

ПРИЛОЖЕНИЕ

К Приказу № П-14 ООО «РОЛИС»

К Приказу № 274 ЗАО «ПКТ»

**ПРАВИЛА**

**ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА  
КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «КОНТЕРРА»**

	<b>ПРАВИЛА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «КОНТЕРРА»</b>	<b>Страница 2</b>
--	--	-------------------

## **Термины и общие положения**

Для целей настоящих Правил, используются следующие термины и определения:

**Система «КОНТЕРРА»** (далее Система) – корпоративная информационная система, представляющая собой совокупность программного, информационного и аппаратного обеспечения, обеспечивающая обмен электронными документами и электронными сообщениями в соответствии с настоящими Правилами.

**Удостоверяющий центр** – ООО «Крипто-Про», выполняющее функции Удостоверяющего центра в соответствии с Законом об электронной цифровой подписи от 10 февраля 2002 г и действующее на основании лицензий Центра ФСБ по лицензированию, сертификации и защите государственной тайны №№ 6386П, 6387Х, 6388Р, 6389У от 30 ноября 2008 г.

**Электронная цифровая подпись** - реквизит электронного документа, предназначенный для защиты 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 утраты, добавления, перестановки или искажения содержащейся в электронном документе информации.

**Организатор** – ООО «Российские логистические информационные системы» (ИНН 7805353227), являющееся лицензиатом Системы и выполняющее функции уполномоченного представителя Удостоверяющего центра, заключившее с Удостоверяющим центром договор на предоставление услуг по изготовлению сертификатов ключей подписей и уполномоченное Удостоверяющим центром осуществлять регистрацию и управление сертификатами ключей подписей.

**Оператор** – юридическое лицо, являющееся лицензиатом Системы и использующее Систему для технологического, информационного и документального обслуживания Клиентов.

**Клиент** – юридическое лицо, условиями договорных отношений которого закреплено полное и безусловное признание настоящих Правил и их неотъемлемых частей.

**Участник** – Оператор или Клиент, участвующий в электронном документообороте в соответствии с настоящими Правилами.

**Электронное сообщение** – логически целостная совокупность структурированных данных, имеющих смысл для участников информационного взаимодействия. Информация в электронном сообщении представлена в электронно-цифровой форме, позволяющей обеспечить ее обработку средствами вычислительной техники, передачу по каналам связи и хранение на машиночитаемых носителях информации.

**Электронный документ** – электронное сообщение, заверенное электронной цифровой подписью.

**Электронный документооборот** – обмен электронными документами/сообщениями в Системе в соответствии с настоящими Правилами.

**Доставка электронного документа/сообщения** – процесс пересылки электронного документа/сообщения между Участниками.

**Подтверждение подлинности электронной цифровой подписи в электронном документе** - положительный результат проверки принадлежности электронной цифровой подписи в электронном документе Участнику и отсутствия искажений в данном электронном документе.

**Уполномоченное лицо** – сотрудник или иной представитель Участника, действующий от его имени на основании Устава, договора, доверенности на право совершения соответствующих операций.

Настоящее Приложение № 1 к Правилам утверждены Приказом Генерального директора ООО «РОЛИС» №П-14 от 16.12.2009г., Приказом Генерального директора ЗАО «ПКТ» №274 от 16.12.2009 г.

	<b>ПРАВИЛА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «КОНТЕРРА»</b>	<b>Страница 3</b>
--	--	-------------------

**Владелец сертификата ключа подписи** – уполномоченное лицо, на имя которого Организатором выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронно-цифровой подписи, позволяющим создавать электронную цифровую подпись в электронных документах.

**Средства криптографической защиты информации (СКЗИ)** – аппаратные и(или) программные средства, обеспечивающие применение ЭЦП и шифрования при организации электронного документооборота. СКЗИ могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.

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

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

**Сертификат ключа подписи** - электронный документ, доступный любому Участнику, включающий в себя открытый ключ электронной цифровой подписи владельца сертификата ключа подписи.

**Компрометация ключа** – констатация владельцем сертификата ключа подписи обстоятельств, при которых возможно несанкционированное использование закрытого ключа другими лицами.

