

Утверждено приказом от «20» мая 2011 года

Генеральный директор ООО «АТОН»
А.В. Шеметов

**ПРАВИЛА
ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
ООО «АТОН»**

(редакция, действующая с «06» июня 2011 года)

Москва 2011

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	4
§ 1. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	4
§ 2. ПРЕДМЕТ РЕГУЛИРОВАНИЯ НАСТОЯЩИХ ПРАВИЛ	4
§ 3. ПОРЯДОК ДЕЙСТВИЯ НАСТОЯЩИХ ПРАВИЛ	5
§ 4. ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ НАСТОЯЩИХ ПРАВИЛ ДЛЯ ВСЕХ УЧАСТНИКОВ.....	5
§ 5. УВЕДОМЛЕНИЯ	5
РАЗДЕЛ 1. ПОРЯДОК ОРГАНИЗАЦИИ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА	5
§ 1. НАЗНАЧЕНИЕ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ООО «АТОН»	5
§ 2. УЧАСТНИКИ ИНФОРМАЦИОННОЙ СИСТЕМЫ	5
§ 3. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА	6
§ 4. ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ	6
§ 5. ТРЕБОВАНИЯ К ЭЛЕКТРОННОМУ ДОКУМЕНТУ.....	7
§ 6. ФОРМИРОВАНИЕ ЭЛЕКТРОННОГО ДОКУМЕНТА	7
§ 7. ПОДЛИННИК ЭЛЕКТРОННОГО ДОКУМЕНТА	7
§ 8. КОПИИ ЭЛЕКТРОННОГО ДОКУМЕНТА НА БУМАЖНОМ НОСИТЕЛЕ	7
§ 9. ПРОВЕРКА ПОДЛИННОСТИ ДОСТАВЛЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТА.....	7
§ 10. ОТЗЫВ ЭЛЕКТРОННОГО ДОКУМЕНТА.....	8
РАЗДЕЛ 2. ПОРЯДОК ФУНКЦИОНИРОВАНИЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	8
§ 1. ОСНОВНЫЕ ПОЛОЖЕНИЯ.....	8
1.1. УДОСТОВЕРЯЮЩИЙ ЦЕНТР (УЦ).....	8
1.2. РЕГИСТРАЦИОННЫЙ ЦЕНТР.....	9
1.3. ПОЛЬЗОВАТЕЛИ УЦ.....	9
1.4. СЕРТИФИКАТЫ КЛЮЧЕЙ ПОДПИСИ	9
1.5. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.....	10
§ 2. ПРАВА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА И ПОЛЬЗОВАТЕЛЕЙ УЦ	10
2.1. ПРАВА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	10
2.2. ПРАВА ПОЛЬЗОВАТЕЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	11
§ 3. ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА И ПОЛЬЗОВАТЕЛЕЙ УЦ	11
3.1. ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	11
3.2. ОБЯЗАННОСТИ РЕГИСТРАЦИОННЫХ ЦЕНТРОВ	11
3.3. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ УЦ	11
§ 4. ОТВЕТСТВЕННОСТЬ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА И ПОЛЬЗОВАТЕЛЕЙ УЦ.....	12
4.1. ОТВЕТСТВЕННОСТЬ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА И РЕГИСТРАЦИОННОГО ЦЕНТРА	12
4.2. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ УЦ.....	12
§ 5. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ УЦ.....	12
5.1. ПЕРВОНАЧАЛЬНАЯ ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ УЦ	12
5.2. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ЗАРЕГИСТРИРОВАННОГО ПОЛЬЗОВАТЕЛЯ УЦ	12
§ 6. СПОСОБЫ УДАЛЕННОГО ВЗАИМОДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ С УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ.....	13
§ 7. ПЕРВИЧНАЯ РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ В УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ.....	13

§ 8. ФОРМИРОВАНИЕ ПАРОЛЯ ДЛЯ ВХОДА ПОЛЬЗОВАТЕЛЯ УЦ В ИНФОРМАЦИОННУЮ СИСТЕМУ	13
§ 9. ПЕРВОНАЧАЛЬНОЕ ФОРМИРОВАНИЕ КЛЮЧЕЙ И СЕРТИФИКАТОВ КЛЮЧЕЙ	14
9.1. ПЕРВОНАЧАЛЬНОЕ ФОРМИРОВАНИЕ КЛЮЧЕЙ И СЕРТИФИКАТА КЛЮЧА ПРИ УДАЛЕННОМ ОБРАЩЕНИИ ПОЛЬЗОВАТЕЛЯ УЦ.....	14
9.2. ПЕРВОНАЧАЛЬНОЕ ФОРМИРОВАНИЕ КЛЮЧЕЙ И СЕРТИФИКАТА КЛЮЧА ПРИ ОЧНОМ ОБРАЩЕНИИ ПОЛЬЗОВАТЕЛЯ УЦ	14
§ 10. ПОДКЛЮЧЕНИЕ УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ УЦ	15
10.1. ПОДКЛЮЧЕНИЕ УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ УЦ К ИНФОРМАЦИОННОЙ СИСТЕМЕ С ПОМОЩЬЮ СОТРУДНИКОВ ООО «АТОН».....	15
10.2. ПОДКЛЮЧЕНИЕ УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ К ИНФОРМАЦИОННОЙ СИСТЕМЕ ЧЕРЕЗ ПОСРЕДНИКОВ	15
§ 11. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ ПОДПИСИ ПОЛЬЗОВАТЕЛЯ УЦ.....	16
11.1. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ И ОБНОВЛЕНИЕ СЕРТИФИКАТА КЛЮЧА ПОЛЬЗОВАТЕЛЯ УЦ ПРИ УДАЛЕННОМ ОБРАЩЕНИИ	16
11.2. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ И ОБНОВЛЕНИЕ СЕРТИФИКАТА КЛЮЧА ПОЛЬЗОВАТЕЛЯ УЦ ПРИ УДАЛЕННОМ ОБРАЩЕНИИ С ИСПОЛЬЗОВАНИЕМ ДЕЙСТВУЮЩЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ.	17
11.3. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ И ОБНОВЛЕНИЕ СЕРТИФИКАТА КЛЮЧА ПОЛЬЗОВАТЕЛЯ УЦ ПРИ ОЧНОМ ОБРАЩЕНИИ	17
§ 12. ВНЕПЛАНОВАЯ СМЕНА КЛЮЧЕЙ ПОЛЬЗОВАТЕЛЯ УЦ	17
§ 13. АННУЛИРОВАНИЕ (ОТЗЫВ) СЕРТИФИКАТА КЛЮЧА ПОЛЬЗОВАТЕЛЯ УЦ.....	18
§ 14. УВЕДОМЛЕНИЕ О ФАКТЕ АННУЛИРОВАНИЯ (ОТЗЫВА) СЕРТИФИКАТА КЛЮЧА	18
§ 15. ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.....	18
15.1. ТРЕБОВАНИЯ К СРЕДСТВАМ ЭЛЕКТРОННОЙ ПОДПИСИ ПОЛЬЗОВАТЕЛЕЙ УЦ	18
15.2. СМЕНА КЛЮЧЕЙ УПОЛНОМОЧЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	19
РАЗДЕЛ 3. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТОВ.....	19
РАЗДЕЛ 4. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ	19
§ 1. СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	19
§ 2. МЕРЫ ЗАЩИТЫ ЗАКРЫТЫХ КЛЮЧЕЙ	20
§ 3. КОМПРОМЕТАЦИЯ КЛЮЧЕВЫХ НОСИТЕЛЕЙ УПОЛНОМОЧЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	21
§ 4. КОМПРОМЕТАЦИЯ КЛЮЧЕВЫХ НОСИТЕЛЕЙ ПОЛЬЗОВАТЕЛЯ УЦ	21
§ 5. КОМПРОМЕТАЦИЯ ПАРОЛЯ ДЛЯ ДОСТУПА В ИНФОРМАЦИОННУЮ СИСТЕМУ	21
ПРОЧИЕ ПОЛОЖЕНИЯ	22
§ 1. ТАРИФЫ НА УСЛУГИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА. ПОРЯДОК РАСЧЕТОВ	22
§ 2. ПРИЛОЖЕНИЯ К НАСТОЯЩИМ ПРАВИЛАМ	23
<i>ПРИЛОЖЕНИЕ №1</i>	24
<i>ПРИЛОЖЕНИЕ № 2</i>	26
<i>ПРИЛОЖЕНИЕ № 3</i>	27
<i>ПРИЛОЖЕНИЕ № 4</i>	28
<i>ПРИЛОЖЕНИЕ № 5</i>	29
<i>ПРИЛОЖЕНИЕ № 6</i>	30

§ 1. Основные термины и определения

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности. Задача аутентификации – гарантированное установление подлинности физического лица или юридического лица, выступающих под некоторым именем и запрашивающих доступ к тому или иному ресурсу.

Администратор Удостоверяющего центра (Администратор УЦ) – уполномоченный представитель Удостоверяющего центра, ответственный за выполнение операций по изготовлению и обслуживанию сертификатов.

Доверенный канал – это канал связи, который обеспечивает аутентификацию источника передаваемых данных, их конфиденциальность и контроль целостности, исключающие возможность подмены данных.

Запрос сертификата – электронный документ, содержащий открытый ключ с параметрами алгоритма, сведения о владельце открытого ключа и некоторые дополнительные данные, заверенные электронной подписью владельца открытого ключа.

Идентификация – процедура присвоения субъектам и объектам доступа некоторого идентификатора и/или сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов. Идентификация заключается в установлении факта соответствия заданного имени и реально существующего субъекта (физического лица или юридического лица) и к установлению факта, что субъект, запрашивающий доступ к ресурсам под заданным именем, является именно тем субъектом, которому заданное имя было присвоено в результате легальной процедуры.

Компрометация ключа – утрата доверия к тому, что используемый ключ обеспечивает безопасность информации; констатация владельцем сертификата обстоятельств, при которых возможно несанкционированное использование его закрытого ключа неуполномоченными лицами.

Криптографическая защита – защита информации от ее несанкционированной модификации и доступа посторонних лиц при помощи алгоритмов криптографического преобразования;

Плановая смена ключей – регламентируемая Администратором УЦ периодическая смена криптографических ключей пользователей и уполномоченного лица УЦ, не вызванная их компрометацией.

Регистрационный центр (РЦ) – опциональный субъект инфраструктуры открытых ключей, отвечающий за идентификацию и аутентификацию заявителей, претендующих на получение сертификата, но не подписывающий и не выпускающий сертификаты (Удостоверяющий центр делегирует Регистрационному центру часть своих полномочий).

Список отозванных сертификатов (СОС) – электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей, которые на определенный момент времени были аннулированы (отозваны) или действие которых было приостановлено.

Электронный документооборот (ЭДО) - обмен электронными документами между ООО «АТОН» и участниками информационной системы в соответствии с настоящими Правилами.

Настоящие Правила содержат также иные термины (и их сокращения), которые используются в значениях, определенных в соответствующих разделах Правил.

Все иные термины используются в значениях, определенных действующим законодательством Российской Федерации (далее – РФ).

§ 2. Предмет регулирования настоящих Правил

1. Настоящие Правила устанавливают общий порядок электронного документооборота при осуществлении взаимодействия между ООО «АТОН» и участниками информационной системы, в области оказания ООО «АТОН» услуг на рынках ценных бумаг, а также порядок выпуска и обслуживания Удостоверяющим центром ООО «АТОН» (далее - УЦ) сертификатов ключей электронных подписей в рамках данной информационной системы.

