Приложение № 1

К Соглашению о сотрудничестве от «01» июля 2010 г.

«СОГЛАСОВАНО»
Генеральный директор
ЗАО «ПЕТЕРБУРГРЕГИОНГАЗ»

В.З. Казаченков.

_____ 2010 г.

«УТВЕРЖДАЮ»
Зам. генерального директора
ООО «Газинформсервис»
»

В.Н. Кустов

_____ 2010 г.

РЕГЛАМЕНТ

использования автоматизированной системы установления доверительных отношений (АСУДО)

Санкт-Петербург

2010 г.

Юридический отдел

1. ВВЕДЕНИЕ

1.1. Регламент использования автоматизированной системы установления доверительных отношений (далее Регламент) разработан на основании действующего законодательства Российской Федерации, а также учредительных и иных документов Организатора Системы и определяет:

- Область применения автоматизированной системы использования открытых каналов связи для подготовки, формирования и передачи юридически значимых электронных документов, а также контролируемого и ограниченного доступа к информации - «Автоматизированная система установления доверительных отношений - АСУДО» (далее – Система).
- Порядок применения криптографической защиты информации при взаимодействии Участников в рамках Системы.
- Порядок регистрации и подключения Участников к Системе.
- Порядок использования Системы Участником.

1.2. Организатором Системы является ЗАО «ПЕТЕРБУРГРЕГИОНГАЗ». Деятельность по обслуживанию средств, предназначенных для криптографической защиты конфиденциальной информации, передаваемой в рамках Системы, а также выполнение функций Удостоверяющего Центра в рамках Системы выполняется ООО «Газинформсервис»_» (далее – Удостоверяющий Центр) в соответствии с Соглашением о сотрудничестве между ЗАО «ПЕТЕРБУРГРЕГИОНГАЗ» и ООО «Газинформсервис» от «____» _____2010г. и обеспечена соответствующими лицензиями.

1.3. Область применения Системы:

1.3.1. Область применения Системы на момент ввода ее в действие ограничивается передачей подписанных ЭЦП информационных сообщений между Участниками Системы.

1.3.2. Область применения Системы изменяется документом – уведомлением об изменении области применения – выпускаемым Организатором Системы и согласованным с Удостоверяющим Центром.

1.3.3. В случае расширения области применения Системы за счет ввода нового раздела в указанном документе описываются особенности использования Системы в этом разделе, а также регламентируется деятельность и ответственность Участников при использовании Системы в рамках этого раздела.

1.3.4. Все документы, изменяющие область применения Системы, становятся неотъемлемой частью настоящего Регламента.

1.3.5. Разделы области применения Системы могут быть:

- общедоступными для всех участников Системы;
- специальными, в случае выполнения участником специализированных функций в рамках раздела Системы.

1.3.6. В рамках раздела области применения Системы доступ к информации может быть:

- общим для всех Участников Системы;
- разграничен между Участниками Системы по принадлежности этой информации.

1.4. Участники используют для защиты представленной в электронном виде информации, передаваемой с помощью Системы, сертифицированные в порядке, установленном законодательством Российской Федерации, средства электронной цифровой подписи (далее – ЭЦП), позволяющие идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации.

1.5. Участники используют для защиты информации при передаче ее по открытым каналам связи в рамках Системы сертифицированные в порядке, установленном законодательством Российской Федерации, средства криптографической защиты информации (далее – СКЗИ).

1.6. Используемые во взаимоотношениях между Участниками Системы электронные документы, заверенные ЭЦП, являются оригиналами, имеют юридическую силу, подлежат хранению в хранилище юридически значимых документов и могут использоваться в качестве доказательств в суде, а также при рассмотрении споров в досудебном порядке.

Примечание: Если Пользователь с целью контроля самостоятельно или по согласованию с Организатором системы копирует информацию, представленную в электронном виде по каналам связи, на бумажный носитель, то на первом листе бумажной копии следует отметить, что оригинал был отправлен в электронном виде, и указать реквизиты электронного документа-оригинала, заверив подписью уполномоченного лица Пользователя и печатью.