#### **Общие положения**

- 1.1. Настоящие Правила определяют нормы и принципы электронного документооборота в корпоративной информационной системе в рамках исполнения обязательств между Участниками.
- 1.2. Организатор обеспечивает доставку электронных документов/сообщений между Участниками путем обеспечения функционирования Системы и предоставления доступа к Системе Участникам.
- 1.3. Участники признают электронные документы, переданные в рамках настоящих Правил, имеющими равную силу с аналогичными бумажными документами в случае соблюдения процедур и форматов, предусмотренными настоящими Правилами. В рамках Системы Участники применяют СКЗИ, использующую алгоритмы криптования, рекомендованные стандартами ГОСТ Р34.10-94, ГОСТ Р34.10-2001, ГОСТ Р34.11-94 и обеспечивающую контроль авторства и юридической значимости электронного документа. Для подписания электронных документов используется криптографическая библиотека Crypto-Pro CSP версии 3.0 или более поздней.
- 1.4. Любой электронный документ, направленный Клиентом Оператору за подписью уполномоченного лица, подтверждает полное согласие отправителя электронного документа с правилами, технологическими схемами и иными нормативными документами, регламентирующими работу Оператора и опубликованными на интернет-сайте Оператора. Участник осуществляет самостоятельное ознакомление с перечисленными документами и контроль возможных изменений в соответствии с правилами, установленными Оператором.

#### **Порядок и условия допуска Участников к осуществлению электронного документооборота**

- 1.5. Участник допускается к осуществлению электронного документооборота после установки необходимых аппаратных средств и программного обеспечения для доступа к Системе. Для Участников, являющихся отправителями электронных документов, необходимо исполнение следующих условий:
  - 1.5.1. Создание открытого и закрытого ключей, а при необходимости открытого и закрытого ключей шифрования и получение у Организатора сертификата ключа подписи;

	<b>ПРАВИЛА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «КОНТЕРРА»</b>	<b>Страница 4</b>
--	--	-------------------

- 1.5.2. Регистрация сертификатов ключей подписи и при необходимости сертификатов ключей шифрования Организатором, действующим по поручению получателя электронных документов.

#### **Электронный документ**

- 1.6. Электронный документ, используемый в Системе, считается надлежащим образом оформленным при условии его соответствия законодательству Российской Федерации и настоящим Правилам.
- 1.7. Электронный документ должен быть сформирован в формате, предусмотренном текущей технологией Системы на момент формирования электронного документа.
- 1.8. Электронный документ считается подписанным Участником, если он заверен электронной цифровой подписью, сертификат ключа которой закреплен за Уполномоченным представителем Участника.
- 1.9. Электронная цифровая подпись в электронном документе, сертификат ключа подписи которой зарегистрирован за юридическим лицом, признается равнозначной собственноручной подписи уполномоченного лица этого юридического лица в документе на бумажном носителе, заверенном печатью.
- 1.10. Подтверждением получения электронного документа является присвоение ему в Системе статуса «Оформлен», устанавливаемого после выполнения необходимых проверок электронного документа.
- 1.11. В случае, если Правилами предусмотрена необходимость подписания электронного документа электронными цифровыми подписями нескольких лиц, то электронный документ признается таковым только при условии наличия всех необходимых подписей.
- 1.12. Копии электронного документа могут быть изготовлены (распечатаны) на бумажном носителе и должны быть заверены собственноручной подписью уполномоченного лица Оператора или Участника, являющимся отправителем или получателем электронного документа.
- 1.13. Копии электронного документа на бумажном носителе должны соответствовать требованиям действующего законодательства, а также содержать обязательную отметку "Копия Электронного Документа".

#### **Организация электронного документооборота**

##### **Электронный документооборот**

- 1.14. Электронный документооборот может включать:
- 1.14.1. формирование электронного документа;
  - 1.14.2. отправку и доставку электронного документа;
  - 1.14.3. проверку электронного документа;
  - 1.14.4. подтверждение получения электронного документа;
  - 1.14.5. учет электронных документов (регистрацию входящих и исходящих ЭД);
  - 1.14.6. хранение электронных документов (ведение архивов ЭД);
  - 1.14.7. создание дополнительных экземпляров электронного документа;
  - 1.14.8. создание бумажных копий электронного документа.