2. Настоящие Правила содержат условия соглашения, налагающего обязательства и устанавливающего ответственность сторон, вовлеченных в процесс предоставления и использования услуг УЦ (соглашения об электронном документообороте). С 06 июня 2011 года соглашение об электронном документообороте (далее - Соглашение об ЭДО) заключается путем присоединения участника к установленным настоящими Правилами условиям в целом.

3. В части, не урегулированной настоящими Правилами, на отношения УЦ и участников информационной системы распространяются правила, установленные действующим законодательством РФ для корпоративных информационных систем.

§ 3. Порядок действия настоящих Правил

1. Настоящие Правила, включая все Приложения, а также изменения и дополнения к ним, утверждаются в одностороннем порядке по решению Удостоверяющего центра, который вправе определять сроки и порядок вступления в силу изменений и дополнений в настоящие Правила и Приложения к ним.

2. Приложения к настоящим Правилам являются их неотъемлемой частью. Правила и Приложения могут дублироваться на английском языке. В случае расхождения русского и английского текстов приоритетным является текст на русском языке.

3. Удостоверяющий центр вправе по своему усмотрению отказаться от заключения Соглашения об ЭДО с лицом, имеющим намерение стать Участником.

4. Действующая редакция настоящих Правил размещается на странице www.skrin.ru в сети «Интернет». ООО «АТОН» вправе заменить указанный адрес в сети «Интернет», опубликовав соответствующее уведомление в периодическом печатном издании, распространяемом на территории РФ тиражом не менее 50 000 (Пятидесяти тысяч) экземпляров не позднее, чем за 10 (Десять) рабочих дней.

5. Изменения и дополнения к настоящим Правилам и Приложений к ним, а также решения Удостоверяющего центра о сроках и порядке вступления их в силу, доводятся до сведения Участников путем размещения на странице www.skrin.ru в сети «Интернет» не позднее, чем за 10 (Десять) рабочих дней до вступления в силу изменений в Правилах и Приложений к ним, и решений Удостоверяющего центра.

§ 4. Прекращение действия настоящих Правил для всех Участников

1. Настоящие Правила прекращают свое действие на основании решения Удостоверяющего центра.

2. Прекращение действия настоящих Правил и Приложений к ним не влияет на юридическую силу и действительность электронных документов, которыми Удостоверяющий центр и Участники обменивались до прекращения действия настоящих Правил и Приложений к ним.

§ 5. Уведомления

1. Предоставление Удостоверяющим центром каких-либо уведомлений (за исключением уведомлений об изменении настоящих Правил), в том числе о приостановлении действия или аннулировании сертификатов, может осуществляться путем размещения информации на странице www.aton-line.ru в сети «Интернет».

2. В случае прекращения действия Правил Удостоверяющий центр уведомляет об этом за 30 (Тридцать) дней до даты прекращения его действия.

РАЗДЕЛ 1. ПОРЯДОК ОРГАНИЗАЦИИ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА.

§ 1. Назначение системы электронного документооборота ООО «АТОН»

1. Система ЭДО ООО «АТОН» представляет собой защищенное приложение, обеспечивающее безопасный обмен через Интернет электронными документами между ООО «АТОН» и физическими и юридическими лицами.

2. Передача электронных документов осуществляется исключительно в рамках информационных систем, предоставленных ООО «АТОН».

3. Аутентификация и целостность электронных документов в системе ЭДО ООО «АТОН» обеспечивается квалифицированной электронной подписью, реализуемой средствами СКЗИ «Крипто-Ком 3.2» разработки ЗАО «Сигнал-КОМ».

§ 2. Участники информационной системы

Участниками информационной системы (далее – Участники или Пользователи УЦ) являются:

- физические лица, владеющие сертификатами ключей проверки электронной подписи (далее - сертификаты ключа), выданными Удостоверяющим центром, или находящиеся в процессе получения таких сертификатов;
- физические и юридические лица, от имени которых передаются и принимаются электронные документы,

заключившие с ООО «АТОН» Соглашение об ЭДО: путем подписания заявления о заключении договоров по форме Приложения № 1, либо соглашения об использовании электронно-цифровой подписи, либо договора о брокерском обслуживании, в рамках которого предусмотрен обмен с ООО «АТОН» документами в электронном виде, подписанными электронной подписью.

§ 3. Особенности организации электронного документооборота

1. Условиями допуска Участника к осуществлению Электронного документооборота являются:
 - заключение соглашения об электронном документообороте;
 - установка необходимого программного обеспечения (ПО) (подробнее Раздел 2 п.1.5).
 - выполнение Удостоверяющим центром или самим Участником процедуры формирования ключей подписи (подробнее Раздел 2, п.9);
 - изготовление Удостоверяющим центром сертификата ключа для Участника (подробнее Раздел 2 п.9)

2. В действующей системе ЭДО ООО «АТОН» все услуги по управлению открытыми ключами и сертификатами ключей пользователей (регистрация, формирование, обновление, отзыв) возлагаются на Удостоверяющий центр ООО «АТОН» (подробнее Раздел 2).

3. Для формирования электронной подписи под электронными документами каждый Участник должен иметь ключевой носитель с закрытым ключом и сертификатом открытого ключа (подробнее Раздел 2).

§ 4. Использование электронной подписи

1. Электронный документ может быть подписан только тем закрытым (секретным) ключом электронной подписи, для которого Удостоверяющим центром изготовлен сертификат ключа (подробнее Раздел 2 п.1.4, п.9)

2. Электронный документ считается исходящим от Участника, если он подписан электронной подписью, владельцем сертификата ключа которой является данный Участник.

3. Риск неправомерного подписания электронного документа электронной подписью несет Участник, от имени которого данный документ подписан.

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.

5. Электронный документ должен быть подписан электронной подписью определенной области действия, указанной в действующем сертификате ключа подписи и использование которой допускается в данной Информационной системе.

6. Замена закрытых ключей электронной подписи не влияет на юридическую силу электронного документа, если он был подписан действующим на дату подписания закрытым ключом электронной подписи в соответствии с настоящими Правилами (подробнее Раздел 2 п.11, п.12).

7. Каждый Участник должен иметь свой индивидуальный закрытый ключ электронной подписи для подписания исходящих от него электронных документов.

8. Любой электронный документ, содержащий конфиденциальную информацию и пересылаемый по открытым каналам связи, должен быть зашифрован, при этом конфиденциальность электронного документа должна определяться его отправителем.

9. В случае получения зашифрованного электронного документа, электронный документ должен быть расшифрован.

10. Проверка электронной подписи проводится при проверке подлинности доставленного электронного документа.

11. Участником используются ключи, соответствующие сертификаты ключей, полученные в установленном настоящими Правилами порядке (подробнее Раздел 2 п.9)

§ 5. Требования к электронному документу

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 настоящими Правилами.
2. Электронное сообщение приобретает правовой статус электронного документа при его соответствии требованиям, установленным настоящими Правилами.
3. Электронный документ должен быть сформирован в одном из форматов, определенных в настоящих Правилах и подписан электронной подписью.
4. Все действия с электронными документами, оформленными, переданными и/или полученными в соответствии с настоящими Правилами, признаются ООО «АТОН» и Участниками совершенными в письменной форме и не могут быть оспорены только на том основании, что они совершены в электронном виде.

§ 6. Формирование электронного документа

Формирование электронного документа осуществляется в следующем порядке:

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

§ 7. Подлинник электронного документа

1. Электронный документ может иметь неограниченное количество экземпляров. Для создания дополнительного экземпляра существующего электронного документа осуществляется воспроизводство содержания документа вместе с электронной подписью.
2. Все экземпляры электронного документа являются подлинниками данного электронного документа.
3. Электронный документ не может иметь копий в электронном виде.
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 электронной подписи.

§ 8. Копии электронного документа на бумажном носителе

1. Копии электронного документа могут быть изготовлены (распечатаны) на бумажном носителе и заверены собственноручной подписью уполномоченного лица ООО «АТОН», и скреплены оттиском печатью ООО «АТОН».
2. Копии электронного документа на бумажном носителе должны содержать обязательную отметку, свидетельствующую о том, что это копия.
3. Электронный документ и его копии на бумажном носителе должны быть аутентичными.
4. Программные средства, осуществляющие преобразование электронного документа для изготовления (распечатки) в виде бумажного документа, являются неотъемлемой составной частью программного обеспечения, используемого в системе ЭДО.

§ 9. Проверка подлинности доставленного электронного документа

1. Полученный электронный документ проверяется на целостность, т.е. его доставку в неискаженном (по отношению к первоначальному) виде. При проверке документа на целостность в случае необходимости производится его расшифрование, а также обязательная проверка электронной подписи.
2. Полученный электронный документ проверяется на соответствие установленному для него формату.
3. Электронный документ подлежит дальнейшей обработке и исполнению только в случае положительного результата проверки целостности электронного документа, его соответствия установленному формату..
4. В случае невозможности расшифрования электронного документа, а также при отрицательном результате проверки целостности электронного документа, в том числе подлинности электронной подписи, документ считается не полученным и не подлежит дальнейшей обработке и исполнению.

§ 10. Отзыв электронного документа

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

2. Электронный документ может быть отозван в любой момент, когда это позволяет соответствующая система.

РАЗДЕЛ 2. ПОРЯДОК ФУНКЦИОНИРОВАНИЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

§ 1. Основные положения

1.1. УДОСТОВЕРЯЮЩИЙ ЦЕНТР (УЦ)

1. Удостоверяющий центр (УЦ) обеспечивает выполнение интегрированного набора услуг сертификационного центра и в процессе своей деятельности реализует следующие функции:

- формирование корневых сертификатов ключей УЦ;
- первичная идентификация и аутентификация Участников информационной системы – владельцев сертификатов (Пользователей УЦ);
- регистрация в реестре УЦ Участников информационной системы – владельцев сертификатов;
- формирование пароля и логина для доступа Пользователей УЦ в информационную систему;
- изменение по заявлению Пользователя УЦ пароля и логина для доступа Пользователя УЦ в информационную систему;
- предоставление Пользователям УЦ программного обеспечения и ключевой информации, необходимых для работы в информационной системе;
- формирование ключевых носителей Пользователям УЦ, включая генерацию закрытого и открытого ключей;
- формирование Запросов Пользователей УЦ сертификатов ключей;
- прием и регистрацию Запросов сертификатов ключей Пользователей УЦ;
- консультировать Пользователей УЦ по всем вопросам, связанным с использованием сертификата ключа;
- контроль уникальности открытых ключей в регистрируемых Запросах;
- изготовление и выдача на основании Запросов электронных сертификатов ключей;
- изготовление и выдача сертификатов ключей в форме документов на бумажных носителях;
- аутентификация Пользователей УЦ, запрашивающих аннулирование (отзыв), сертификатов ключей;
- аннулирование (отзыв) сертификатов ключей по запросам Пользователей УЦ, ;
- выпуск Списка отозванных сертификатов (СОС);
- ведение реестра выпущенных сертификатов ключей и СОС;
- публикация реестра выпущенных сертификатов и СОС в общедоступном сетевом справочнике;
- подтверждение подлинности электронных подписей в документах, представленных в электронной форме, по запросам Пользователей УЦ;
- архивное хранение сертификатов в электронном виде в течение всего срока действия сертификатов;
- архивное хранение сертификатов в течение 5 (пяти) лет после их аннулирования (отзыва) или окончания срока действия для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с их применением;

2. Удостоверяющий Центр ООО «АТОН» осуществляет свою деятельность на основании соответствующих лицензий, в том числе:

• Лицензии ФСБ № 0021016 от 07.10.10 на осуществление технического обслуживания шифровальных (криптографических) средств.

