Утверждено приказом от 18 февраля 2020 года

Генеральный директор ООО «АТОН»
А.М. Звездочкин

ПРАВИЛА
ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
ООО «АТОН»

(редакция, действующая с 25 февраля 2020 года)

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

§ 1. Основные термины и определения

Адрес электронной почты Участника – адрес электронной почты, владельцем которого является только участник электронного взаимодействия.

Аутентификация – проверка принадлежности участнику электронного взаимодействия предъявленного им идентификатора, подтверждение подлинности идентификатора.

Администратор удостоверяющего центра *(далее – «Администратор УЦ»)* – уполномоченный представитель удостоверяющего центра, ответственный за выполнение операций по изготовлению и обслуживанию сертификатов.

Графический пользовательский интерфейс – графическая среда организации действий на сайте www.aton.ru, в личном кабинете Участника на странице www.aton.ru или web.atonspace.ru в сети «Интернет».

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

Журнал событий/записей - отчет об операциях, технический протокол, создаваемый программно-техническими средствами ООО «АТОН», который фиксирует все действия/события, совершаемые Участниками электронного взаимодействия в информационных системах.

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

Идентификатор устройства - это уникальный идентификатор устройства с установленным на нем Мобильным приложением.

Идентификация – процедура присвоения участникам электронного взаимодействия некоторого идентификатора и/или сравнение предъявленного идентификатора с идентификатором этого участника, содержащимся в перечне присвоенных идентификаторов.

ИТС QUIK – информационная торговая система, предназначенная, в том числе, для торговли на финансовом рынке, подачи ООО «АТОН» поручений и обмена иными сообщениями, разработанная ARQA Technologies (ООО "АРКА ТЕКНОЛОДЖИЗ").

Ключевой носитель - материальный носитель, содержащий один или несколько криптографических ключей.

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

Конфликтная ситуация - ситуация, при которой у участника электронного взаимодействия возникает необходимость разрешения вопросов принадлежности усиленной неквалифицированной электронной подписи участнику и/или подлинности электронных документов, обработанных средствами криптографической защиты информации.

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

Личный кабинет – раздел на сайте www.aton.ru, web.atonspace.ru, https://www.interactivebrokers.co.uk, в сети «Интернет», доступ к которому осуществляется после аутентификации участника электронного взаимодействия, используемый для предоставления в электронной форме отчетов, подачи поручений, распоряжений, инструкций, обмена иными документами и информацией между ООО «АТОН» и участником электронного взаимодействия/участниками электронного взаимодействия между собой в соответствии с настоящими Правилами и иными соглашениями, заключенными между участником электронного взаимодействия и ООО «АТОН»/ участниками электронного взаимодействия.

Мобильное приложение – программное приложение для использования его на мобильных устройствах, на платформах Android и iOS, доступное для скачивания через официальные Интернет-магазины Google Play или AppStore.

Мобильное приложение Aton Line - мобильная версия кабинета клиента - один из каналов обмена информацией и электронными документами между ООО «АТОН» и участниками электронного взаимодействия.

Мобильное приложение Aton Space – один из каналов обмена информацией и электронными документами между ООО «АТОН» и участниками электронного взаимодействия. Посредством Мобильного приложения Aton Space участник электронного взаимодействия осуществляет пользование ресурсами сети ATON SPACE.

Информационная торговая система Aton Trading - мобильное приложение Aton Trading или раздел на сайте, предназначенные для торговли на международных рынках через ООО «АТОН» с привлечением иностранного брокера, подачи поручений и обмена иными сообщениями в связи с оказанием ООО «АТОН» услуг по совершению сделок на международных рынках.

Мобильное устройство – техническое устройство участника электронного взаимодействия (смартфон или электронный планшет) на базе операционных систем iOS и Android, посредством которого участник электронного взаимодействия использует Мобильное приложение.

Номер мобильного телефона Участника – абонентский номер участника электронного взаимодействия /уполномоченного лица участника электронного взаимодействия в сети подвижной радиотелефонной связи одного из российских операторов сотовой связи.

Одноразовый пароль (код) – последовательность символов, которая используется для идентификации лица, подписавшего электронный документ в Мобильном приложении или Личном Кабинете. Одноразовый пароль (код) направляется в тексте СМС-уведомления на Номер мобильного телефона Участника, зарегистрированный в ООО «АТОН», либо PUSH – уведомления на Мобильное устройство участника электронного взаимодействия, идентификатор которого зарегистрирован в ООО «АТОН».