##### **Формирование электронного документа**

- 1.15. Формирование электронного документа осуществляется в следующем порядке:
- 1.15.1. формирование электронного сообщения в формате, установленном для данного электронного документа.
  - 1.15.2. подписание сформированного электронного сообщения электронной цифровой подписью. Подписание электронного документа осуществляется отправителем электронного документа с применением средств криптографической защиты информации, предусмотренных настоящими Правилами.
  - 1.15.3. Электронный документ считается подписанным владельцем сертификата ключа подписи в случае подтверждения подлинности электронной цифровой подписи в электронном документе.

##### **Отправка и доставка электронного документа**

- 1.16. После создания электронный документ направляется отправителем получателю с использованием средств, предоставленных Системой. Отправитель обязан явно указать

	<b>ПРАВИЛА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «КОНТЕРРА»</b>	<b>Страница 5</b>
--	--	-------------------

получателя электронного документа путем указания его идентификатора. Идентификатором являются наименование, ИНН или иной уникальный признак, позволяющий определить получателя сообщения.

1.17. В случае, если Договором между Клиентом и Оператором предусмотрена проверка подлинности документа либо его отдельных реквизитов на предмет соответствия условиям, налагаемым Участником, Организатор выполняет процедуру проверки и создает электронный документ, отражающий результаты этой процедуры и подписанный электронной цифровой подписью уполномоченного лица Организатора. Формат данного документа и порядок его передачи Оператору определяется Договором между Оператором и Организатором.

1.18. Организатор имеет право приостановить работу Системы, с уведомлением Участников не менее чем за 3 рабочих дня, в моменты времени, в которые вступают в силу новые/измененные форматы электронных документов (электронных сообщений) с целью исключить возможность неоднозначной интерпретации сообщений отправителем и получателем из-за изменения требований в период доставки сообщения.

#### **Проверка и подтверждение подлинности доставленного электронного документа**

1.19. Проверка подлинности электронного документа осуществляется получателем документа с применением СКЗИ, предусмотренной к использованию настоящими Правилами.

1.20. Проверка электронного документа включает:

1.20.1. проверку электронного документа на соответствие установленного для него формата;

1.20.2. проверку подлинности всех электронных цифровых подписей электронного документа.

1.21. В случае положительного результата проверки электронного документа Система присваивает данному документу статус «Оформлен».

#### **Хранение электронных документов**

1.22. Обязанность по хранению электронных документов возлагается на Организатора.

1.23. Все электронные документы должны храниться в течение сроков, установленных законодательством РФ, отраслевыми нормами и правилами или традициям документооборота для соответствующего типа документов, а при их отсутствии - правилами, установленными Оператором.

1.24. Электронные документы должны храниться в том же формате, в котором они были сформированы, отправлены или получены.

### **Система обеспечения информационной безопасности**

#### **Средства обеспечения информационной безопасности**

1.25. Соблюдение требований информационной безопасности при организации электронного документооборота обеспечивает:

1.25.1. конфиденциальность информации (расшифровать информацию могут только уполномоченные лица);

1.25.2. целостность передаваемой информации (гарантирование, что данные передаются без искажений и исключается возможность подмены информации);

1.25.3. аутентичность информации (отправителем информации является именно тот, от чьего имени она отправлена).

1.26. Требования по информационной безопасности при организации электронного документооборота реализуются посредством применения программно-технических средств и организационных мер.

1.27. Участники применяют следующие программно-технические средства и предпринимают организационные меры, необходимые для обеспечения безопасности:

1.27.1. лицензированные программные средства, предусмотренные в п. 1.3 настоящих Правил;

1.27.2. систему паролей и идентификаторов для ограничения доступа пользователей и операторов к техническим и программным средствам системы электронного документооборота;

1.27.3. программно-аппаратные средства защиты от несанкционированного доступа;

1.27.4. средства защиты от программных вирусов и атак;

	<b>ПРАВИЛА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «КОНТЕРРА»</b>	<b>Страница 6</b>
--	--	-------------------

- 1.27.5. соблюдение режима использования паролей и идентификаторов владельцем сертификата ключа подписи, определяемого самим Участником.