1.7. Участник Системы признает, что использование в Системе сертифицированных СКЗИ, которые реализуют ЭЦП и шифрование, достаточно для обеспечения конфиденциальности информационного взаимодействия Пользователей и/или конфиденциальности информации, переданной в рамках Системы, а также подтверждения того:

- что электронный документ исходит от Пользователя (подтверждение авторства документа);
- что электронный документ не претерпел изменений с момента подписи его Пользователем с помощью ЭЦП (подтверждение целостности и подлинности документа);
- что информация, переданная в рамках Системы от Организатора Системы, не претерпела изменений (подтверждение целостности и подлинности информации).

1.8. Регламент начинает действовать в отношении Участника с момента заключения им Договора с Удостоверяющим Центром или с Уполномоченной Организацией Удостоверяющего Центра и согласования Организатором Системы Заявки Участника на присоединение к Системе.

1.9. При обмене электронными документами в Системе и/или получении информации в рамках Системы Участники должны руководствоваться положениями настоящего Регламента и Регламента удостоверяющего центра (далее Регламент УЦ), публикация которого осуществляется на портале http://www.gaz-is.ru/repository/cps.pdf.

2. ТЕРМИНЫ И СОКРАЩЕНИЯ, ИСПОЛЬЗУЕМЫЕ В РЕГЛАМЕНТЕ

Автоматизированная система использования открытых каналов связи для подготовки, формирования и передачи юридически значимых электронных документов, а также контролируемого и ограниченного доступа к информации (Система) - комплекс организационных и технических мероприятий, включающий регламенты, соглашения и другие документы, определяющие порядок и правила обмена юридически значимыми электронными документами, а также предоставления доступа к информации Организатора Системы, порядок и правила применения электронной цифровой подписи, а также технические средства, включая аппаратное и программное обеспечение, необходимое для применения электронной цифровой подписи и/или шифрования данных, и документы, определяющие порядок их применения.

Автоматизированная система установления доверительных отношений – см. «Автоматизированная система использования открытых каналов связи для подготовки, формирования и передачи юридически значимых электронных документов, а также контролируемого и ограниченного доступа к информации».

АСУДО - см. «Автоматизированная система использования открытых каналов связи для подготовки, формирования и передачи юридически значимых электронных документов, а также контролируемого и ограниченного доступа к информации».

Владелец сертификата ключа подписи – см. Регламент УЦ.

Договор – Договор, заключенный между Участником и Удостоверяющим Центром. Договор определяет состав, порядок исполнения и стоимость услуг, оказываемых Участнику Удостоверяющим Центром.

Заявка – Заявка Участника на присоединение к Системе.

Закрытый (секретный) ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи и/или получения контролируемого и ограниченного доступа к информации. Закрытые ключи хранятся Пользователями Системы в тайне. Закрытые ключи используются для формирования ЭЦП Пользователя и шифрования.

Ключевой носитель – отчуждаемый носитель (дискета, eToken, ruToken и т.п.), содержащий один или несколько ключей.

Компрометация ключа - утрата доверия к тому, что используемые закрытые ключи недоступны посторонним лицам. К событиям, связанным с компрометацией ключей, относятся, включая, но, не ограничиваясь, следующие:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевым носителям;
- возникновение подозрений на утечку информации или ее искажение в Системе;
- нарушение целостности печатей на сейфах с ключевыми носителями, если используется процедура опечатывания;
- утрата ключей от сейфов (помещений) в момент нахождения в них ключевых носителей;
- утрата ключей от сейфов (помещений) в момент нахождения в них ключевых носителей с последующим обнаружением;
- доступ посторонних лиц к ключевой информации.
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе, когда ключевой носитель вышел из строя и не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, а также настоящим Регламентом, и требующая защиты.

Конфликтная ситуация - ситуация, при которой у пользователей Системы возникает необходимость разрешить вопросы признания или непризнания авторства и/или подлинности электронных документов, обработанных средствами криптографической защиты информации.

Ключ (криптографический ключ) – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразования.

Несанкционированный доступ (НСД) к информации - доступ к информации, нарушающий установленные правила ее получения.

Организатор Системы – ЗАО «ПЕТЕРБУРГРЕГИОНГАЗ».

Открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю Системы и предназначенная для подтверждения с использованием

средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе. Открытый ключ Пользователя является действующим на момент подписания, если он зарегистрирован (сертифицирован) и введен в действие.