Пакет электронных документов - несколько связанных между собой электронных документов

Плановая смена ключей – регламентируемая Администратором УЦ периодическая смена ключей участников электронного взаимодействия и уполномоченного лица удостоверяющего центра, не вызванная их компрометацией.

Регистрационный центр *(далее – «РЦ»)* – опциональный субъект инфраструктуры ключей проверки электронных подписей, отвечающий за идентификацию и аутентификацию участников электронного взаимодействия, претендующих на получение сертификата, но не подписывающий и не выпускающий сертификаты (Удостоверяющий центр делегирует Регистрационному центру часть своих полномочий).

Свертка документа (хэш-функция) – контрольная сумма электронного документа, которая рассчитывается с использованием 256 битного алгоритма хеширования. Изменение содержания документа приводит к изменению его свертки.

СМС (SMS) (Short Message Service – служба коротких сообщений) – технология, позволяющая осуществлять прием и передачу коротких текстовых сообщений при помощи мобильного телефона.

СМС-уведомление – отправка ООО «АТОН» короткого текстового сообщения, состоящего из букв или символов, набранных в определенной последовательности, предназначенного для передачи одноразового пароля по сети подвижной радиотелефонной связи участнику электронного взаимодействия.

Список аннулированных сертификатов – реестр аннулированных сертификатов, в форме электронного документа с электронной подписью уполномоченного лица удостоверяющего центра, в том числе включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, информацию о датах аннулирования сертификатов ключей проверки электронных подписей.

Уникальная ссылка - это уникальный единый указатель ресурса (URL), который ссылается на уникальный раздел сайта www.aton.ru, отличный от Личного кабинета, используемый для организации электронного документооборота между ООО «АТОН» и Участником в соответствии с настоящими Правилами. Уникальная ссылка и уникальный раздел сайта www.aton.ru создаются индивидуально для каждого Участника и существуют ограниченное время, продолжительность которого определяется по усмотрению ООО «АТОН»[1].

Электронный документ – документированная информация, представленная в электронной форме.

Электронный документооборот *(далее – «ЭДО»)* - обмен в информационной системе электронными документами между ООО «АТОН» и участниками электронного взаимодействия (далее – «Участниками»), а также между отдельными Участниками в соответствии с настоящими Правилами.

Aton Space - веб платформа, использующаяся для обмена информацией и размещения аналитических материалов в области финансовых рынков, предоставления участникам электронного взаимодействия отчетов, подачи поручений, распоряжений, инструкций, обмена иными документами и информацией между ООО «АТОН» и участником электронного взаимодействия/участниками электронного взаимодействия между собой в соответствии с настоящими Правилами и иными соглашениями, заключенными между участником электронного взаимодействия и ООО «АТОН»/ участниками электронного взаимодействия. Aton Space имеет несколько равнозначных интерфейсов доступа – веб интерфейс по адресу web.atonspace.ru и мобильное приложение Aton Space.

iQUIK X - пользовательское приложение ИТС QUIK, разработанное для мобильных устройств на базе операционных систем iOS и Android.

PUSH – уведомление – короткое текстовое сообщение, направляемое ООО «АТОН» Участнику в виде всплывающего сообщения на экране Мобильного устройства, на которое установлено Мобильное приложение.

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

Термины, не определенные в настоящих Правилах, используются в значениях, определенных действующим законодательством Российской Федерации (далее – «РФ»).

§ 2. Предмет регулирования настоящих Правил

1. Настоящие Правила устанавливают общий порядок электронного документооборота в информационных системах, а также порядок создания, выдачи и обслуживания Удостоверяющим центром ООО «АТОН» (далее – «УЦ») сертификатов ключей проверки электронных подписей (далее –«Сертификатов ключей») и осуществления ООО «АТОН» иных функций, предусмотренных настоящими Правилами, в рамках соответствующей информационной системы.

Информационная система (далее – «Информационная система») – система, предназначеная для осуществлении взаимодействия между:

1.1. ООО «АТОН» и Участниками в области оказания ООО «АТОН» услуг на рынках ценных бумаг, а также оказания ООО «АТОН» услуг по совершению сделок с иностранной валютой на организованных торгах ПАО Московская Биржа, услуг по учету иностранных финансовых инструментов, которые в соответствии с действующим законодательством не квалифицированы в качестве ценных бумаг.

1.2. отдельными Участниками в области, не связанной с оказанием ООО «АТОН» услуг на рынках ценных бумаг.