• Лицензии ФСБ № 0021015 от 07.10.10 на осуществление предоставления услуг в области шифрования информации

• Лицензии ФСБ № 0021017 от 07.10.10 на осуществление распространения шифровальных (криптографических) средств

• Лицензии ФСБ № 0021012 от 07.10.10 на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

3. Удостоверяющий центр использует средство криптографической защиты информации (СКЗИ) Крипто-Ком 3.2 разработки ЗАО «Сигнал-Ком», имеющее сертификаты ФСБ России СФ/114-1551, СФ/114-1552, СФ/124-1553, СФ/124-1554 от 07.11.2010 г., СФ/114-1170 от 15.07.2008 г., СФ/124-1337 от 05.06.2009 г.,

удостоверяющие, что СКЗИ соответствует требованиям российских государственных стандартов в области криптографической защиты, требованиям ФСБ России к стойкости СКЗИ и может, соответственно, использоваться для обеспечения безопасности информации уровня КС1 и КС2, не содержащей сведений, составляющих государственную тайну.

1.2. РЕГИСТРАЦИОННЫЙ ЦЕНТР

1. Регистрационный центр (РЦ) – субъект инфраструктуры открытых ключей, которому УЦ делегирует часть своих полномочий по регистрации участников защищенных прикладных систем, их первичной идентификации и аутентификации. РЦ регистрирует Запросы на выпуск и отзыв сертификатов ключей, обеспечивает их доставку в УЦ и отвечает за передачу сформированных сертификатов и их бумажных копий Пользователям.

2. Регистрационные центры выступают в роли уполномоченных представителей Удостоверяющего центра и занимают по отношению к УЦ подчиненное положение.

3. В процессе своей деятельности Регистрационный центр реализует следующие функции:

- первичная идентификация и аутентификация пользователей информационной системы – владельцев сертификатов;
- предоставление Пользователям УЦ программного обеспечения и ключевой информации, необходимых для работы в информационной системе;
- формирование ключевых носителей Пользователей УЦ, включая генерацию закрытого и открытого ключей;
- формирование Запросов сертификатов ключей;
- прием Запросов Сертификатов ключей от Пользователей УЦ;
- предоставление Пользователям УЦ изготовленных сертификатов ключей в электронной форме и бумажных копий сертификатов;
- аутентификация Пользователей УЦ, запрашивающих аннулирование (отзыв) сертификатов ключей;
- прием запросов на аннулирование (отзыв) сертификатов ключей от Пользователей и передача их в УЦ.

1.3. ПОЛЬЗОВАТЕЛИ УЦ

1. Пользователи УЦ - зарегистрированные в УЦ лица, являющиеся владельцами сертификатов ключей.

2. Владельцами сертификатов могут быть:

- физическое лицо;
- физическое лицо, действующее от имени юридического лица по доверенности или на основании уставных документов, дающих право данному физическому лицу представлять юридическое лицо и пользоваться услугами Удостоверяющего центра.

3. Потенциальные пользователи УЦ - незарегистрированные в УЦ лица, намеревающиеся получить сертификат ключа.

1.4. СЕРТИФИКАТЫ КЛЮЧЕЙ ПОДПИСИ

1. Сертификаты ключей формируются Удостоверяющим центром для Участников системы ЭДО АТОН и предназначены для обеспечения целостности и достоверности любых электронных документов исключительно в рамках данной системы.

2. Сертификаты ключей имеют два подкласса: сертификаты для физических лиц, выдаваемые по предъявлению паспорта, и сертификаты для юридических лиц, выдаваемые доверенным физическим лицам на основании паспорта и документов, подтверждающих должностные полномочия этих лиц в рамках своей организации.

3. Алгоритм открытого ключа в сертификатах ключа – ГОСТ Р 34.10-2001.

4. Срок действия сертификата ключа устанавливается Удостоверяющим центром при выдаче сертификата. Данный срок не может превышать 455 дней.

5. Копия Запроса сертификата ключа в бумажной форме является Заявлением на изготовление сертификата с атрибутами, указанными в Запросе.

6. Требования, предъявляемые к содержанию заявления на изготовление сертификата ключа:

- 1) внесение сведений о владельце сертификата, а именно:
 - Ф.И.О. Пользователя или его уполномоченного представителя;
 - паспортные данные: серия, №, дата и место выдачи;
 - фактический адрес проживания (страна, название области/района, город, улица, № дома, корпуса, квартиры);

- 2) значение открытого ключа;
- 3) наименование средств электронной подписи, с которыми используется данный открытый ключ электронной подписи;
- 4) наименование и место нахождения Удостоверяющего центра;
- 5) сведения об отношениях, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение;
- 6) алгоритм шифрования;
- 7) указание даты подписания;
- 8) наличие подписи Пользователя УЦ или его уполномоченного представителя с расшифровкой подписи;
указание кода Пользователя УЦ (логин).

7. Удостоверяющий центр предоставляет владельцам сертификатов ключа следующие услуги:

- формирование по запросу Пользователя УЦ пары его ключей, записанных на ключевой носитель;
- формирование сертификата ключа, запись его на ключевой носитель (при необходимости) и передача его Пользователю УЦ;
- аннулирование (отзыв) сертификата ключа по требованию владельца либо по решению Администратора УЦ;
- архивное хранение сертификата ключа в течение 5 (Пяти) лет в защищенном хранилище сертификатов.

1.5. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Удостоверяющий центр предоставляет Участнику информационной системы программное обеспечение производства ЗАО «Сигнал-Ком», созданное на «СКЗИ «Крипто-КОМ 3.2».

2. Программное обеспечение может быть предоставлено Пользователю УЦ на каком-либо из типов носителей, предложенных Удостоверяющим центром, либо (при наличии возможности) самостоятельно скопировано Участником в сети «Интернет» на странице www.aton-line.ru.

3. Пользователи УЦ не вправе распространять, копировать или модифицировать полученное программное обеспечение без согласия Удостоверяющего центра.

4. Удостоверяющий центр вправе принять решение о замене предоставленного программного обеспечения полностью или в какой-либо части.

5. Удостоверяющий центр обязан предоставить Пользователям УЦ подлежащее замене программное обеспечение.

6. Пользователь УЦ обязан осуществить действия, необходимые с его стороны для замены программного обеспечения.

§ 2. Права Удостоверяющего центра и Пользователей УЦ

2.1. ПРАВА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Удостоверяющий центр имеет право:

- Требовать подтверждения достоверности информации, содержащейся в сертификатах ключей Пользователей УЦ и уполномоченных представителей Пользователей УЦ.
- Отказать в формировании ключей Пользователю УЦ в случае ненадлежащего оформления заявления на формирование ключей.
- Отказать в изготовлении сертификата ключа Пользователя УЦ в случае ненадлежащего оформления заявления на изготовление сертификата ключа.
- Отказать в изготовлении сертификата ключа Пользователя УЦ при отсутствии соответствующих полномочий у лица, представившего заявление на изготовление сертификата ключа.
- Отказать в аннулировании (отзыве) сертификата ключа Пользователя УЦ в случае ненадлежащего оформления заявления на аннулирование (отзыв) сертификата ключа.
- Отказать в аннулировании (отзыве) сертификата ключа Пользователя УЦ в случае, если истек установленный срок действия этого сертификата.
- Аннулировать (отозвать) сертификат ключа владельца сертификата в случае установленного факта компрометации соответствующего ему закрытого ключа, с уведомлением владельца аннулированного (отозванного) сертификата и указанием обоснованных причин, либо указания лиц или органов, имеющих такое право в силу закона.
- Заменить предоставленное Пользователю УЦ программное обеспечение полностью или в какой-либо части.

2.2. ПРАВА ПОЛЬЗОВАТЕЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Пользователь Удостоверяющего центра имеет право:

- Получить сертификат ключа уполномоченного лица Удостоверяющего центра.
- Получить ключи электронной подписи и сертификат ключа с возможной их записью на ключевой носитель.
- Обратиться в Удостоверяющий центр для аннулирования (отзыва) сертификата ключа, если период действия этого сертификата еще не истек.
- Обращаться в УЦ за подтверждением подлинности электронных подписей, связанных с использованием сертификатов ключей, выданных УЦ в документах, представленных в электронной форме.
- Обращаться в УЦ для получения средства электронной подписи.
- Сформировать закрытый и открытый ключи на своем рабочем месте с использованием средства электронной подписи и программных средств со встроенной библиотекой СКЗИ «Крипто-КОМ 3.2», предоставляемых Удостоверяющим Центром.

§ 3. Обязанности Удостоверяющего центра и Пользователей УЦ

3.1. ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

УЦ должен строго соблюдать порядок, изложенный в настоящих Правилах, в частности:

- использовать закрытый ключ уполномоченного лица УЦ только для заверения издаваемых им сертификатов и Списков отозванных сертификатов;
- обеспечивать надежную защиту закрытого ключа уполномоченного лица УЦ от несанкционированного доступа;
- обеспечивать конфиденциальность в отношении изготавливаемых закрытых ключей Пользователей УЦ;
- соблюдать конфиденциальность в отношении регистрационной информации о Пользователе УЦ;
- обеспечивать уникальность серийных номеров изготавливаемых сертификатов;
- извещать Пользователя УЦ о причинах отказа в изготовлении сертификата ключа;
- принимать и обрабатывать запросы от владельцев сертификатов ключа на отзыв сертификатов:
 - принимать и обрабатывать запросы на отзыв сертификатов ключа;
 - аутентифицировать Пользователей УЦ, запрашивающих отзыв сертификата ключа;
 - отзывать сертификаты ключа по запросам Пользователей УЦ;
 - информировать Пользователей УЦ об отзыве сертификатов путем периодического выпуска Списка отозванных сертификатов (СОС) не реже 1 (одного) раза в 30 (тридцать) дней;
- публиковать реестр выпущенных сертификатов и СОС в сетевом справочнике;
- уведомлять Пользователя УЦ о фактах, которые стали известны УЦ и которые существенным образом могут сказаться на возможности дальнейшего использования его сертификата ключа;
- уведомлять о факте отзыва сертификата ключа Пользователя УЦ или его уполномоченного представителя.
- синхронизировать по времени все программные и технические средства обеспечения деятельности в соответствии с их предназначением.

3.2. ОБЯЗАННОСТИ РЕГИСТРАЦИОННЫХ ЦЕНТРОВ

Регистрационные центры должны строго соблюдать порядок, изложенный в настоящих Правилах, в частности:

- осуществлять регистрацию Пользователей УЦ;
- осуществлять регистрацию поступающих Запросов сертификатов и передавать их по защищенному каналу в УЦ;
- передавать полученные из УЦ сформированные сертификаты Пользователям УЦ.