Открытый ключ шифрования – криптографический ключ, предназначенный для шифрования разового (сеансового) ключа шифрования с целью его передачи адресату по открытым каналам связи. Открытые ключи шифрования могут быть известны всем пользователям Системы.

Подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством ЭЦП 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 – сотрудник организации Участника или Организатора Системы, владелец сертификата ключа подписи.

Сертификат ключа подписи (сертификат открытого ключа) - документ на бумажном носителе или электронный документ с ЭЦП уполномоченного лица Удостоверяющего Центра, которые включают в себя открытый ключ (ЭЦП и/или шифрования) и которые выдаются Удостоверяющим Центром участнику информационной системы для подтверждения подлинности открытого ключа и идентификации владельца сертификата ключа подписи.

СОС (Список отозванных сертификатов, Certificate Revocation List, CRL) – см. Регламент УЦ.

Средства криптографической защиты информации – средства вычислительной техники, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности.

Средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи 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[1] – информационная система ООО «Газинформсервис», обеспечивающая сертификацию открытых ключей пользователей Системы и выполняющая иные функции, предусмотренные Федеральным законом от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи».

Управление ключами - создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учет и применение, а также издание, приостановление и аннулирование сертификатов открытых ключей в соответствии с Регламентом УЦ.

Участник Системы (Участник) – юридическое лицо, подавшее в установленном порядке заявку на присоединение к Системе и получившее согласование от Организатора Системы, а также подписавшее договор с ООО «Газинформсервис» на услуги Удостоверяющего центра.

Целостность информации – способность автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

Электронная цифровая подпись – реквизит электронного документа, предназначенный

---

[1] Когда речь идет об информационной системе, второе слово в словосочетании Удостоверяющий центр пишется с маленькой буквы. В случае, если упоминается организация, исполняющая роль Удостоверяющего Центра системы – оба слова пишутся с большой буквы.

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. В соответствии с ФЗ «Об ЭЦП» признается аналогом собственноручной подписи.

ЭЦП – см. Электронная цифровая подпись

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Участники Системы осуществляют обмен электронными документами и/или получают доступ к информации, предоставляемой Организатором Системы, по открытым каналам связи.

3.2. Пользователи соблюдают установленную в соответствии с требованиями документа «КриптоПро CSP. Правила пользования» (поставляется в электронном виде) последовательность действий при обмене электронными документами и проверке их подлинности и/или получении доступа к информации, предоставляемой Организатором Системы.

3.3. Удостоверяющий Центр осуществляет работы по управлению ключами в соответствии с требованиями Федерального Закона «Об электронной цифровой подписи» и регламентом УЦ.

3.4. В случае нарушения правил использования СКЗИ и/или возникновения конфликтных ситуаций, связанных с подтверждением авторства и/или подлинности электронных документов, заверенных ЭЦП, или иных конфликтных ситуаций, связанных с использованием ЭЦП, Стороны руководствуются Регламентом УЦ.

4. ПОРЯДОК РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМЕ. ПОРЯДОК ПОЛУЧЕНИЯ СКЗИ, КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТОВ

4.1. Участник Системы самостоятельно заключает Договор с Удостоверяющим Центром и за свой счет производит оплату Программного обеспечения, услуг по выпуску и обслуживанию сертификата.

4.2. Удостоверяющий Центр выполняет комплекс работ по регистрации Пользователей Участника в соответствии с Регламентом УЦ.

5. ФУНКЦИИ И ЗАДАЧИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

5.1. Удостоверяющий Центр предоставляет Участникам Системы услуги в соответствии с положениями ФЗ от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи» и Регламентом УЦ.

5.2. Удостоверяющий Центр уведомляет Участников Системы о фактах, которые стали ему известны и которые существенным образом могут сказаться на возможности дальнейшего использования СКЗИ и сертификата ключа.

5.3. Удостоверяющий Центр участвует в работе Экспертной комиссии при рассмотрении спорных вопросов (конфликтных ситуаций).

5.4. Удостоверяющий Центр контролирует правила использования СКЗИ Пользователями Системы.

