОРУЧНОЙ

16.1. ЭЦП в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

- подтверждена подлинность ЭЦП в электронном документе;

- ЭЦП используется в соответствии со сведениями, указанными в сертификате ключа подписи.

16.2. Сертификат ключа подписи действует на определенный момент времени (действующий сертификат), если:

- наступил момент времени начала действия сертификата ключа подписи;

- срок действия сертификата ключа подписи не истек;

- сертификат ключа подписи не аннулирован (отозван) и действие его не приостановлено;

- подтверждена подлинность ЭЦП уполномоченного лица Удостоверяющего центра в данном сертификате.

Закрытый ключ подписи действует на определенный момент времени (действующий закрытый ключ), если:

- наступил момент времени начала действия закрытого ключа;

- срок действия закрытого ключа не истек;

- сертификат ключа подписи, соответствующий данному закрытому ключу действует на данный момент времени.

- Соответствующий открытый ключ ЭЦП занесён в реестр открытых ключей Удостоверяющего центра.

17. ПОРЯДОК ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

17.1. Формирование электронной цифровой подписи электронного документа осуществляется с использованием применяемого средства ЭЦП и программного обеспечения Системы электронного документооборота.

Формирование ЭЦП может быть осуществлено только владельцем сертификата ключа подписи при соблюдении п. 16.2. настоящего Регламента ЭЦП.

17.2. Подтверждение подлинности электронной цифровой подписи электронного документа осуществляется с использованием применяемого средства ЭЦП и программного обеспечения Системы ЭДО.

Подтверждение подлинности ЭЦП может быть осуществлено пользователями сертификатов ключей подписей.

18. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ, СВЯЗАННЫХ С ПРИМЕНЕНИЕМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

18.1. В случае возникновения конфликтов при использовании электронных документов, в частности, спора в отношении авторства, подлинности или целостности электронных документов, подписанных ЭЦП, применяется порядок разрешения конфликтов, предусмотренный настоящим Регламентом.

18.2. В случае возникновения споров о подлинности ЭЦП в электронном документе бремя доказывания лежит на лице, оспаривающем наличие подписи.

18.3. В случае возникновения споров о факте внесения изменений в электронный документ после его подписания ЭЦП бремя доказывания лежит на лице, утверждающем, что в документ были внесены изменения.

18.4. Подтверждение подлинности ЭЦП в случае возникновения разногласий осуществляется с использованием средств ЭЦП.

18.5. Для подтверждения подлинности ЭЦП используется сертификат ключа, принадлежащий лицу, наличие подписи которого предполагается под документом. Сертификат ключа должен быть действителен на момент подписания электронного документа.

18.7. При возникновении между участниками споров, связанных с наличием ЭЦП в электронном документе, для экспертизы может быть привлечен разработчик используемых средств ЭЦП или государственный орган, осуществляющий лицензирование деятельности в области криптографии.

18.8. Споры между Участниками Системы ЭДО и Удостоверяющим центром могут быть переданы на рассмотрение в соответствующий суд в г. Москве.

19. СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

19.1. Электронные документы, участвующие в электронном документообороте, и средства ЭЦП являются конфиденциальной информацией.

19.2. Участники обязаны соблюдать меры по обеспечению информационной безопасности при использовании Системы ЭДО.

19.3. Соблюдение требований информационной безопасности при использовании Системы ЭДО обеспечивает:

- конфиденциальность информации;
- целостность передаваемой информации (целостность защищаемых данных обеспечивается использованием функций ЭЦП электронного документа);
- аутентификацию (передаваемую информацию может получить только лицо, кому она предназначена, а отправителем является именно тот, от чьего имени она отправлена).

19.4. Основные мероприятия по обеспечению информационной безопасности разделяются на применение аппаратно-программных средств и применение организационных мер.

К аппаратно-программным средствам относятся:

Программные средства, специально разработанные для осуществления электронного документооборота;

Средства аутентификации и разграничения доступа;

Средства криптографической защиты информации;

Средства антивирусной защиты, включая средства обеспечения безотказной работы.

К организационным мерам относятся:

Размещение аппаратно-программных средств в помещении с контролируемым доступом;

Административные ограничения доступа к этим средствам, допуск только специально подготовленных и уполномоченных лиц;

Защита от повреждающих внешних воздействий (пожар и т.п.).

19.5. Участники обязаны перед первым использованием на компьютере и в дальнейшем не реже 1 (одного) раза в месяц проводить контроль целостности исполняемых файлов программного обеспечения, используемого для получения услуг, программными средствами, входящими в сейф-пакет, передаваемый Участнику ЭДО.