3.3. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ УЦ

Пользователи УЦ должны строго соблюдать правила, изложенные в настоящих Правилах, в частности:

- обеспечивать сохранность закрытого ключа и ключевого носителя, принимать все возможные меры для предотвращения их потери, раскрытия, модифицирования или несанкционированного использования;
- проверять достоверность и целостность сертификата ключа при его использовании;
- проверять текущий статус сертификатов ключа (на предмет их отзыва);
- не использовать закрытый ключ и соответствующий ему сертификат по истечении срока их действия;

- своевременно (до истечения периода действия сертификата) осуществлять смену закрытого ключа и сертификата ключа;
- использовать сертификат ключа исключительно в рамках приложений, разрешенных настоящими Правилами;
- точно соблюдать формат и структуру Запроса сертификата, предоставляемого в УЦ;
- предоставлять в УЦ регистрационную и идентифицирующую информацию в объеме, определенном положениями настоящих Правил;
- указывать в Запросе сертификата ключа максимально точные и действительные сведения;
- подтверждать по требованию УЦ достоверность информации, содержащейся в сертификате ключа, выдаваемом Пользователю;
- своевременно информировать УЦ или уполномоченного представителя УЦ о факте компрометации собственного закрытого ключа или ключевого носителя;
- не использовать для формирования электронной подписи скомпрометированные закрытые ключи;
- в случае компрометации ключей своевременно прислать в УЦ запрос на аннулирование (отзыв) сертификата ключа;
- своевременно информировать УЦ или уполномоченного представителя УЦ о фактах изменения персональных данных, содержащихся в сертификатах ключа;
- перед первым использованием на компьютере и в дальнейшем не реже 1 (одного) раза в месяц проводить контроль целостности состава прикладного программного обеспечения, используя для этого утилиту gush, входящую в состав СКЗИ «Крипто-КОМ 3.2» .

§ 4. Ответственность Удостоверяющего центра и Пользователей УЦ

4.1. ОТВЕТСТВЕННОСТЬ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА И РЕГИСТРАЦИОННОГО ЦЕНТРА

Удостоверяющий центр и регистрационный центр несут ответственность в соответствии с законодательством РФ:

УЦ не несет ответственности за любые прямые или косвенные убытки, любую потерю прибыли, явившиеся результатом:

- несоблюдения подписчиками конфиденциальности собственных закрытых ключей, а также достоверности и целостности сертификатов уполномоченного лица Удостоверяющего центра;

4.2. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ УЦ

Пользователи УЦ несут ответственность за:

- несохранение конфиденциальности собственных закрытых ключей,
- несохранение личных ключевых носителей;
- несохранение достоверности и целостности сертификатов уполномоченного лица УЦ;
- несвоевременное уведомление УЦ о компрометации собственного закрытого ключа.

§ 5. Идентификация и аутентификация Пользователей УЦ

5.1. ПЕРВОНАЧАЛЬНАЯ ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ УЦ

1. Идентификация Пользователя УЦ выполняется в процессе его регистрации в УЦ. Результатом идентификации является присвоение Пользователю УЦ уникального имени и занесение данного имени в реестр зарегистрированных Пользователей Удостоверяющего центра. Идентификация опирается на наличие у каждого владельца сертификата уникального имени, отличного от имен всех остальных пользователей.

2. Начальная аутентификация физического лица производится с использованием документа, удостоверяющего личность.

3. В том случае, если Пользователь УЦ является уполномоченным представителем юридического лица ему необходимо вместе с документом, удостоверяющим личность, представить официальный документ (доверенность, учредительные документы юридического лица), дающий право данному физическому лицу представлять юридическое лицо и пользоваться услугами Удостоверяющего центра.

5.2. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ЗАРЕГИСТРИРОВАННОГО ПОЛЬЗОВАТЕЛЯ УЦ

1. Идентификация зарегистрированного Пользователя УЦ осуществляется по уникальному имени, занесенному в реестр Удостоверяющего центра при его первичной регистрации, и паспортным данным Пользователя УЦ.

2. Аутентификация зарегистрированного Пользователя УЦ при его обращении в УЦ с заявлением на формирование сертификата, замену и отзыв сертификата выполняется путем проверки подлинности подписи Пользователя в заявлении.

3. Удаленная аутентификация по электронной подписи выполняется при удаленном обращении зарегистрированного Пользователя УЦ с заявлением на формирование сертификата, поданного в электронной форме с электронной подписью Пользователя. Удаленная аутентификация в этом случае осуществляется путем выполнения процедуры проверки в электронном документе электронной подписи Пользователя УЦ.

§ 6. Способы удаленного взаимодействия Пользователей с Удостоверяющим центром

1. Взаимодействия пользователей с УЦ через доверенных посредников:

Данный вариант используется только на этапе начального подключения Пользователя к информационной системе путем передачи Пользователю документов, необходимых для регистрации в УЦ и формирования сертификата ключа, и съемного носителя с записанной ключевой информацией.

2. Взаимодействия пользователей с УЦ через Web-интерфейс:

Данный вариант используется для организации режима автоматической сертификации запросов, импортируемых в УЦ по доверенному каналу.

3. Взаимодействия Пользователей с УЦ через Регистрационные центры:

Данный способ используется для более оперативной регистрации и обслуживания региональных Участников.

§ 7. Первичная регистрация Пользователей в Удостоверяющем центре

Регистрация Пользователей УЦ – это внесение регистрационной информации о Пользователях УЦ в реестр Удостоверяющего центра.

Процедура регистрации проводится только в отношении физических лиц и включает следующие этапы:

- изготовление ключевых носителей Пользователя УЦ;
- формирование Запроса сертификата ключа;
- передача в УЦ (РЦ) Запроса сертификата ключа и заявления на выдачу сертификата ключа;
- регистрация Запроса в УЦ;
- изготовление сертификата;
- передача сертификата Пользователю УЦ.

§ 8. Формирование пароля для входа Пользователя УЦ в информационную систему

Для доступа в информационную систему Удостоверяющий центр предоставляет Пользователю УЦ логин и пароль. УЦ формирует с помощью специализированного ПО Карту клиента, которая содержит логин и пароль для входа в информационную систему, и передает ее Пользователю в запечатанном конверте. Факт передачи пароля фиксируется в «Журнале учета и движения паролей Пользователей» либо в «Журнале передачи комплектов ключей».

Конверт с Картой клиента передается Пользователю несколькими способами:

1. При личном визите Пользователя УЦ в ООО «АТОН».
2. При личном визите в ООО «АТОН» курьера, уполномоченного Пользователем доставлять, принимать, расписываться в получении документов.
3. По почте России срочным письмом.
4. Через посредников

Пользователь УЦ обязан хранить полученные логин и пароль в тайне.

Пользователь УЦ ключа может заменить пароль для входа в информационную систему по собственному желанию после предоставления им в УЦ заявления о замене пароля с указанием причины (по форме Приложения № 5).

§ 9. Первоначальное формирование ключей и сертификатов ключей

9.1. ПЕРВОНАЧАЛЬНОЕ ФОРМИРОВАНИЕ КЛЮЧЕЙ И СЕРТИФИКАТА КЛЮЧА ПРИ УДАЛЕННОМ ОБРАЩЕНИИ ПОЛЬЗОВАТЕЛЯ УЦ

1. Формирование ключей подписи выполняется Пользователем УЦ самостоятельно с помощью ПО, разработанного на базе сертифицированного СКЗИ «Крипто-КОМ 3.2» и скопированным им в личном кабинете на странице www.aton-line.ru в сети «Интернет».

Запрос сертификата ключа, сформированный Пользователем УЦ, в электронной форме передается в базу данных Удостоверяющего центра по доверенному каналу или по электронной почте.

2. Подписанное заявление на выдачу сертификата ключа (по форме Приложениям №3) Пользователю необходимо доставить в УЦ:

- при личном визите в ООО «АТОН»
- курьером, уполномоченным Пользователем УЦ доставлять, принимать, расписываться в получении документов;
- по почте России заказным письмом или письмом с объявленной ценностью.

3. При получении заявления Пользователя УЦ на выдачу сертификата ключа УЦ проверяет соответствие идентификационных данных Пользователя УЦ. В случае идентичности указанной информации УЦ изготавливает сертификат ключа на основании Запроса.

4. В случае отказа в изготовлении сертификата ключа Пользователь УЦ уведомляется об этом с указанием причины отказа.

5. Изготовленный сертификат ключа в виде электронного документа вместе с действующим сертификатом ключа уполномоченного лица УЦ передается Пользователю УЦ на рабочее место автоматически или по электронной почте.

6. УЦ заполняет заявление на выдачу сертификата ключа на бумажном носителе, указывая следующие сведения:

- регистрационный номер сертификата,
- дату начала действия сертификата,
- дату окончания действия сертификата,
- уполномоченное лицо,
- основание полномочий.

7. Уполномоченный представитель УЦ подписывает заполненное заявление на изготовление сертификата ключа, заверяет печатью УЦ. С данного момента заявление на изготовление сертификата ключа признается документом «Сертификат ключа подписи».

8. Полученный личный сертификат ключа и сертификат Удостоверяющего центра Пользователь УЦ помещает на свой ключевой носитель. Сертификат УЦ рекомендуется хранить на ключевом носителе вместе с закрытыми ключами Пользователя УЦ.

9.2. ПЕРВОНАЧАЛЬНОЕ ФОРМИРОВАНИЕ КЛЮЧЕЙ И СЕРТИФИКАТА КЛЮЧА ПРИ ОЧНОМ ОБРАЩЕНИИ ПОЛЬЗОВАТЕЛЯ УЦ

1. Формирование ключей подписи при очном обращении Пользователя УЦ выполняется Удостоверяющего центра при наличии подписанного Пользователем УЦ заявления о формировании ключей (по форме Приложения № 2).

2. УЦ осуществляет формирование ключей и сертификата ключа с помощью ПО, разработанного на базе сертифицированного СКЗИ «Крипто-КОМ 3.2», и записывает на отчуждаемый ключевой носитель:

- сформированные ключи электронной подписи;
- созданный (зарегистрированный) сертификат в электронной форме;
- сертификат ключа уполномоченного лица Удостоверяющего центра
- утилиту *wire*, предназначенную для удаления файлов с ключевых носителей с предварительным их физическим затиранием.
- программное обеспечение, необходимое для работы в информационной системе.

Ключевой носитель помещается в конверт, который скрепляется печатью.

3. УЦ заполняет заявление на выдачу сертификата ключа (по форме Приложения № 3), указывая следующие сведения:

- регистрационный номер сертификата,
- дату начала действия сертификата,
- дату окончания действия сертификата,

- уполномоченное лицо,
- основание полномочий.

4. Пользователь УЦ заверяет собственноручной подписью заполненное заявление на выдачу сертификата ключа.

5. После подписания заявления на выдачу сертификата УЦ передает Пользователю УЦ конверт с электронным носителем с записанной на него ключевой информацией.

Факт выдачи конверта с электронным носителем, содержащего ключевую информацию, фиксируется в Журнале передачи комплекта ключей и заверяется собственноручной подписью Пользователя УЦ.