#### **Порядок разрешения конфликтных ситуаций, возникших в связи с осуществлением электронного документооборота в Системе**

##### **Возникновение конфликтных ситуаций в связи с осуществлением электронного документооборота в Системе**

- 1.28. В связи с осуществлением электронного документооборота возможно возникновение конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения электронных документов, а также использованием в данных документах электронной цифровой подписи. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:
- 1.28.1. Неподтверждение подлинности электронных документов средствами проверки электронной цифровой подписи принимающей стороны;
  - 1.28.2. Заявление Участника об искажении электронного документа;
  - 1.28.3. Иные случаи возникновения конфликтных ситуаций, связанных с функционированием Системы.

##### **Уведомление и предварительный разбор конфликтной ситуации**

- 1.29. В случае возникновения конфликтной ситуации Участник, предполагающий возникновение конфликтной ситуации, должен незамедлительно направить уведомление о конфликтной ситуации Организатору и при необходимости иному Участнику.
- 1.30. Уведомление должно содержать информацию о существовании конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии конфликтной ситуации, реквизиты электронного документа, а также фамилию, имя, отчество, должность, контактные телефоны, факс, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации.
- 1.31. Уведомление о наличии конфликтной ситуации составляется в письменной форме и направляется способом, обеспечивающим подтверждение вручения корреспонденции адресату.
- 1.32. Организатор обязан не позднее чем в течение трех рабочих дней с момента получения уведомления провести предварительный разбор конфликтной ситуации и направить уведомителю информацию о результатах разбора.
- 1.33. В случае если уведомитель не удовлетворен информацией, полученной от Организатора, уведомитель в течение трех рабочих дней направляет Организатору и при необходимости иным Участникам требование о формировании согласительной комиссии.

##### **Формирование и полномочия согласительной комиссии**

- 1.34. Согласительная комиссия формируется Организатором в течение 5 рабочих дней.
- 1.35. В состав согласительной комиссии входит равное количество, но не менее чем по одному уполномоченному представителю каждой из конфликтующих сторон и представитель Организатора.
- 1.36. Право представлять в комиссии Участника и Организатора должно подтверждаться доверенностью, выданной представителю на срок работы комиссии.
- 1.37. По инициативе любой из сторон к работе комиссии для проведения технической экспертизы могут привлекаться независимые эксперты без права голоса. Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.
- 1.38. Работа согласительной комиссии осуществляется по месту нахождения Организатора.
- 1.39. Участники обязаны предоставлять по запросу согласительной комиссии все имеющиеся сертификаты открытых ключей и сведения о действиях по аннулированию и приостановке действия сертификатов если они имели место, а также электронные документы, являющиеся предметом спора.
- 1.40. В случае, если Согласительная комиссия не приходит к единому мнению относительно подтверждения подлинности электронной цифровой подписи в электронном документе, Стороны обращаются в Удостоверяющий центр, оказывающий услугу по разбору конфликтных ситуаций. Согласительная комиссия передает в Удостоверяющий центр документы, необходимые для разбора конфликтной ситуации. Оплату услуг Удостоверяющего центра по разбору конфликтной ситуации осуществляет сторона, подавшая требование о формировании согласительной комиссии.

	<b>ПРАВИЛА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «КОНТЕРА»</b>	<b>Страница 7</b>
--	---	-------------------

- 1.41. Решение Удостоверяющего центра относительно подлинности электронного документа является обязательным для признания Участниками.
- 1.42. Если устанавливается обоснованность претензии стороны – инициатора разбора, затраты на разбор конфликтной ситуации силами Удостоверяющего центра возмещаются стороной, допустившей нарушение. Иные расходы сторон по обеспечению работы согласительной комиссии не возмещаются.

**Акт по итогам работы согласительной комиссии**

- 1.43. По итогам работы согласительной комиссии, но не позднее, чем 30 календарных дней с момента ее формирования, составляется Акт, в котором содержатся следующие данные:
  - 1.43.1. состав комиссии;
  - 1.43.2. дата и место составления Акта;
  - 1.43.3. даты и время начала и окончания работы комиссии;
  - 1.43.4. краткий перечень мероприятий, проведенных комиссией;
  - 1.43.5. выводы, к которым пришла комиссия в результате проведенных мероприятий;
  - 1.43.6. подписи членов комиссии;
  - 1.43.7. указание на особое мнение члена (или членов комиссии), в случае наличия такового.
- 1.44. Акт составляется по одному экземпляру для каждого из Участников и Организатора. Особое мнение составляется в произвольной форме в таком же количестве экземпляров, что и Акт.