2. Настоящие Правила содержат условия соглашения, налагающего обязательства и устанавливающего ответственность сторон, вовлеченных в процесс предоставления и использования услуг УЦ, а также иных услуг оказываемых ООО «АТОН» Участникам ЭДО (соглашения об электронном документообороте).

3. После 06 июня 2011 года соглашение об электронном документообороте (далее – «Соглашение об ЭДО») заключается путем присоединения участника к установленным настоящими Правилами условиям в целом в следующем порядке:

[1] Правила электронного документооборота ООО «АТОН», в части регулирующей отношения между Участниками и ООО «АТОН», связанные с обменом электронными документами через уникальный раздел сайта www.aton.ru , доступ к которому получает Участник посредством Уникальной ссылки, применяются с 25.12.2018 г.

3.1. Лицо, желающее заключить с ООО «АТОН» Соглашение об ЭДО подает в ООО «АТОН» собственноручно подписанное заявление о заключении договоров (по форме, установленной Приложением №1 к настоящим Правилам). В случае согласия на заключение Соглашения об ЭДО ООО «АТОН» уведомляет об этом лицо, подавшее заявление. Уведомление может быть совершено путем направления Участнику копии или второго экземпляра поданного Участником заявления с соответствующей отметкой или путем совершения ООО «АТОН» действий по выполнению условий Соглашения об ЭДО; либо

3.2. Лицо, желающее заключить с ООО «АТОН» Соглашение об ЭДО и удовлетворяющее требованиям, предусмотренным в приложении № 1 к Оферте ООО «АТОН» на заключение соглашения об электронном документообороте (далее – «Оферта»), опубликованной в сети Интернет по адресу www.e-disclosure.ru, совершает полное и безоговорочное принятие предложения ООО «АТОН» на заключение Соглашения об ЭДО (Оферты) путем выполнения действий, указанных в Оферте (акцепт).

4. В части, не урегулированной настоящими Правилами, на отношения ООО «АТОН», участников электронного взаимодействия в Информационной системе 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 ООО «АТОН», 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. ООО «АТОН» вправе по своему усмотрению отказаться от заключения Соглашения об ЭДО с лицом, направившим ООО «АТОН» заявление о заключении договоров (по форме, установленной Приложением №1 к настоящим Правилам).

4. Действующая редакция настоящих Правил размещается на странице www.e-disclosure.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 Приложениям к ним, а также решения ООО «АТОН» о сроках и порядке вступления их в силу, доводятся до сведения Участников путем размещения на странице www.e-disclosure.ru в сети «Интернет» не позднее, чем за 3 (Три) рабочих дня до вступления в силу изменений в Правилах и Приложений к ним, и решений ООО «АТОН».

§ 4. Прекращение действия настоящих Правил для всех участников электронного взаимодействия

1. Настоящие Правила прекращают свое действие на основании решения ООО «АТОН».

2. Прекращение действия настоящих Правил и Приложений к ним не влияет на юридическую силу и действительность электронных документов, которыми ООО «АТОН», участники электронного взаимодействия обменивались до прекращения действия настоящих Правил и Приложений к ним.

§ 5. Уведомления

1. Предоставление ООО «АТОН» каких-либо уведомлений (за исключением уведомлений об изменении настоящих Правил, СМС-уведомлений и PUSH-уведомлений), в том числе о приостановлении действия, прекращении действия или аннулировании Сертификатов ключей, может осуществляться путем размещения информации на странице www.aton.ru в сети Интернет, а также на Адрес электронной почты Участника.

2. В случае прекращения действия Правил ООО «АТОН» уведомляет об этом за 30 (Тридцать) дней до даты прекращения действия Правил.

РАЗДЕЛ 1. ПОРЯДОК ОРГАНИЗАЦИИ СИСТЕМЫ ЭДО.

§ 1. Назначение системы ЭДО ООО «АТОН»

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

2. Передача электронных документов осуществляется исключительно в рамках Информационной системы.

3. Доступ Участника к Информационной системе предоставляется следующими способами:

через браузер на странице www.aton.ru**,** Уникальную ссылку, направленную на Адрес электронной почты Участника или web.atonspace.ru в сети Интернет (Личный кабинет) и Мобильные приложения (Aton Line, Aton Space).

4. Достоверность и целостность электронных документов в Информационной системе обеспечивается усиленной неквалифицированной электронной подписью, созданной с использованием средств электронной подписи СКЗИ «Крипто-Ком 3.3» разработки ЗАО «Сигнал-КОМ», факт формирования клиентом электронной подписи при обмене электронными документами в Информационной системе в случаях, установленных настоящими Правилами, подтверждается простой электронной подписью.