§ 10. Подключение удаленных Пользователей УЦ

10.1. ПОДКЛЮЧЕНИЕ УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ УЦ К ИНФОРМАЦИОННОЙ СИСТЕМЕ С ПОМОЩЬЮ СОТРУДНИКОВ ООО «АТОН»

1. В Удостоверяющем центре формируются комплекты быстрой активации для передачи сотрудникам ООО «АТОН». Каждый комплект включает, в том числе, следующие документы:

- сейф-пакет, запечатанный таким образом, что любая попытка его вскрытия не может остаться незамеченной, содержащий:
 - ключи электронной подписи;
 - Запрос сертификата с анонимными атрибутами;
 - утилиту RUSH из состава СКЗИ «Крипто-КОМ 3.2» для вычисления контрольной суммы дистрибутивных файлов (контроля целостности);
 - сертификат ключа уполномоченного лица Удостоверяющего центра
 - карту клиента с логином и паролем для входа в информационную систему.
- Бланк заявления на формирование ключей подписи (Приложение № 2).
- Бланк заявления на создание сертификата ключа в двух экземплярах (Приложение № 3).
- Бланк заявления о заключении договоров (Приложение № 1).
- Сейф-пакет для обратной доставки документов.

2. Сотрудник ООО «АТОН» после идентификации потенциального Пользователя УЦ с помощью документа, удостоверяющего личность, передает ему комплект быстрой активации.

3. Потенциальный Пользователь УЦ вскрывает комплект и заполняет бланки заявлений, находящиеся в нем.

4. Сотрудник ООО «АТОН» проверяет правильность заполнения документов. При отсутствии ошибок он помещает заполненные документы вместе с копией документа, удостоверяющего личность потенциального Пользователя, в сейф-пакет обратной доставки и направляет его в УЦ.

6. УЦ, получив сейф-пакет обратной доставки и проверив правильность содержащихся в нем документов, после открытия счета Пользователю УЦ, формирует сертификат ключа.

7. Изготовленный сертификат ключа в виде электронного документа передается Пользователю УЦ на рабочее место автоматически или по электронной почте.

8. Полученный личный сертификат ключа Пользователь УЦ помещает на свой ключевой носитель.

9. УЦ заполняет заявление на выдачу сертификата ключа на бумажном носителе (по форме Приложения № 3), указывая следующие сведения:

- регистрационный номер сертификата,
- дату начала действия сертификата,
- дату окончания действия сертификата,
- уполномоченное лицо,
- основание полномочий.

10. Уполномоченный представитель УЦ подписывает заполненное заявление на изготовление сертификата ключа, заверяет печатью УЦ.

10.2. ПОДКЛЮЧЕНИЕ УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ К ИНФОРМАЦИОННОЙ СИСТЕМЕ ЧЕРЕЗ ПОСРЕДНИКОВ

1. В Удостоверяющем центре формируются комплекты быстрой активации для передачи посредникам. Каждый комплект включает, в том числе, следующие документы:

- сейф-пакет, запечатанный таким образом, что любая попытка его вскрытия не может остаться незамеченной, содержащий:
 - ключи электронной подписи;
 - Запрос сертификата с анонимными атрибутами;

- утилиту RUSH из состава СКЗИ «Крипто-КОМ 3.2» для вычисления контрольной суммы дистрибутивных файлов (контроля целостности);
 - сертификат ключа подписи уполномоченного лица Удостоверяющего центра
 - карту клиента с логином и паролем для входа в информационную систему.
- Бланк заявления на формирование ключей подписи (Приложение № 2)
 - Бланк заявления на создание сертификата ключа в двух экземплярах (Приложение № 3)
 - Бланк заявления о заключении договоров (Приложение № 1)
 - Сейф-пакет для обратной доставки документов.
2. Комплект быстрой активации передается посреднику.
3. Потенциальный Пользователь УЦ, получивший от посредника после идентификации посредником потенциального Пользователя УЦ с помощью документа, удостоверяющего личность, комплект быстрой активации, вскрывает конверт и заполняет бланки заявлений, находящиеся в конверте.
4. Посредник проверяет правильность заполнения документов. При отсутствии ошибок посредник помещает заполненные документы вместе с копией документа, удостоверяющего личность потенциального Пользователя УЦ, в сейф-пакет обратной доставки и направляет его в УЦ.
6. Уполномоченный представитель УЦ, получив сейф-пакет обратной доставки и проверив правильность содержащихся в нем документов, после открытия счета Пользователю УЦ формирует сертификат ключа.
7. Изготовленный сертификат ключа в виде электронного документа передается Пользователю УЦ на рабочее место автоматически или по электронной почте.
8. Полученный личный сертификат ключа Пользователь помещает на свой ключевой носитель.
9. УЦ заполняет заявление на выдачу сертификата ключа на бумажном носителе (по форме Приложения № 3), указывая следующие сведения:
- регистрационный номер сертификата,
 - дату начала действия сертификата,
 - дату окончания действия сертификата,
 - уполномоченное лицо,
 - основание полномочий.
10. Уполномоченный представитель УЦ подписывает заполненное заявление на изготовление сертификата ключа, заверяет печатью УЦ.

§ 11. Плановая смена ключей подписи Пользователя УЦ

1. Плановая смена ключей Пользователей УЦ производится в связи с истечением периода действия сертификата ключа Пользователя УЦ.
2. По истечении срока действия сертификат аннулируется, использование соответствующих ключей подписи прекращается.
3. Программное обеспечение Пользователя УЦ заблаговременно предупреждает его о предстоящей плановой смене ключей. Не позднее, чем за 40 (сорок) рабочих дней до истечения срока действия текущего сертификата ключа владелец сертификата должен выполнить процедуру плановой смены ключей: сформировать новые ключи и получить сертификат ключа.
4. Если владелец сертификата не успеет получить новый сертификат до истечения периода действия старого, документы, подписанные ключом, парным «устаревшему» сертификату, будут блокироваться при проверке электронной подписи.
5. В случае если Пользователь УЦ не успел обновить сертификат ключа до истечения периода его действия, обновление сертификата выполняется так же, как первоначальная сертификация при очном обращении (согласно п.9.2. настоящих Правил).

11.1. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ И ОБНОВЛЕНИЕ СЕРТИФИКАТА КЛЮЧА ПОЛЬЗОВАТЕЛЯ УЦ ПРИ УДАЛЕННОМ ОБРАЩЕНИИ

1. При наличии возможности пользователь УЦ самостоятельно с помощью ПО, разработанного на базе сертифицированного СКЗИ «Крипто-КОМ 3.2» и скопированным им в личном кабинете на странице www.aton-line.ru в сети «Интернет», выполняет генерацию ключей электронной подписи и формирует Запрос сертификата ключа.
2. Запрос сертификата ключа, сформированный Пользователем УЦ, в электронной форме импортируется в базу данных Удостоверяющего центра при наличии канала сетевого взаимодействия с УЦ автоматически или по электронной почте.
3. Пользователь УЦ распечатывает и подписывает заявление на выдачу сертификата ключа (по форме Приложения №3) и доставляет его в УЦ:
- при личном визите в ООО «АТОН»

- курьером, уполномоченным Пользователем УЦ доставлять, принимать, расписываться в получении документов;

- по почте России заказным письмом или письмом с объявленной ценностью.

4. При получении заявления Пользователя УЦ на выдачу сертификата ключа УЦ проверяет соответствие идентификационных данных Пользователя УЦ. В случае идентичности указанной информации УЦ изготавливает сертификат ключа на основании Запроса.

5. В случае отказа в изготовлении сертификата ключа Пользователь УЦ уведомляется об этом с указанием причины отказа.

6. Изготовленный сертификат ключа в виде электронного документа вместе с действующим сертификатом ключа уполномоченного лица УЦ передается Пользователю УЦ на рабочее место автоматически или по электронной почте.

7. УЦ заполняет заявление на выдачу сертификата ключа на бумажном носителе (по форме Приложения № 3), указывая следующие сведения:

- регистрационный номер сертификата,
- дату начала действия сертификата,
- дату окончания действия сертификата,
- уполномоченное лицо,
- основание полномочий.

8. Уполномоченный представитель УЦ подписывает заполненное заявление на изготовление сертификата ключа, заверяет печатью УЦ.

9. Полученный личный сертификат ключа и сертификат Удостоверяющего центра Пользователь помещает на свой ключевой носитель. Сертификат УЦ рекомендуется хранить на ключевом носителе вместе с закрытыми ключами Пользователя.

11.2. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ И ОБНОВЛЕНИЕ СЕРТИФИКАТА КЛЮЧА ПОЛЬЗОВАТЕЛЯ УЦ ПРИ УДАЛЕННОМ ОБРАЩЕНИИ С ИСПОЛЬЗОВАНИЕМ ДЕЙСТВУЮЩЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ.

1. При наличии возможности пользователь УЦ самостоятельно с помощью ПО, разработанного на базе сертифицированного СКЗИ «Крипто-КОМ 3.2» и скопированным им в личном кабинете на странице www.aton-line.ru в сети «Интернет», выполняет генерацию ключей электронной подписи и формирует Запрос сертификата ключа, который подписывает действующей электронной подписью.

2. Сформированный Запрос сертификата ключа в электронной форме автоматически импортируется в базу данных Удостоверяющего центра при наличии канала сетевого взаимодействия с УЦ.

3. В УЦ выполняется автоматическая проверка электронной подписи, содержащейся в поступившем Запросе.

4. При отсутствии ошибок в Запросе сертификата ключа, поступившем от Пользователя, Запрос передается на сертификацию.

5. Изготовленный сертификат ключа в виде электронного документа передается Пользователю на рабочее место автоматически или по электронной почте.

11.3. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ И ОБНОВЛЕНИЕ СЕРТИФИКАТА КЛЮЧА ПОЛЬЗОВАТЕЛЯ УЦ ПРИ ОЧНОМ ОБРАЩЕНИИ

1. Изготовление ключей и обновление сертификата ключа Пользователя УЦ осуществляется Удостоверяющим центром на основании заявления Пользователя о формировании ключей и заявления на изготовление сертификата ключа (по форме Приложений №№ 2, 3)

2. Обновление сертификата ключа в этом случае выполняется так же, как первоначальная сертификация при очном обращении (см.п.9.2).

§ 12. Внеплановая смена ключей Пользователя УЦ

1. Внеплановой считается замена сертификатов ключей по инициативе Пользователя УЦ, не связанная с истечением периода действия сертификата ключа пользователя УЦ.

Внеплановая смена ключей и обновление сертификата ключа осуществляются Пользователем УЦ в следующих случаях:

- при компрометации закрытого ключа Пользователя УЦ;
- при компрометации закрытого ключа уполномоченного лица УЦ;

- при компрометации ключевых носителей;
- в случае иных форс-мажорных обстоятельств.

2. При внеплановой смене ключей Пользователю УЦ необходимо:

При удаленном обращении:

- самостоятельно сформировать ключи и запрос сертификата ключа,
- подписать заявление о замене сертификата ключа с указанием причины замены и заявление на изготовление сертификата ключа и направить их в УЦ.

При очном обращении:

- подписать заявление о замене сертификата ключа с указанием причины замены, заявление на формирование ключей электронной подписи и заявление на изготовление сертификата ключа;
- получить сформированные УЦ ключи и сертификат ключа на каком-либо из типов носителя.

§ 13. Аннулирование (отзыв) сертификата ключа Пользователя УЦ

1. Аннулирование (отзыв) сертификата ключа Пользователя УЦ осуществляется:

- по заявлению владельца сертификата ключа;
- по заявлению на отзыв доверенности уполномоченного представителя Пользователя УЦ (для юридических лиц), зарегистрированного в Удостоверяющем центре;
- по решению Администрации УЦ.

2. Заявление на аннулирование (отзыв) сертификата ключа в бумажной форме подается Пользователем в УЦ лично, заказным письмом или курьерской связью.