**Порядок внесения изменений в настоящие Правила**

- 1.45. Действующие Правила размещаются по адресу <http://www.container.ru> в формате Adobe Acrobat (PDF).
- 1.46. В случае изменения настоящих Правил Организатор публикует уведомление о предстоящем изменении и вновь вводимую редакцию не позднее чем за 30 дней до введения в действие новой редакции. Уведомление и новая редакция размещается в информационной части Системы по адресу: [www.container.ru](http://www.container.ru).
- 1.47. В случае, если Участник не может использовать для работы электронную версию Правил, он обязан самостоятельно связаться с Организатором и получить Правила и информацию о возможных изменениях в бумажном виде. Указанные в настоящем пункте документы должны быть направлены Участнику в течение 5 дней после получения соответствующего запроса Участника.

**Перечень приложений**

- 1.48. К настоящим Правилам прилагаются и являются их неотъемлемой частью:
  - 1.48.1. Приложение № 1. «Спецификация электронных документов и электронных сообщений, поддерживаемых Оператором ЗАО «ПКТ».

	<b>ПРАВИЛА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «КОНТЕРРА»</b>	<b>Страница 8</b>
--	--	-------------------

**Приложение № 1. Спецификация электронных документов и электронных сообщений, поддерживаемых Оператором ЗАО «ПКТ»**

Электронные документы/сообщения принимаются и отправляются Оператором в форматах UN EDIFACT, XML либо с помощью интерфейсов Системы. В качестве транспорта доставки сообщений UN EDIFACT и XML используется электронная почта.  
ЗАО «ПКТ» принимает и отправляет электронные документы/сообщения, перечисленные в приведенной ниже таблице:

Данные	Отправитель	Получатель	Доступные форматы обмена	Электронная цифровая подпись
Импортный грузовой манифест (коносаменты)	Линия /Агент	Терминал	EDIFACT CUSCAR v.D95/96B Manifest xml	Не требуется
План размещения контейнеров на судне			EDIFACT BAPLIE v.D95B	Не требуется
Выгрузка, включая транзитные контейнеры погрузка предварительный план	Линия /Агент	Терминал		
Погрузка окончательный план	Терминал	Линия /Агент		
Список выгрузки прибывающего судна с указанием предварительных данных о вывозе контейнеров	Линия /Агент	Терминал	EDIFACT COPRAR v.D95B DischargeList XML	Не требуется
Список погрузки на судно	Линия /Агент	Терминал	EDIFACT COPRAR v.D95B	Не требуется
Инструкции по обработке судна	Линия /Агент	Терминал	EDIFACT MOVINS v.D95B	Не требуется
Отчет о выгрузке/погрузке с местоположением	Терминал	Линия/Агент	EDIFACT COARRI v.D95B	Не требуется
Релиз-ордер	Агент	Терминал	EDIFACT COREOR v.D00B Release order XML	Требуется
Расписка о получении Релиз-ордера	Экспедитор	Агент	TXT	Требуется
Доверенность на получение импортного контейнера	Экспедитор	Терминал	TXT	Требуется
Подтверждение отгрузки/доставки контейнеров автомобильным или ж/д транспортом	Терминал	Линия/Агент	EDIFACT CODECO v.D95B	Не требуется
ДУ	Терминал	Агент	<a href="#">XML</a>	Не требуется
Уведомление о досмотре	Терминал	Агент	XML	Не требуется
Уведомление о взвешивании	Терминал	Агент	XML	Не требуется
Приемные акты	Терминал	Агент	<a href="#">XML</a>	Не требуется
Букинг на экспортные контейнеры	Агент	Терминал	EDIFACT COPARN v.D95B Booking XML	Не требуется
Результат обработки входящих сообщений	Терминал	Отправитель сообщения	EDIFACT APERAK v.D95B	Не требуется

Описание форматов электронных документов/сообщений приведено на официальном сайте Оператора ЗАО «ПКТ» (<http://www.fct.ru>) в разделе «Электронный обмен данными». Сообщения, требующие наличия электронной цифровой подписи, обрабатываются Оператором только при соблюдении требований, предусмотренных Правилами.