§ 2. Особенности организации ЭДО

1. Условиями допуска юридических и физических лиц к осуществлению ЭДО являются:
   - заключение Соглашения об ЭДО: путем акцепта Оферы либо подписания заявления о заключении договоров по форме Приложения № 1, либо соглашения об использовании электронной подписи, либо договора о брокерском обслуживании, в рамках которого предусмотрен обмен с ООО «АТОН» документами в электронном виде, подписанными электронной подписью, в случае обмена электронными документами между отдельными Участниками в области, не связанной с оказанием ООО «АТОН» услуг на рынках ценных бумаг, необходимым условием допуска является также заключение с ООО «АТОН» отдельного соглашения об оказании услуг по обеспечению ЭДО;

1.1. Дополнительными условиями обмена электронными документами, подписанными усиленной неквалифицированной электронной подписью, в системе ЭДО являются:
   - установка необходимого программного обеспечения (далее – «ПО») (подробнее Раздел 2 §1 п.1.5).
   - выполнение УЦ или самим Участником процедуры формирования ключей подписи (подробнее Раздел 2 § 9);
   - изготовление УЦ Сертификата ключа для Участника (подробнее Раздел 2 § 9)

2. В действующей системе ЭДО все услуги по управлению ключами проверки электронной подписи и Сертификатами ключей (регистрация, формирование, обновление, аннулирование) возлагаются на УЦ (подробнее Раздел 2).

3. Для формирования усиленной неквалифицированной электронной подписи каждый Участник должен иметь ключевой носитель с ключом электронной подписи и Сертификатом ключа (подробнее Раздел 2).

§ 3. Использование усиленной неквалифицированной электронной подписи

1. Электронный документ может быть подписан только тем ключом электронной подписи, для которого УЦ изготовлен Сертификат ключа (подробнее Раздел 2 § 1 п.1.4, § 9)

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

3. Риск неправомерного подписания электронного документа усиленной неквалифицированной 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. Замена ключей электронной подписи не влияет на юридическую силу электронного документа, если он был подписан действующим на дату подписания ключом электронной подписи в соответствии с настоящими Правилами (подробнее Раздел 2 § 11, § 12).

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

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

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

9. Проверка усиленной неквалифицированной электронной подписи проводится при проверке подлинности доставленного электронного документа.

10. Участником используются ключи, соответствующие Сертификаты ключей, полученные в установленном настоящими Правилами порядке (подробнее Раздел 2 § 9)

§ 3.1 Использование простой электронной подписи

1. Простой электронной подписью является электронная подпись, которая посредством использования (1) идентификаторов и паролей к ним, предназначенных для аутентификации в Информационной системе, (2) идентификаторов и одноразовых паролей либо (3) иной информации, включающей ключевую информацию, участвующую в аутентификации в Информационной системе, подтверждает факт формирования электронной подписи Участником или его уполномоченным лицом.

2. Электронный документ считается исходящим от Участника, если он содержит реквизиты Участника предназначенные для аутентификации в Информационной системе.

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 об аннулировании или блокировке идентификаторов/иной информации, включающей ключевую информацию, участвующую в аутентификации в Информационной системе.

5. Применение положений Правил, относящихся к электронному документу, подписанному простой электронной подписью с использованием одноразового пароля, распространяется также на каждый электронный документ, входящий в состав пакета электронных документов, подписанного простой электронной подписью с использованием одноразового пароля.

§ 4. 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 Правилам.

3. Электронный документ должен быть сформирован в определенном формате и подписан электронной подписью.

4. Электронные документы, оформленные, переданные и/или полученные в соответствии с настоящими Правилами, признаются равнозначными документам на бумажных носителях, подписанным собственноручной подписью, и не могут быть оспорены только на том основании, что они совершены в электронном виде.

5. Одной простой электронной подписью с использованием одноразового пароля может быть подписан пакет электронных документов, состоящий из нескольких электронных документов, выведенных одновременно в графический пользовательский интерфейс для просмотра и подписания электронных документов.

При подписании простой электронной подписью с использованием одноразового пароля пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным простой электронной подписью.

§ 5. Формирование электронных документов

5.1. ФОРМИРОВАНИЕ ЭЛЕКТРОННОГО ДОКУМЕНТА

Формирование электронного документа осуществляется в следующем порядке:

- формирование электронного сообщения определенного формата;
- подписание сформированного электронного сообщения электронной подписью;
- расчёт свертки подписанного Участником электронного документа.