3. Сертификат ключа Пользователя УЦ может быть аннулирован (отозван) по инициативе Администрации УЦ в случае:

- установленного факта компрометации закрытого ключа Пользователя УЦ;
- по указанию лиц или органов, имеющих такое право в силу закона.

§ 14. Уведомление о факте аннулирования (отзыва) сертификата ключа

1. В случаях аннулирования сертификата ключа Удостоверяющий центр выпускает соответствующие уведомления.

Официальным уведомлением владельца сертификата ключа о факте аннулирования (отзыва) сертификата является публикация Удостоверяющим центром Списка отозванных сертификатов (СОС), содержащего сведения об аннулированном (отозванном) сертификате.

2. Временем публикации считается время издания этого Списка.

§ 15. Дополнительные положения

15.1. ТРЕБОВАНИЯ К СРЕДСТВАМ ЭЛЕКТРОННОЙ ПОДПИСИ ПОЛЬЗОВАТЕЛЕЙ УЦ

Средство электронной подписи должно обеспечивать выполнение следующих процедур:

- генерацию закрытых и открытых ключей;
- формирование электронной подписи;
- проверку электронной подписи.

Средства электронной подписи должны обеспечивать выполнение мер защиты закрытых ключей (см. Раздел 4 § 2).

В качестве средства электронной подписи Пользователи УЦ должны использовать ПО, разработанное с использованием сертифицированных в соответствии с правилами сертификации средств криптографической защиты информации по уровню защиты КС1, КС2.

15.2. СМЕНА КЛЮЧЕЙ УПОЛНОМОЧЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Формирование ключей подписи и сертификата ключа уполномоченного лица УЦ выполняется УЦ с помощью программного обеспечения, разработанного на базе сертифицированного СКЗИ «Крипто-КОМ 3.2» .

Рекомендуемый срок действия сертификата ключа Удостоверяющего Центра 5 (пять) лет.

Плановая смена ключей Уполномоченного Лица Удостоверяющего центра выполняется не позднее, чем за 1 (один) год до окончания периода действия его закрытого ключа. Процедура плановой смены ключей Уполномоченного Лица УЦ (ключей УЦ) осуществляется в следующем порядке:

- УЦ формирует новый закрытый ключ и соответствующий ему новый открытый ключ и сертификат ключа УЦ;
- сформированный новый сертификат Удостоверяющего центра УЦ должен довести до всех Пользователей УЦ по надежному каналу сетевого взаимодействия;
- до окончания срока действия текущего секретного ключа Удостоверяющего центра Пользователи УЦ должны получить новый сертификат УЦ и добавить его в справочники сертификатов, не удаляя действующий сертификат УЦ;
- старый закрытый ключ Удостоверяющего центра используется в течение своего срока действия для формирования Списков отозванных сертификатов, изданных Удостоверяющим центром в период действия старого закрытого ключа УЦ.

РАЗДЕЛ 3. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТОВ

1. В случае возникновения конфликтов при использовании электронных документов, в частности, спора в отношении авторства, подлинности или целостности электронных документов, подписанных электронной подписи, применяется порядок разрешения конфликтов, предусмотренный настоящими Правилами.

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

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

4. Подтверждение подлинности электронной подписи в случае возникновения разногласий осуществляется с использованием программного обеспечения «Arbiter-PKI», разработанного ЗАО «Сигнал-Ком» на базе СКЗИ «Крипто-КОМ 3.2». Процедура подтверждения подлинности электронной подписи основывается на математических свойствах алгоритма электронной подписи, реализованного в соответствии с ГОСТ 34.10-2001.

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

6. Подлинность электронной подписи считается подтвержденной, если по итогам проверки подписи с использованием программного обеспечения «Arbiter-PKI» формируется следующее сообщение:

«Результат проверки: подпись подтверждена», а также символ «» или «»

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

8. Споры между Участниками и Удостоверяющим центром подлежат рассмотрению в Третейском суде Саморегулируемой организации «Национальная ассоциация участников фондового рынка». Решение данного третейского суда будет являться окончательным.

РАЗДЕЛ 4. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

§ 1. Система обеспечения информационной безопасности

1. Электронные документы, участвующие в электронном документообороте, и средства электронной подписи являются конфиденциальной информацией.

2. Участники обязаны соблюдать меры по обеспечению информационной безопасности при организации электронного документооборота.

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

- конфиденциальность информации (при передаче данных конфиденциальность обеспечивается использованием функций шифрования);

- целостность передаваемой информации (целостность защищаемых данных обеспечивается использованием функций электронной подписи электронного документа);
- аутентификацию (передаваемую информацию может получить только лицо, кому она предназначена, а отправителем является именно тот, от чьего имени она отправлена).
- неотказуемость от передачи электронного документа (невозможность отрицания факта отправления или получения передаваемой информации обеспечивается подписанием документа отправителем с использованием функций электронной подписи и хранением принимающей стороной документа с электронной подписи в течение установленного срока)
- защиту от переповторов (обеспечивается использованием криптографических функций электронной подписи, шифрования с добавлением уникального идентификатора сетевой сессии (электронного документа) с последующей его проверкой принимающей стороной или разработкой).
- защиту от навязывания информации (обеспечивается использованием функций электронной подписи с проверкой атрибутов электронного документа и открытого ключа отправителя).

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.).

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. Для проведения контроля целостности используется утилита *rush*, входящая в состав СКЗИ «Крипто-КОМ 3.2» .

§ 2. Меры защиты закрытых ключей

1. Закрытые ключи Пользователей УЦ при их генерации должны записываться на отчуждаемые носители ключевой информации.

2. Пользователь УЦ 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.

3. Закрытые ключи на отчуждаемом носителе необходимо защищать паролем. Пароль формирует лицо, выполняющее процедуру генерации ключей.

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

5. Не допускается использование одного и того же пароля для защиты нескольких закрытых ключей.

6. Доступ к закрытым ключам электронной подписи должен осуществляться только для выполнения действий, описанных в документации к системам электронного документооборота, в других случаях закрытые ключи электронной подписи должны быть недоступны.

7. Хранение закрытых ключей электронной подписи систем электронного документооборота, предоставляемых ООО «АТОН», 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.

8. Пересылка (передача) закрытых ключей электронной подписи по открытым каналам связи не допускается.

9. В целях обеспечения конфиденциальности ключей, вышедших из обращения, может применяться процедура уничтожения. Для уничтожения ключей с ключевых носителей используется утилита *wire*, входящая в состав СКЗИ «Крипто-КОМ 3.2», предназначенная для удаления файлов с ключевых носителей с предварительным их физическим затиранием.

§ 3. Компрометация ключевых носителей уполномоченного лица Удостоверяющего центра

1. В случае компрометации закрытого ключа уполномоченного лица Удостоверяющего центра выполняется аннулирование (отзыв) его сертификата.

2. Информация о факте компрометации ключей уполномоченного лица Удостоверяющего центра размещается на страницах www.aton-line.ru, а Пользователи УЦ оповещаются о компрометации путем соответствующей рассылки по электронной почте.

3. Процедура внеплановой смены скомпрометированных ключей уполномоченного лица Удостоверяющего центра осуществляется в соответствии с порядком, установленным в п.15.2 настоящих Правил для процедуры плановой смены ключей уполномоченного лица УЦ.

4. Все действующие (на момент компрометации), а также приостановленные, сертификаты ключей, подписанные с использованием скомпрометированного закрытого ключа уполномоченного лица Удостоверяющего центра, считаются аннулированными (отозванными) и подлежат внеплановой смене.

§ 4. Компрометация ключевых носителей Пользователя УЦ

1. Пользователь УЦ (юридическое или физическое лицо) самостоятельно принимает решение о факте или угрозе компрометации своего закрытого ключа.

2. К событиям, относящимся к явной компрометации ключевых носителей, относятся:

- утрата ключевых носителей и (или) оборудования, содержащего ключевые носители;
- утрата ключевых носителей и (или) оборудования, содержащего ключевые носители с последующим обнаружением;
- для юридических лиц: увольнение сотрудников, имевших доступ к ключевым носителям;
- обнаружение нарушения правил хранения ключевых носителей.

3. К событиям неявной компрометации закрытого ключа могут быть отнесены следующие подозрения:

- возникновение подозрений на утечку информации или ее искажение на оборудовании, содержащем закрытый ключ (например, в случае обнаружения вирусного заражения средствами антивирусной защиты, установки нелегального программного обеспечения и т.д.);
- нарушение печати на сейфе, хранилище ключевого носителя, содержащего закрытый ключ;
- доступ третьих лиц к оборудованию, содержащему закрытый ключ;
- другие случаи, когда нельзя достоверно установить, что произошло с ключевым носителем, содержащим закрытый ключ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий третьих лиц).

При наступлении одного из вышеперечисленных событий, отнесенных к неявной компрометации закрытого ключа, владельцу необходимо произвести оценку ситуации и самостоятельно принять решение по дальнейшему использованию ключевого носителя, содержащего закрытый ключ.

4. В случае компрометации или угрозы компрометации закрытого ключа Пользователь УЦ прекращает его использование, обращается в Удостоверяющий Центр с заявлением об аннулировании (отзыве) сертификата ключа, соответствующего скомпрометированному ключу. Ответственность за несвоевременное информирование УЦ, в том числе за возможные последующие негативные события, произошедшие в результате компрометации закрытого ключа, возлагается только на Пользователя.

5. УЦ помещает соответствующий сертификат в Список отозванных сертификатов (СОС) с указанием причины «Компрометация ключа» и публикует СОС в сетевом справочнике сертификатов.

§ 5. Компрометация пароля для доступа в информационную систему

1. Под компрометацией пароля понимается утрата доверия к тому, что пароль известен только его владельцу.

2. К событиям, относящимся к явной компрометации пароля, могут быть отнесены следующие:

- получение Карты клиента в поврежденном конверте;

- утеря Карты клиента;
- временная утеря Карты клиента, содержащей пароль, с последующим обнаружением (возвратом);
- для юридических лиц: увольнение уполномоченных сотрудников со стороны клиента, имевших доступ к паролю;
- нарушение правил хранения и (или) уничтожения пароля;
- раскрытие пароля при разговоре (в том числе при общении с сотрудниками ООО «АТОН»).

При наступлении одного из вышеперечисленных событий, отнесенных к явной компрометации пароля, Пользователю УЦ необходимо незамедлительно сообщить о произошедшем в УЦ.

3. К неявной компрометации пароля могут быть отнесены следующие события:

- возникновение подозрений на утечку информации о пароле, хранящемся владельцем на оборудовании (например, в случае обнаружения вирусного заражения средствами антивирусной защиты, установки нелегального программного обеспечения, передачу оборудования в сервисный центр и т.д.);
- нарушение печати на сейфе (хранилище) пароля;
- другие события, произошедшие при работе с паролем (например, при работе в общественных местах)

При наступлении одного из вышеперечисленных событий, отнесенных к неявной компрометации пароля, владельцу необходимо произвести оценку ситуации и самостоятельно принять решение по дальнейшему использованию пароля.

4. Ответственность за несвоевременное информирование УЦ, в том числе за возможные последующие негативные события, произошедшие в результате компрометации пароля, возлагается только на Пользователя.

ПРОЧИЕ ПОЛОЖЕНИЯ

§ 1. Тарифы на услуги Удостоверяющего центра. Порядок расчетов

1. Участник обязан оплачивать услуги, а также возмещать расходы, понесенные ООО «АТОН» в связи с оказанием услуг Удостоверяющего центра.