6. ПРАВА И ОБЯЗАННОСТИ УЧАСТНИКА СИСТЕМЫ

6.1. Участник Системы, в соответствии с Договором, лицензионным соглашением и эксплуатационной документацией на СКЗИ, самостоятельно и за свой счет подготавливает и содержит в рабочем состоянии ПЭВМ и программное обеспечение, предназначенные для работы в Системе. Пользователю рекомендуется не использовать средства разработки и отладки программ на ПЭВМ, на которой установлено СКЗИ.

6.2. Участник Системы обязан самостоятельно и за свой счет организовать режим функционирования рабочих мест таким образом, чтобы исключить возможность доступа к СКЗИ, несанкционированной модификации или использования СКЗИ лицами, не имеющими допуска к работе с СКЗИ, а также исключить возможность использования криптографических ключей не уполномоченными на то лицами.

6.3. Участник Системы обязан самостоятельно и за свой счет обеспечить осуществление Пользователями при обработке электронных документов их архивирование и хранение этих архивов в течение срока, установленного соответствующими законами и нормативными актами для хранения бумажных документов.

6.4. Участник Системы обязан при разрешении конфликтных ситуаций, связанных с установлением подлинности и/или авторства спорного документа или иных конфликтных ситуаций, связанных с использованием ЭЦП, предоставлять Экспертной комиссии, создаваемой и действующей в соответствии с Регламентом УЦ, все документы и материалы, относящиеся к предмету конфликтной ситуации.

6.5. Участник Системы самостоятельно и за свой счет производит замену сертификатов своих Пользователей в соответствии с Регламентом УЦ.

6.6. Участник Системы принимает решение о сроках и порядке архивного хранения или об уничтожении старых ключей и соответствующих сертификатов, так как все риски, связанные с несанкционированным использованием старых ключей, ложатся на Пользователя.

Факт уничтожения или сохранения старых ключей оформляется Актом, который заверяется подписями владельца старого ключа, руководителя организации - Участника Системы и печатью организации. 2-й экземпляр данного документа передается в Удостоверяющий Центр.

Примечание: В случае уничтожения старых ключей – перед уничтожением старых ключей необходимо расшифровать все электронные документы, зашифрованные с их использованием, иначе в дальнейшем прочитать эти документы будет невозможно!

6.7. Участник Системы самостоятельно и за свой счет обеспечивает хранение расшифрованных документов в электронном виде в соответствии с требованиями, установленными законодательством и настоящим Регламентом.

6.8. Участник Системы имеет право:

- не принимать к исполнению электронные документы, заверенные ЭЦП, если:
  - сертификат ключа подписи отправителя утратил силу (не действует, находится в СОС) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

Примечание: перед принятием решения по исполнению полученного электронного документа, в зависимости от его важности, Пользователь самостоятельно определяет необходимость проверки нахождения сертификата ЭЦП отправителя в СОС.

  - не подтверждена подлинность ЭЦП в электронном документе;
  - ЭЦП используется не в соответствии со сведениями, указанными в сертификате ключа подписи.

- запрашивать подтверждение по полученным им электронным документам в случае возникновения сомнений;
- требовать от Удостоверяющего Центра аннулирования сертификата открытого ключа Пользователя в случае наступления событий, трактуемых как компрометация ключевой информации;
- требовать исполнения обязательств от других Участников Системы по принятым ими электронным документам;
- в случае возникновения конфликтной ситуации, связанной с установлением подлинности и/или авторства спорного документа, требовать разрешения указанных вопросов Экспертной комиссией в соответствии с согласованным порядком.

6.9. Участник Системы имеет право использовать или не использовать в своей деятельности какие-либо общедоступные разделы области применения Системы.

6.10. Участник Системы имеет право в любой момент принять решение об использовании или неиспользовании в своей деятельности каких-либо общедоступных разделов области применения Системы.

6.11. В случае решения об использовании какого-либо общедоступного раздела области применения Системы Участник автоматически соглашается со всеми положениями настоящего Регламента, определяющими деятельность и/или ответственность участника, использующего Систему в рамках этого раздела.

6.12. Об использовании какого-либо общедоступного раздела области применения Системы Участник информирует Организатора Системы передачей информационного сообщения, подписанного ЭЦП Пользователя – сотрудника организации Участника.