5.2. ФОРМИРОВАНИЕ ПАКЕТА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Формирование пакета электронных документов осуществляется в следующем порядке:

- формирование нескольких электронных сообщений определенного формата;
- формирование интерфейса просмотра электронных документов в составе пакета;
- подписание сформированного пакета электронных документов простой электронной подписью с использованием одноразового пароля;
- расчёт свертки подписанного Участником пакета электронных документов.

§ 6. Статус электронного документа.

1. Статус электронного документа – информация о текущем состоянии электронного документа в системе ЭДО, показывающая на каком этапе обработки находится электронный документ.

2. Текущее состояние электронного документа отражается в системе ЭДО посредством изменения статуса электронного документа. Для получения актуального статуса Участнику требуется выполнить операцию обновления отображаемой информации в системе ЭДО при помощи штатных средств обновления.

3. Статус электронного документа считается доведенным до сведения Участника не позднее рабочего дня, следующего за днем последнего изменения статуса в системе ЭДО.

4. Учет статусов электронных документов ведется в реестре электронных документов системы ЭДО.

§ 7. Подлинник электронного документа

1. Электронный документ может иметь неограниченное количество экземпляров. Для создания дополнительного экземпляра существующего электронного документа осуществляется воспроизведение 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, заверены собственноручной подписью уполномоченного представителя ООО «АТОН» и 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, подписанный усиленной неквалифицированной электронной подписью, 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 (если применимо), 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

1. 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;
- регистрация в реестре УЦ владельцев Сертификатов ключей;
- формирование пароля и логина для доступа Участников в информационную систему;
- изменение по заявлению Участника пароля и логина для доступа Участника в информационную систему;
- предоставление Участникам программного обеспечения и ключевой информации, необходимых для работы в информационной системе;
- формирование ключевых носителей Участникам, включая генерацию ключа электронной подписи и ключа проверки электронной подписи;
- формирование Запросов сертификатов ключей Участников;
- прием и регистрацию Запросов сертификатов ключей Участников;
- консультация Участников по всем вопросам, связанным с использованием Сертификата ключа;
- проверка уникальности ключей проверки электронной подписи;
- изготовление и выдача на основании Запросов сертификатов электронных Сертификатов ключей;
- изготовление и выдача Сертификатов ключей в форме документов на бумажных носителях;
- аутентификация Участников, запрашивающих аннулирование Сертификатов ключей;
- аннулирование Сертификатов ключей по запросам Участников;
- создание Списка аннулированных сертификатов;
- ведение реестра выпущенных Сертификатов ключей и Списка аннулированных сертификатов;
- публикация реестра выпущенных сертификатов и Списка аннулированных сертификатов в общедоступном сетевом справочнике;
- подтверждение подлинности электронных подписей в документах, представленных в электронной форме, по запросам Участников;
- архивное хранение Сертификатов ключей в электронном виде в течение всего срока действия сертификатов;
- архивное хранение Сертификатов ключей в течение 5 (Пяти) лет после их аннулирования или прекращения действия для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с их применением.

2. Удостоверяющий Центр ООО «АТОН» осуществляет свою деятельность на основании лицензии ФСБ № 0012009 рег. номер №14687Н от 22 октября 2015 года на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

3. Удостоверяющий центр использует **средство криптографической защиты информации (СКЗИ) Крипто-Ком 3.2 и Крипто-Ком 3.3 разработки ЗАО «Сигнал-Ком», имеющее сертификаты ФСБ России ,**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. РЦ – субъект инфраструктуры ключей проверки электронных подписей, которому УЦ делегирует часть своих полномочий по регистрации участников защищенных прикладных систем, их первичной идентификации и аутентификации. РЦ регистрирует запросы на выпуск и аннулирование Сертификатов ключей, обеспечивает их доставку в УЦ и отвечает за передачу сформированных Сертификатов ключей и их бумажных копий Участникам.

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 Участников;

- предоставление Участникам программного обеспечения и ключевой информации, необходимых для работы в информационной системе;
- формирование Запросов сертификатов;
- прием Запросов сертификатов от Участников;
- предоставление Участникам изготовленных Сертификатов ключей в электронной форме и их бумажных копий;
- аутентификация Участников, запрашивающих аннулирование Сертификатов ключей;
- прием запросов на аннулирование Сертификатов ключей от Участников и передача их в УЦ.