1.1. Размер и порядок оплаты услуг Удостоверяющего центра устанавливаются Тарифами на услуги Удостоверяющего центра ООО «АТОН», являющимися Приложением № 6 к настоящим Правилам.

1.2. Расходы Удостоверяющего центра ООО «АТОН» подлежат возмещению по мере их возникновения при условии их предварительного согласования с Участником.

1.3. Участник, допустивший просрочку исполнения обязательств по расчетам, обязан по письменному требованию ООО «АТОН» уплатить пеню в размере двух десятых процента от несвоевременно уплаченной суммы за каждый день просрочки платежа. Неустойка подлежит уплате Участником в течение 10 (Десяти) дней с даты письменного требования Удостоверяющего центра.

2. Внесение изменений в Тарифы Удостоверяющего центра ООО «АТОН» осуществляется в порядке, установленном для внесения изменений в настоящие Правила

3. Если Участник не является клиентом ООО «АТОН» по договору о брокерском обслуживании, то Участник обязан с 5 (пятого) по 10 (десятый) рабочий день по окончании календарного месяца, в котором между Участником и Удостоверяющим центром заключено Соглашение об ЭДО, получить в ООО «АТОН» счет-фактуру, содержащую сведения о подлежащем уплате вознаграждении Удостоверяющего центра. Уплата вознаграждения Удостоверяющего центра должна быть осуществлена Участником одновременно в течение 15 (пятнадцати) рабочих дней по окончании календарного месяца, в котором между Участником и Удостоверяющим центром заключено Соглашение об ЭДО.

4. Если Участник одновременно является клиентом ООО «АТОН» по договору о брокерском обслуживании, то размер и порядок оплаты услуг и возмещения расходов ООО «АТОН» устанавливаются Регламентом оказания ООО «АТОН» брокерских услуг на рынке ценных бумаг и Тарифными планами ООО «АТОН» являющимися Приложением №23 к Регламенту.

§ 2. Приложения к настоящим Правилам

К настоящим Правилам прилагаются и являются их неотъемлемой частью:

Приложение № 1. Заявление о заключении договоров;

Приложение № 2. Заявление на формирование ключей электронной подписи

Приложение № 3. Заявление на выдачу Сертификата ключа;

Приложение № 4. Заявление на внеплановую замену ключа электронной подписи и сертификата ключа электронной подписи

Приложение № 5. Заявления о замене логина-пароля для входа в информационную систему

Приложение № 6. Тарифы на услуги Удостоверяющего центра ООО «АТОН»

ЗАЯВЛЕНИЕ О ЗАКЛЮЧЕНИИ ДОГОВОРОВ путем присоединения к условиям оказания ООО «АТОН» услуг на рынках ценных бумаг и порядку функционирования корпоративной информационной системы ООО «АТОН»

Клиент заявляет о намерении заключить следующий договор (договоры) путем присоединения к установленным ООО «АТОН» стандартным условиям:

Договор о брокерском обслуживании на рынке ценных бумаг
(Брокерское обслуживание клиента на рынке ценных бумаг включает в себя услуги по совершению маржинальных сделок и срочных сделок, если совершение таких сделок клиентом не запрещено правовыми актами Российской Федерации.)

Депозитарный договор

Соглашение об электронном документообороте

Клиент заявляет о согласии использовать электронную цифровую подпись в документообороте между клиентом и ООО «АТОН».
Использование электронной цифровой подписи допускается при условии, что клиент или уполномоченное им лицо является владельцем сертификата ключа электронной цифровой подписи, выданного удостоверяющим центром, определенным ООО «АТОН».

Документы, устанавливающие стандартные условия договоров об оказании клиенту услуг и о порядке взаимодействия сторон:

- «Регламент оказания ООО «АТОН» брокерских услуг на рынках ценных бумаг» и приложения к нему – условия брокерского обслуживания на рынке ценных бумаг (включая маржинальные и срочные сделки)
- «Условия осуществления депозитарной деятельности ООО «АТОН»» и приложения к ним – условия депозитарного договора;
- «Правила электронного документооборота ООО «АТОН»» и приложения к ним – порядок функционирования информационной системы, обеспечивающей передачу электронных документов между участниками данной системы, а также порядок использования электронной цифровой подписи в документообороте между клиентом и ООО «АТОН»;
- «Тарифные планы ООО «АТОН» на оказание услуг на рынках ценных бумаг» - размер оплаты услуг и возмещения расходов ООО «АТОН» по заключенным договорам.

ООО «АТОН» в одностороннем порядке утверждает и вносит изменения в вышеуказанные документы. О вступлении в силу изменений к данным документам ООО «АТОН» обязано уведомлять клиента не позднее, чем за 10 (десять) рабочих дней. Текст вышеуказанных документов и уведомления об их изменении размещаются в сети «Интернет» (www.skrin.ru). Иные уведомления и требования, адресованные клиенту, предоставляются клиенту путем их размещения в сети «Интернет» (www.aton-line.ru). Риск неблагоприятных последствий, вызванных неполучением клиентом информации, размещенной в сети «Интернет», несет клиент. ООО «АТОН» вправе изменить указанные адреса в сети «Интернет», опубликовав соответствующее уведомление в периодическом печатном издании, распространяемом на территории Российской Федерации тиражом не менее 50 000 (Пятидесяти тысяч) экземпляров не позднее, чем за 10 (Десять) дней.

Клиент подтверждает:

- ознакомление и согласие со всеми условиями и требованиями, установленными вышеуказанными документами;
- ознакомление с декларацией о рисках, связанных с осуществлением операций на рынке ценных бумаг (в том числе – при совершении маржинальных и необеспеченных сделок);
- ознакомление с декларациями о рисках, связанных с осуществлением операций с ценными бумагами, включенными в котировальные списки "И", (по формам, утвержденным ОАО «РТС» и ЗАО «ФБ ММББ»);
- получение письменного уведомления, содержащего информацию о том, что денежные средства клиента будут учитываться на специальном брокерском счете (счетах) вместе со средствами других клиентов (за исключением случаев, когда это запрещено правовыми актами Российской Федерации), а также о рисках, возникающих при учете средств клиента на одном счете со средствами других клиентов; информацию о возможности и условиях открытия отдельного специального брокерского счета для учета денежных средств клиента; информацию о возможности и условиях использования брокером в собственных интересах денежных средств клиента (за исключением случаев, когда это запрещено правовыми актами Российской Федерации), а также о возникающих в данной связи рисках, в том числе, связанных с возможностью зачисления денежных средств на собственный счет брокера; информацию о порядке внутреннего учета денежных средств клиента, находящихся на специальном брокерском счете (счетах) и (или) собственном счете брокера, и отчетности брокера перед клиентом; информацию о кредитных организациях, на счетах в которой будут учитываться средства клиента, включающую информацию, опубликование которой предусмотрено федеральными законами;
- получение отчета об операции по открытию клиенту счета депо (в случае заключения Депозитарного договора);
- факт уведомления о наличии у клиента прав и гарантий, установленных Федеральным законом «О защите прав и законных интересов инвесторов на рынке ценных бумаг», а также о совмещении ООО «АТОН» депозитарной деятельности с брокерской и дилерской деятельностью на рынке ценных бумаг;
- факт уведомления о том, что если подана настоящая заявка не была предварительно согласована клиентом с ООО «АТОН», ООО «АТОН» вправе отказать клиенту в оказании предусмотренных настоящей заявкой услуг.

Все споры между клиентом и ООО «АТОН» подлежат рассмотрению в Третейском суде Саморегулируемой организации «Национальная ассоциация участников фондового рынка». Решение данного третейского суда будет являться окончательным.

Клиент (в случае заключения депозитарного договора – депонент) поручает ООО «АТОН» осуществлять списание со счета депо и зачисление на счет депо ценных бумаг, а также осуществлять иные необходимые операции для исполнения сделок, совершенных за счет клиента (депонента) в рамках договора о брокерском обслуживании на рынке ценных бумаг между клиентом (депонентом) и ООО «АТОН». Состав и количество ценных бумаг, с которыми должны быть осуществлены операции для исполнения сделок; сроки осуществления операций; лица, на счета (со счетов) которых должны быть переведены ценные бумаги; а также иные необходимые сведения определяются на основании условий соответствующих сделок. Настоящее поручение действует до его отмены.

Сведения о клиенте									
Фамилия, имя, отчество (полностью)									
Паспорт		серия / №				дата выдачи			
		выдавший орган							
ИНН									
Контактные телефоны									
Электронная почта									
Адрес для отправки корреспонденции									
Реквизиты банковского счета в рублях РФ	расчетный счет								
	наименование банка								
	БИК банка			место нахождения банка (город)					
	корреспондентский счет банка								
лицевой счет (при наличии)									
Дополнительная информация									

Заполняется, если заявление подписывается по доверенности	
№ доверенности	Дата выдачи

Заполняется прописью, без сокращений, клиентом или представителем клиента!	
_____ фамилия	
_____ имя	
_____ отчество	_____ подпись

Заполняется ООО «АТОН»									
№ / код договора (брокерского счета, счета депо)									
Дата заключения договора									

ЗАЯВЛЕНИЕ О ЗАКЛЮЧЕНИИ ДОГОВОРОВ путем присоединения к условиям оказания ООО «АТОН» услуг на рынках ценных бумаг и порядку функционирования корпоративной информационной системы ООО «АТОН»

Клиент заявляет о намерении заключить следующий договор (договоры) путем присоединения к установленным ООО «АТОН» стандартным условиям:

- Договор о брокерском обслуживании на рынке ценных бумаг**
(Брокерское обслуживание клиента на рынке ценных бумаг включает в себя услуги по совершению маржинальных сделок и срочных сделок, если совершение таких сделок клиентом не запрещено правовыми актами Российской Федерации.)
- Депозитарный договор** счет владельца; счет доверительного управляющего
- Договор о междепозитарных отношениях** (счет номинального держателя)
- Соглашение об электронном документообороте**

Клиент заявляет о согласии использовать электронную цифровую подпись в документообороте с ООО «АТОН».

Использование электронной цифровой подписи допускается при условии, что клиент или уполномоченное им лицо является владельцем сертификата ключа электронной цифровой подписи, выданного удостоверяющим центром, определенным ООО «АТОН».

Документы, устанавливающие стандартные условия договоров об оказании клиенту услуг и о порядке взаимодействия сторон:

- «Регламент оказания ООО «АТОН» брокерских услуг на рынках ценных бумаг» и приложения к нему – условия брокерского обслуживания на рынке ценных бумаг (включая маржинальные и срочные сделки);
- «Условия осуществления депозитарной деятельности ООО «АТОН» и приложения к ним – условия депозитарного договора;
- «Правила электронного документооборота ООО «АТОН»» и приложения к ним – порядок функционирования информационной системы, обеспечивающей передачу электронных документов между участниками данной системы, а также порядок использования электронной цифровой подписи в документообороте между клиентом и ООО «АТОН»;
- «Тарифные планы ООО «АТОН» на оказание услуг на рынках ценных бумаг» – размер оплаты услуг и возмещения расходов ООО «АТОН» по заключенным договорам

ООО «АТОН» в одностороннем порядке утверждает и вносит изменения в вышеуказанные документы. О вступлении в силу изменений к данным документам ООО «АТОН» обязано уведомлять клиента не позднее чем за 10 (Десять) рабочих дней. Текст вышеуказанных документов и уведомления об их изменении размещаются в сети «Интернет» (www.skrin.ru). Иные уведомления и требования, адресованные клиенту, направляются клиенту путем их размещения в сети «Интернет» (www.aton-line.ru). Риск неблагоприятных последствий, вызванных неполучением клиентом информации, размещенной в сети «Интернет», несет клиент. ООО «АТОН» вправе заменить указанные адреса в сети «Интернет», опубликовав соответствующее уведомление в периодическом печатном издании, распространяемом на территории Российской Федерации тиражом не менее 50 000 (Пятидесяти тысяч) экземпляров не позднее чем за 10 (Десять) дней.