20. МЕРЫ ЗАЩИТЫ ЗАКРЫТЫХ КЛЮЧЕЙ

20.1. Закрытые ключи Пользователей Системы ЭДО при их генерации Удостоверяющим центром записываются на отчуждаемые носители ключевой информации.

20.2. Пользователь Системы ЭДО должен обеспечить надежное хранение в тайне своего закрытого ключа электронной подписи. Личные ключевые носители пользователей должны храниться в сейфе. Пользователь УЦ несет персональную ответственность за хранение личных ключевых носителей.

20.3. Закрытые ключи на отчуждаемом носителе необходимо защищать ПИН-Кодом. ПИН-Код формирует Пользователь сертификата ключа подписи используя средства ЭЦП.

20.4. Ответственность за конфиденциальность пароля возлагается на владельца закрытого ключа.

20.7. Хранение закрытых ключей ЭЦП Системы ЭДО, допускается в одном хранилище с другими документами в условиях, исключающих их непреднамеренное уничтожение, а также компрометацию в результате хранения с документами, содержащими пароль на закрытый ключ.

20.8. Пересылка (передача) закрытых ключей ЭЦП по открытым каналам связи не допускается.

20.9. В целях обеспечения конфиденциальности ключей, вышедших из обращения, может применяться процедура уничтожения с использованием средств ЭЦП.

Приложение 1
к Регламенту использования электронной
цифровой подписи в Системе электронного
документооборота ООО «Спектр Инвест»

ЗАЯВЛЕНИЕ
на формирование ключей электронной подписи

число месяц год

Клиент (Наименование/ФИО):
ИНН:

ФИО и паспортные данные лица, которому будет выдан Сертификат ключа подписи

№/Дата/Код договора:

Прошу сформировать

- первично
- повторно

мне ключи электронной подписи и сертификат ключа подписи.

Подпись _____ / _____ /

Приложение 2
к Регламенту использования электронной
цифровой подписи в Системе электронного
документооборота ООО «Спектр Инвест»

АКТ
Приема-передачи сейф-пакета

г. Москва

число месяц год

Общество с ограниченной ответственностью «Спектр Инвест», именуемое далее «Оператор Удостоверяющего центра», в лице Генерального директора _____, действующего на основании Устава, с одной стороны, и _____, именуемое далее «Участник Системы ЭДО», в лице _____, действующего на основании _____, с другой стороны, вместе именуемые «Стороны», составили настоящий Акт приема-передачи сейф-пакета (Далее – Акт).

1. Оператор Удостоверяющего центра передает, а Участник Системы ЭДО принимает сейф-пакет, содержащий:

- сертификаты ключей электронной подписи;
- ключи электронной подписи;
- программное обеспечение, в т.ч. средства криптографической защиты;

2. Участник Системы ЭДО подтверждает, что сейф-пакет не имеет видимых повреждений и следов вскрытия, либо иного воздействия.

3. Настоящий Акт составлен в 2 (двух) экземплярах, по одному для каждой из Сторон.

ПОДПИСИ СТОРОН

Оператор Удостоверяющего центра:

Участник Системы ЭДО

Генеральный директор

_____/_____/_____/_____/

Приложение 3
к Регламенту использования электронной
цифровой подписи в Системе электронного
документооборота ООО «Спектр Инвест»

РАСХОДЫ
НА СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ И ОБОРУДОВАНИЕ
(Одно рабочее место клиента)

1. Расходы/Регистрация нового клиента

Лицензия на использование криптопровайдера «Signal-COM CSP v.2.x» на одном рабочем месте с записанным ключом и сертификатом в руб.	4700-00	Без НДС
Носитель Rutoken 32Кб в руб.	750-00	В т.ч. НДС
Сейф-пакет с услугой по его комплектации в руб.	400-00	В т.ч. НДС
ИТОГО:	5 850-00	

Примечание: Обновление ключей и сертификатов производится ежегодно по отдельным счетам.

2. Обновление по истечении сроков действия (через год)

Обновление ключей и сертификатов	3500-00	В т.ч. НДС
Сейф-пакет с услугой по его комплектации в руб.	400-00	В т.ч. НДС
ИТОГО:	3 900-00	

В соответствии с подпунктом 26 пункта 2 статьи 149 Налогового кодекса РФ вознаграждение за использование программного обеспечения НДС не облагается.