1.3. УЧАСТНИКИ

Участники электронного взаимодействия в информационной системе - физические лица и юридические лица, осуществляющие ЭДО.

1.4. СЕРТИФИКАТЫ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

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

2. Сертификаты ключей имеют два подкласса: сертификаты для физических лиц, выдаваемые по предъявлению паспорта, и сертификаты для юридических лиц, выдаваемые физическим лицам, действующим от имени такого юридического лица, на основании паспорта и документов, подтверждающих полномочия этих лиц.

3. Алгоритм ключа проверки электронной подписи в Сертификатах ключа – ГОСТ Р 34.10-2001.

4. Срок действия Сертификата ключа устанавливается УЦ при выдаче Сертификата ключа. Данный срок не может превышать 455 (Четыреста пятьдесят пять) дней.

5. Копия Сертификата ключа на бумажном носителе является заявлением на выдачу Сертификата ключа. Форма заявления установлена Приложением № 3

6. УЦ предоставляет владельцам Сертификатов ключей следующие услуги:

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

1.5. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. УЦ предоставляет Участнику ПО производства ЗАО «Сигнал-Ком», созданное на «СКЗИ «Крипто-КОМ 3.2» и «СКЗИ «Крипто-КОМ 3.3».

2. ПО может быть предоставлено Участнику на носителе, установленного УЦ типа, либо (при наличии возможности) самостоятельно скопировано Участником в сети Интернет на странице www.aton.ru.

3. Участники не вправе распространять, копировать или модифицировать ПО без согласия УЦ.

4. УЦ вправе принять решение о замене предоставленного ПО полностью или в какой-либо части. В этом случае УЦ обязан предоставить Участникам подлежащее замене ПО, Участники, со своей стороны, обязаны осуществить все действия, необходимые для замены ПО.

§ 2. Права УЦ и Участников

2.1. ПРАВА УЦ

УЦ имеет право:

- Требовать подтверждения достоверности информации, содержащейся в Сертификатах ключей, в отношении Участников и уполномоченных представителей Участников.
- Отказать в формировании ключей Участнику в случае ненадлежащего оформления заявления на формирование ключей.
- Отказать в изготовлении Сертификата ключа в случае ненадлежащего оформления заявления на изготовление сертификата ключа.
- Отказать в изготовлении Сертификата ключа при отсутствии соответствующих полномочий у лица, представившего заявление на изготовление сертификата ключа.
- Отказать в аннулировании Сертификата ключа Участнику в случае, если истек установленный срок действия этого Сертификата ключа.

- Аннулировать Сертификат ключа в случае установленного факта компрометации соответствующего ему ключа электронной подписи, с уведомлением владельца аннулированного Сертификата ключа и указанием обоснованных причин аннулирования.
- Заменить предоставленное Участнику программное обеспечение полностью или в какой-либо части.

2.2. ПРАВА УЧАСТНИКОВ

Участник имеет право:

- Получить Сертификат ключа уполномоченного лица УЦ.
- Получить ключи электронной подписи и Сертификат ключа с возможной их записью на ключевой носитель.
- Обратиться в УЦ для аннулирования Сертификата ключа, если период действия этого Сертификата ключа 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 ключ электронной подписи и ключ проверки электронной подписи на своем рабочем месте с использованием средства электронной подписи и программных средств со встроенной библиотекой СКЗИ «Крипто-КОМ 3.2» или «СКЗИ «Крипто-КОМ 3.3», предоставляемых УЦ.

§ 3. Обязанности УЦ и Участников

3.1. ОБЯЗАННОСТИ УЦ

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

- использовать ключ электронной подписи уполномоченного лица УЦ только для заверения издаваемых им Сертификатов ключей и Списков аннулированных сертификатов;
- обеспечивать надежную защиту ключа электронной подписи уполномоченного лица УЦ от несанкционированного доступа;
- обеспечивать конфиденциальность в отношении изготовляемых ключей электронной подписи Участников;
- соблюдать конфиденциальность в отношении регистрационной информации об Участнике;
- обеспечивать уникальность серийных номеров изготавливаемых Сертификатов ключей;
- извещать Участника о причинах отказа в изготовлении Сертификата ключа;
- принимать и обрабатывать заявления от владельцев Сертификатов ключа на аннулирование сертификатов:
  - − принимать и обрабатывать заявления на аннулирование Сертификата ключа;
  - − аутентифицировать Участников, запрашивающих аннулирование Сертификата ключа;
  - − аннулировать Сертификаты ключа по заявлениям Участников;
  - − информировать Участников об аннулировании Сертификатов ключа путем периодического выпуска Списка анулированных сертификатов не реже 1 (одного) раза в 30 (тридцать) дней;
- публиковать реестр выпущенных Сертификатов ключей и Списка аннулированных сертификатов в сетевом справочнике;
- уведомлять Участника о фактах, которые стали известны УЦ и которые существенным образом могут сказаться на возможности дальнейшего использования его Сертификата ключа;
- уведомлять о факте аннулирования Сертификата ключа Участника или его уполномоченного представителя.
- синхронизировать по времени все программные и технические средства обеспечения деятельности в соответствии с их предназначением.