6.13. В случае прекращения использования Системы в рамках какого-либо из общедоступных разделов области применения Системы Участник обязан не менее чем за 14 календарных дней известить об этом Организатора Системы посредством информационного сообщения, подписанного ЭЦП Пользователя – сотрудника организации Участника. В случае невозможности передачи электронного информационного сообщения Участник обязан в указанные сроки прислать Организатору Системы письменное уведомление.

6.14. Появление любого нового раздела области применения Системы, в котором Участник не согласен с регламентацией деятельности и/или ответственностью участника, не является причиной отказа от соблюдения положений, определенных настоящим Регламентом в отношении разделов области применения Системы, в рамках которых Участник уже использует Систему.

6.15. Для использования Системы в рамках специального раздела Участник обязан заключить с Организатором Системы отдельный договор на выполнение функций в рамках этого раздела.

6.16. Прекращение использования Системы Участником в рамках специального раздела происходит автоматически при окончании действия договора с Организатором Системы на выполнение функций в рамках этого раздела.

6.17. Участник – инициатор запроса – может получить доступ к информации, предоставляемой Организатором Системы и относящейся к другому Участнику, при официально подтвержденном согласии того Участника открыть эту информацию для Участника – инициатора запроса, и наличии у Организатора Системы технической возможности обеспечить такой доступ.

7. ПРАВА И ОБЯЗАННОСТИ ОРГАНИЗАТОРА СИСТЕМЫ.

7.1. Права и обязанности Организатора Системы соответствуют правам и обязанностям любого другого Участника, но не ограничиваются ими.

7.2. Организатор Системы по согласованию с Удостоверяющим Центром имеет право лишать Участника возможности использовать Систему в рамках раздела, по которому этим Участником не выполняются или выполняются ненадлежащим образом требования Регламента и/или отдельных договоров с Организатором Системы.

7.3. В случае использования в каких-либо разделах области применения Системы специализированного программного обеспечения Организатор Системы обязан обеспечивать его исправное функционирование в соответствии с режимом его работы.

7.4. В случае изменения области применения Системы Организатор Системы обязан не менее, чем за 30 календарных дней уведомить всех Участников об этом изменении. Уведомление осуществляется посредством рассылки в адрес всех Участников Системы информационного сообщения, подписанного ЭЦП Организатора Системы.

Датой отправки уведомления считается дата отправки этого информационного сообщения.

Отсутствие возможности у какого-либо Участника использовать Систему в период отправки информационного сообщения не является причиной оспаривать сроки его уведомления.

7.5. Организатор Системы определяет тип раздела области применения Системы при вводе его в действие.

7.6. Организатор Системы определяет тип доступа к информации, предоставляемой им Участникам в рамках раздела области применения Системы.

7.7. В случае предоставления Организатором Системы в рамках раздела области применения Системы информации, доступ к которой должен быть ограничен конкретным Участником, Организатор Системы обеспечивает такой доступ.

7.8. В случае предоставления Организатором Системы в рамках раздела области применения Системы информации, доступ к которой должен быть разграничен между Участниками по принадлежности этой информации, Организатор Системы обеспечивает такое разграничение.

7.9. Организатор Системы по согласованию с Удостоверяющим Центром имеет право изменить в существующем разделе области применения права и/или обязанности и/или ответственность Организатора Системы, Участника, Удостоверяющего Центра. Такое изменение является изменением области применения Системы.

8. ДЕЙСТВИЯ СТОРОН ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕЙ

8.1. Участник Системы в случае принятия решения о компрометации криптографических ключей Пользователя должен действовать в соответствии с регламентом УЦ.

8.2. При компрометации ключа, Участник должен прекратить обмен электронными документами с другими Участниками и/или прекратить получение информации от Организатора Системы.

8.3. Участник Системы, объявивший о компрометации криптографических ключей Пользователя, самостоятельно и за свой счет в течение одного рабочего дня направляет оригинал Заявки на отзыв сертификата в Удостоверяющий Центр (см. Регламент УЦ).

8.4. В случае, если между Участником и Удостоверяющим Центром заключен Договор, не предусматривающий гарантийного обслуживания, Участник, Пользователь которого допустил компрометацию собственных криптографических ключей, несет все издержки, связанные с сертификацией и вводом в действие новых криптографических ключей.