Клиент подтверждает:

- ознакомление и согласие со всеми условиями и требованиями, установленными вышеуказанными документами;
- ознакомление с декларацией о рисках, связанных с осуществлением операций на рынке ценных бумаг (в том числе – при совершении маржинальных и необеспеченных сделок) и срочных сделок.
- ознакомление с декларациями о рисках, связанных с осуществлением операций с ценными бумагами, включенными в котировальные списки "И", (по формам, утвержденным ОАО «РТС» и ЗАО «ФБ ММББ»).
- получение письменного уведомления, содержащего информацию о том, что денежные средства клиента будут учитываться на специальном брокерском счете (счетах) вместе со средствами других клиентов (за исключением случаев, когда это запрещено правовыми актами Российской Федерации), а также о рисках, возникающих при учете средств клиента на одном счете со средствами других клиентов; информацию о возможности и условиях открытия отдельного специального брокерского счета для учета денежных средств клиента; информацию о возможности и условиях использования брокером в собственных интересах денежных средств клиента (за исключением случаев, когда это запрещено правовыми актами Российской Федерации), а также о возникающих в данной связи рисках, в том числе связанных с возможностью зачисления денежных средств на собственный счет брокера; информацию о порядке внутреннего учета денежных средств клиента, находящихся на специальном брокерском счете (счетах) и (или) собственном счете брокера, и отчетности брокера перед клиентом; информацию о кредитных организациях, на счетах в которой будут учитываться средства клиента, включающую информацию, опубликованную которой предусмотрено федеральными законами;
- получение отчета об операции по открытию клиенту счета депо (в случае заключения депозитарного договора или договора о междепозитарных отношениях)
- факт уведомления о наличии у клиента прав и гарантий, установленных Федеральным законом «О защите прав и законных интересов инвесторов на рынке ценных бумаг», а также о совмещении ООО «АТОН» депозитарной деятельности с брокерской и дилерской деятельностью на рынке ценных бумаг;
- факт уведомления о том, что если подача настоящего заявления не была предварительно согласована клиентом с ООО «АТОН», ООО «АТОН» вправе отказать клиенту в оказании предусмотренных настоящим заявлением услуг.

Все споры между клиентом и ООО «АТОН» подлежат рассмотрению в Третейском суде Саморегулируемой организации «Национальная ассоциация участников фондового рынка». Решение данного третейского суда будет являться окончательным.

Клиент (в случае заключения депозитарного договора - депонент) поручает ООО «АТОН» осуществлять списание со счета депо и зачисление на счет депо ценных бумаг, а также осуществлять иные необходимые операции для исполнения сделок, совершенных за счет клиента (депонента) в рамках договора о брокерском обслуживании на рынке ценных бумаг между клиентом (депонентом) и ООО «АТОН». В случае подачи клиентом (депонентом) уведомления в ООО «АТОН» о соответствии счета депо брокерскому счету (портфелю), списание, зачисление ценных бумаг и иные операции по соответствующему счету депо должны осуществляться для исполнения сделок, совершенных в рамках договора о брокерском обслуживании на рынке ценных бумаг, заключенного между ООО «АТОН» и клиентом, подписавшим данное уведомление совместно с клиентом (депонентом). Состав и количество ценных бумаг, с которыми должны быть осуществлены операции для исполнения сделок; сроки осуществления операций; лица, на счета (со счетов) которых должны быть переведены ценные бумаги; а также иные необходимые сведения определяются на основании условий соответствующих сделок. Настоящее поручение действует до его отмены.

Сведения о клиенте

Полное наименование			
Сокращенное наименование			
ОГРН		Дата регистрации	
Место регистрации (страна)			
Место нахождения, указанное в учредительных документах			
Адрес для отправки корреспонденции			
ИНН / код иностр. организации			
Контактные телефоны			
Электронная почта			
Реквизиты банковского счета в рублях РФ	расчетный счет		
	наименование банка		
	БИК банка	место нахождения банка (город)	
	корреспондентский счет банка		
Дополнительная информация			

Сведения о лице, подписывающем заявление

ФИО			
Должность			
Основание полномочий			
Заполняется, если заявление подписывается по доверенности			
№ доверенности		Дата выдачи	

Заполняется ООО «АТОН»

№ / код договора (брокерского счета, счета депо)										
Дата заключения договора										

подпись _____

МП _____

СЕРТИФИКАТ КЛЮЧА ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ

сведения о владельце сертификата																								
ФИО																								
документ, удостоверяющий личность	наименование										дата выдачи													
	выдавший орган																							
	серия/№																							
фактический адрес																								
сведения о сертификате	регистрационный номер										окончание действия													
	начало действия																							
<p>Наименование и место нахождения удостоверяющего центра: Общество с ограниченной ответственностью «АТОН»; 115035, город Москва, Овчинниковская набережная, дом 20, строение 1. Наименование средств электронно-цифровой подписи, с которыми используется открытый ключ электронной подписи: СКЗИ «Крипто-КОМ 3.2». Электронные документы с электронной подписью, открытый ключ которой содержится в настоящем сертификате, будут иметь юридическое значение в гражданско-правовых отношениях.</p>																								
открытый ключ электронной подписи																								
<p>Права и обязанности владельца сертификата и удостоверяющего центра, возникающие в процессе создания и использования ключей электронной подписи и сертификатов, а также иные сопутствующие отношения, регламентируются Правилами удостоверяющего центра ООО «АТОН» (далее – Правилами). Удостоверяющий центр вправе в одностороннем порядке вносить изменения в Правила, уведомляя владельца сертификата не позднее, чем за десять рабочих дней до вступления изменений в силу. Правила и уведомления об их изменении размещаются на странице www.skrin.ru в сети «Интернет». Удостоверяющий центр вправе заменить указанный адрес в сети «Интернет», опубликовав соответствующее уведомление в периодическом печатном издании, распространяемом на территории Российской Федерации тиражом не менее пятидесяти тысяч экземпляров не позднее чем за десять дней. Споры между владельцем сертификата и удостоверяющим центром подлежат рассмотрению в Третейском суде Саморегулируемой организации «Национальная ассоциация участников фондового рынка». Решение данного третейского суда будет являться окончательным.</p>																								
<p>Настоящей подписью владелец сертификата подтверждает: (а) получение СКЗИ «Крипто-КОМ 3.2»; (б) направление удостоверяющему центру настоящего заявления на выдачу сертификата ключа; (в) согласие руководствоваться в отношениях с удостоверяющим центром вышеуказанными положениями, включая третейскую оговорку, и Правилами.</p>												<p>Настоящей подписью удостоверяющий центр подтверждает: (а) передачу СКЗИ «Крипто-КОМ 3.2»; (б) выдачу настоящего сертификата ключа; (в) согласие руководствоваться в отношении с владельцем сертификата вышеуказанными положениями, включая третейскую оговорку, и Правилами.</p>												
дата подписания										уполномоченное лицо														
_____ / _____ подпись расшифровка										основание полномочий														
Для отметок ООО «АТОН»										КОММЕРЧЕСКАЯ ТАЙНА Общество с ограниченной ответственностью «АТОН» 115035, город Москва, Овчинниковская набережная, дом 20, строение 1														

В Удостоверяющий центр
ООО «АТОН»

ЗАЯВЛЕНИЕ
на внеплановую замену ключа электронной подписи и
сертификата ключа электронной подписи

Число

Месяц

Год

Клиент: _____
ФИО

_____ Паспортные данные (серия, номер, дата выдачи, выдавший орган)

№/Код брокерского счета (договора): _____

Прошу произвести замену ключа электронной подписи и сертификата ключа электронной подписи в связи с

_____ Причина замены

Подпись _____ / _____ /

Для отметок ООО «АТОН»

**В Удостоверяющий центр
«ООО АТОН»**

От клиента _____
_____ (ФИО)

Прошу произвести замену логина и пароля в связи с _____

_____ / _____ /
подпись расшифровка

«__» _____ 20__ года

Тарифы на услуги Удостоверяющего центра ООО «АТОН»

Под тарифами на услуги Удостоверяющего центра ООО «АТОН» понимаются установленные ставки вознаграждения ООО «АТОН» за оказание услуг Удостоверяющего центра, предусмотренные Правилами электронного документооборота ООО «АТОН».

Участник оплачивает услуги Удостоверяющего центра по указанным тарифам, увеличенным на сумму НДС в порядке, установленном действующим законодательством РФ.

Вознаграждение рассчитывается как результат сложения цен на все услуги, указанные в Тарифном плане, которыми воспользовался Участник в связи с заключением Соглашения об ЭДО с Удостоверяющим центром.

№	Вид услуги	Цена, руб	Примечание
1	Комплект средств ЭЦП для работы в системе электронного документооборота АТОН (комплект №1)	2900	В состав комплекта входит: - изготовление по обращению владельца сертификата ключа подписи одного сертификата ключа подписи, включая генерацию ключей ЭЦП. Максимальный срок действия сертификата ключа подписи - 455 дней; - один комплект сертифицированных программных средств криптографической защиты информации для работы с ЭЦП на базе СКЗИ Крипто-Ком 3.2; - один сертифицированный электронный ключевой носитель «Rutoken» для хранения сертификата и ключей ЭЦП.
2	Комплект средств ЭЦП для работы в системе электронного документооборота АТОН (комплект № 2)	2300	В состав комплекта входит: - изготовление по обращению владельца сертификата ключа подписи одного сертификата ключа подписи, включая генерацию ключей ЭЦП. Максимальный срок действия сертификата ключа подписи - 455 дней - один комплект сертифицированных программных средств криптографической защиты информации для работы с ЭЦП на базе СКЗИ Крипто-Ком 3.2; - USB- ключевой носитель для записи и хранения и ключей ЭЦП
3	Изготовление сертификата ключа подписи для работы в системе электронного документооборота АТОН	500	Изготовление и обслуживание одного сертификата ключа подписи, включая генерацию ключей ЭЦП по обращению владельца сертификата ключа подписи. Максимальный срок действия сертификата ключа подписи - 455 дней. Ключевой носитель предоставляется пользователем УЦ или приобретается отдельно.
4	Подтверждение подлинности электронной цифровой подписи в электронном документе	1000	Осуществляется по обращению Пользователей УЦ при необходимости получения письменного подтверждения от Удостоверяющего центра подлинности ЭЦП в электронном документе.
5	Электронный ключ «Rutoken»	900	Защищенный USB- ключевой носитель для записи и хранения ключей ЭЦП.
6	Карта флэш-памяти (1Gb)\	300	USB- ключевой носитель для записи и хранения ключей ЭЦП.
7	Cd-диск (210 mb)	27	Оптический ключевой носитель для записи и хранения ключей ЭЦП.