3.2. ОБЯЗАННОСТИ РЦ

РЦ должны строго соблюдать порядок, изложенный в настоящих Правилах, в частности:

- осуществлять регистрацию Участников;
- осуществлять регистрацию поступающих Запросов сертификатов и передавать их по Доверенному каналу в УЦ;
- передавать полученные из УЦ сформированные Сертификаты ключей Участникам.

3.3. ОБЯЗАННОСТИ УЧАСТНИКОВ

Участникидолжны строго соблюдать правила, изложенные в настоящих Правилах, в частности:

- обеспечивать сохранность ключа электронной подписи 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 аннулирования);
- не использовать ключ электронной подписи и соответствующий ему Сертификат ключа по истечении срока их действия;
- своевременно (до истечения периода действия Сертификата ключа) осуществлять смену ключа электронной подписи 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 максимально точные и действительные сведения;
- подтверждать по требованию УЦ достоверность информации, содержащейся в Сертификате ключа, выдаваемом Участнику;
- своевременно информировать УЦ или уполномоченного представителя УЦ о факте компрометации собственного ключа электронной подписи или ключевого носителя;
- не использовать для формирования электронной подписи скомпрометированные ключи электронной подписи;
- в случае компрометации ключей своевременно прислать в УЦ заявление на аннулирование сертификата ключа;
- своевременно информировать УЦ или уполномоченного представителя УЦ о фактах изменения персональных данных, содержащихся в Сертификатах ключа;
- перед первым использованием на рабочем месте и в дальнейшем не реже 1 (одного) раза в месяц проводить контроль целостности состава прикладного программного обеспечения, используя для этого утилиту rush, входящую в состав СКЗИ «Крипто-КОМ 3.3» .

§ 4. Ответственность УЦ и Участников

4.1. ОТВЕТСТВЕННОСТЬ УЦ И РЦ

УЦ и РЦ несут ответственность в соответствии с законодательством РФ.

УЦ не несет ответственности за любые прямые или косвенные убытки, любую потерю прибыли, явившиеся результатом несоблюдения Участниками конфиденциальности собственных ключей электронной подписи, а также нарушение достоверности и целостности Сертификатов ключей УЦ.

4.2. ОТВЕТСТВЕННОСТЬ УЧАСТНИКОВ

Участники несут ответственность за:

• несохранение конфиденциальности собственных ключей электронной подписи,
• несохранение ключевых носителей;
• несохранение достоверности и целостности Сертификатов ключей уполномоченного лица УЦ;
• несвоевременное уведомление УЦ о компрометации собственного ключа электронной подписи.

§ 5. Идентификация и аутентификация Участников

5.1. ПЕРВОНАЧАЛЬНАЯ ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ УЧАСТНИКА

1. В процессе регистрации Участника осуществляется его первоначальная идентификация, по результатам которой Участнику присваивается уникальное имя и заносится данное имя в реестр зарегистрированных Участников. Идентификация опирается на наличие у каждого владельца Сертификата ключа уникального имени, отличного от имен всех остальных Участников.

2. Первоначальная аутентификация Участника, являющегося физическим лицом, производится с использованием документа, удостоверяющего личность.

3. Первоначальная аутентификация Участника, являющегося юридическим лицом, производится с использованием документа, удостоверяющего личность уполномоченного представителя юридического лица, доверенности или учредительных документов юридического лица, на основании которых действует уполномоченный представитель.

5.2. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ЗАРЕГИСТРИРОВАННОГО УЧАСТНИКА

1. Идентификация зарегистрированного Участника, являющегося физическим лицом, осуществляется по уникальному имени, занесенному в реестр УЦ при его первичной регистрации, и паспортным данным Участника.