8.5. В случае, если между Участником и Удостоверяющим Центром заключен Договор, предусматривающий гарантийное обслуживание, сертификация и ввод в действие новых криптографических ключей после события компрометации осуществляется Удостоверяющим Центром в рамках гарантийного обслуживания.

9. КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ

9.1. Удостоверяющий Центр и Участники Системы в процессе работы в Системе обязаны обеспечить сохранность конфиденциальной информации, полученной друг от друга в соответствии с действующим законодательством Российской Федерации.

9.2. Удостоверяющий Центр обязан не разглашать (не публиковать) информацию, полученную от Участников Системы, за исключением регистрационной информации, включенной в изготовленные сертификаты Пользователей.

9.3. Порядок предоставления конфиденциальной информации налоговым, правоохранительным и судебным органам осуществляется в соответствии с действующим законодательством Российской Федерации.

10. ОТВЕТСТВЕННОСТЬ УЧАСТНИКОВ СИСТЕМЫ

10.1. Участник Системы несет ответственность за достоверность сведений, указанных им при оформлении Заявки на присоединение к Системе и договора с Удостоверяющим Центром, а также обязан сообщать обо всех изменениях этих сведений.

10.2. Участник Системы несет ответственность за сохранность и правильность эксплуатации СКЗИ, используемых им для работы с Системой, и закрытых ключей шифрования и ЭЦП его Пользователей, уполномоченных работать с Системой.

10.3. В случае несвоевременного сообщения о факте компрометации ключей Участник Системы, Пользователь которого допустил компрометацию ключей, несет ответственность в полном объеме за ущерб, причиненный им другим Участникам Системы.

10.4. Удостоверяющий Центр не несет ответственности в случае нарушения Участниками Системы и их Пользователями положений настоящего Регламента и Регламента УЦ.

10.5. Удостоверяющий Центр не несёт никакой иной ответственности перед Участниками Системы и их Пользователями - владельцами сертификатов ключей подписи (ключей шифрования) и лицами, использующими сертификаты ключей подписи (ключа шифрования) для проверки подписи и шифрования сообщений, а также перед третьими лицами за любые убытки, потери, иной ущерб, связанный с использованием сертификатов ключей подписи (ключа шифрования), независимо от суммы заключенных с использованием сертификатов ключей подписи (ключа шифрования) сделок и совершения ими иных действий, за исключением случаев нарушения Удостоверяющим Центром обязательств, предусмотренных Регламентом и/или действующим законодательством Российской Федерации.

10.6. Претензии к Удостоверяющему Центру ограничиваются указанием на несоответствие его действий настоящему Регламенту и Регламенту УЦ.

10.7. За неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту и Регламенту УЦ Участники Системы несут ответственность в соответствии с принятыми на себя обязательствами в процессе присоединения к Системе и/или подписания Договора с Удостоверяющим Центром и действующим законодательством Российской Федерации.

10.8. Пользователь несет ответственность за сохранность СКЗИ и своих закрытых ключей, используемых им для работы с Системой.

10.9. В случае невыполнения или ненадлежащего выполнения требований Регламента и/или отдельных договоров с Организатором Системы Участник может быть лишен возможности использовать Систему в рамках раздела, по которому этим Участником не выполняются или выполняются ненадлежащим образом требования Регламента и/или отдельных договоров с Организатором Системы.

11. ОТВЕТСТВЕННОСТЬ ОРГАНИЗАТОРА СИСТЕМЫ

11.1. Организатор Системы несет ответственность перед другими Участниками Системы в объеме, не превышающем ответственность любого другого Участника Системы.

11.2. Организатор Системы не несет ответственности в случае нарушения другими Участниками Системы и их Пользователями положений настоящего Регламента и Регламента УЦ.

11.3. В случае использования в каком-либо разделе области применения Системы специализированного программного обеспечения Организатор Системы несёт перед Участниками Системы никакой иной ответственности за любые убытки, потери, иной ущерб, связанный с использованием или неиспользованием информации, полученной в результате применения этого программного обеспечения, кроме обеспечения доступности этой информации с учетом режима работы программного обеспечения и типа доступа к информации в рамках этого раздела.

11.4. Претензии к Организатору Системы в части предоставления информации посредством применения специализированного программного обеспечения ограничиваются указанием на несоответствие его действий настоящему Регламенту и/или отдельному договору между Организатором Системы и Участником, предъявляющим претензии.

12. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ СТОРОН ПРИ НЕШТАТНЫХ СИТУАЦИЯХ, СВЯЗАННЫХ С ЭКСПЛУАТАЦИЕЙ СКЗИ

12.1. При возникновении нештатных ситуаций, таких как выход из строя ключевого носителя, сбои и отказы в работе СКЗИ, сбои и отказы в работе средств электронной цифровой подписи и др. Участник Системы обязан:

- руководствоваться положениями и инструкциями эксплуатационной документации;
- сообщить о возникшей ситуации в Удостоверяющий Центр;
- выполнить указания специалистов технической поддержки Удостоверяющего Центра, касающиеся выхода из данной внештатной ситуации.

13. ПРОЧИЕ УСЛОВИЯ

13.1. Изменения и дополнения в настоящий Регламент, включая изменения области применения Системы, вносятся Организатором Системы по согласованию с Удостоверяющим Центром с обязательным уведомлением всех Участников Системы.

13.2. Все приложения, изменения и дополнения являются неотъемлемой частью настоящего Регламента.

14. ПРИЛОЖЕНИЯ

Приложение №1 Образец Заявки Участника на присоединение к Системе

Приложение №2 Структура документа – уведомления об изменении области применения Системы.

Генеральный директор
ЗАО «ПЕТЕРБУРГРЕГИОНГАЗ»

Казаченков В.З.

_____ 2010г.

Заместитель Генерального директора,
Начальник Удостоверяющего центра
ООО «Газинформсервис

Кустов В.Н.

_____ 2010 г.

Юридический отдел

Приложение №1
К Регламенту использования автоматизированной
системы установления доверительных отношений

УТВЕРЖДАЮ:
Генеральный директор
ЗАО «Петербургрегионгаз»
_____ /Казаченков В.З./
«__» _____ 20__ г.

Организатору системы

ЗАЯВКА

на присоединение к

Системе установления доверительных отношений

Организация *<ОПФ>*[2] *<название>* в лице *<должность>* *<ФИО>*, действующего(ей) на основании *<документ на право осуществления полномочий>*, подтверждает свое намерение участвовать в работе Системы установления доверительных отношений ЗАО «Петербургрегионгаз» на правах Участника с *<дата присоединения к Системе>*.

Договор с Удостоверяющим Центром *<название Удостоверяющего Центра>* - *<№ договора>* от *<дата заключения договора>*.

Приложение: сертификат ключа подписи (должна прилагаться заверенная копия сертификата ключа подписи пользователя организации, выданная Удостоверяющим Центром)

СОГЛАСОВАНО:

Заместитель Генерального директора,
Начальник Удостоверяющего центра
ООО «Газинформсервис»
_____ /Кустов В.Н./
«__» _____ 20__ г.

<Должность>
<ОПФ> <Наименование>
_____ /<ФИО>/
«__» _____ 20__ г.

[2] ОПФ – Организационно-правовая форма

Юридический отдел

Приложение № 2
К Регламенту использования средств
криптографической защиты информации

Структура документа – уведомления об изменении области применения Системы

Утверждаю:

Генеральный директор
ЗАО «Петербургрегионгаз»
Казаченков В.З.

Согласовано:

Зам. генерального директора
ООО «ГАЗИНФОРМСЕРВИС»
Кустов В.Н.

198097, г. Санкт-Петербург, пр. Стачек, д. 47

Уведомление № NN-YYYY
об изменении области применения

Автоматизированная система
установления доверительных отношений

1. Введение.
2. Изменение области применения Системы.
2.1. Сроки вступления изменений в силу.
2.2. Название раздела (разделов) для добавления / удаления / изменения.
2.3. В случае добавления раздела – дополнительная информация:
   - о виде раздела (документооборот/предоставление информации);
   - о типе раздела (общедоступный/специальный);
   - в случае предоставления информации – тип доступа к ней.
3. Ответственность Организатора Системы.
4. Ответственность Участника Системы.
5. Ответственность Удостоверяющего Центра.
6. Технические особенности использования Системы после изменения области применения.

Юридический отдел