Идентификация зарегистрированного Участника, являющегося юридическим лицом, осуществляется по уникальному имени, занесенному в реестр УЦ при его первичной регистрации, паспортным данным уполномоченного предствителя юридического лица, доверенности или учредительных документов юридического лица, на основании которых действует уполномоченный представитель

2. Аутентификация зарегистрированного Участника при его обращении в УЦ с заявлением на выдачу Сертификата ключа, замену и аннулирование Сертификата ключа выполняется путем проверки подлинности подписи Участника или уполномоченного предствителя Участника (если Участник является юридическим лицом) в заявлении.

3. Аутентификация при удаленном обращении зарегистрированного Участника с заявлением на выдачу сертификата ключа проверки электронной подписи, поданного в электронной форме с электронной подписью Участника осуществляется путем выполнения процедуры проверки в электронном документе электронной подписи Участника.

§ 6. Способы удаленного взаимодействия Участника с УЦ

6.1. Взаимодействие Участников с УЦ через доверенных посредников:

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

6.2. Взаимодействие Участника с УЦ через Web-интерфейс:

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

6.3. Взаимодействие Участника с УЦ через РЦ:

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

§ 7. Первичная регистрация Участников в УЦ

1. Регистрация Участников – это внесение регистрационной информации об Участниках в реестр УЦ.
2. Процедура регистрации включает следующие этапы:
   - изготовление ключевых носителей Участника;
   - формирование Запроса сертификата;
   - передача в УЦ (РЦ) Запроса сертификата и заявления на выдачу сертификата ключа проверки электронной подписи;
   - регистрация Запроса сертификата в УЦ;
   - изготовление Сертификата ключа;
   - передача Сертификата ключа Участнику.

§ 8. Формирование пароля для входа Участника в информационную систему

1. Для доступа в информационную систему УЦ на основании заявления Участника на получение идентификатора (логина) и пароля (по форме Приложения № 5) предоставляет Участнику логин и пароль. УЦ формирует с помощью специализированного ПО карту клиента, которая содержит логин и пароль для входа в информационную систему, (далее – «Карта клиента») и передает ее Участнику в запечатанном конверте.

2. Конверт с Картой клиента передается Участнику несколькими способами:
   1) При личном визите Участника в ООО «АТОН».
   2) При личном визите в ООО «АТОН» курьера, уполномоченного Участником доставлять, принимать, расписываться в получении документов.
   3) По почте России срочным письмом.
   4) Через посредников

Участник обязан хранить полученные логин и пароль в тайне.

Участник 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 № 5А).

§ 9. Формирование ключей и Сертификатов ключа для новых Участников

9.1. ФОРМИРОВАНИЕ КЛЮЧЕЙ И СЕРТИФИКАТА КЛЮЧА ДЛЯ НОВЫХ УЧАСТНИКОВ ПРИ САМОСТОЯТЕЛЬНОМ ФОРМИРОВАНИИ КЛЮЧЕЙ УЧАСТНИКОМ

1. Формирование ключей подписи выполняется Участником самостоятельно с помощью ПО, разработанного на базе сертифицированного СКЗИ «Крипто-КОМ 3.2» или «СКЗИ «Крипто-КОМ 3.3» и скопированным им в личном кабинете на странице www.aton.ru в сети «Интернет».

Запрос сертификата, сформированный Участником, в электронной форме передается в базу данных УЦ по Доверенному каналу или по электронной почте.

2. Подписанное заявление на выдачу сертификата ключа проверки электронной подписи (по форме Приложения №3) Участнику необходимо предоставить в УЦ:

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

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

4. В случае отказа в изготовлении Сертификата ключа Участник уведомляется об этом с указанием причины отказа.

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

9.2. ФОРМИРОВАНИЕ КЛЮЧЕЙ И СЕРТИФИКАТА КЛЮЧА ДЛЯ НОВЫХ УЧАСТНИКОВ ПРИ ОЧНОМ ОБРАЩЕНИИ УЧАСТНИКОВ

1. В УЦ формируются комплекты ускоренной активации для передачи сотрудникам ООО «АТОН», а также доверенным лицам, оказывающим ООО «АТОН» услуги, направленные на обслуживание клиентов ООО «АТОН» (далее – «партнеры»). Каждый комплект включает:

- 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 для вычисления контрольной суммы дистрибутивных файлов (контроля целостности);
- Сертификат ключа УЦ;
- Карту клиента с логином и паролем для входа в информационную систему
- Инструкцию по активации.

2. Сотрудник ООО «АТОН» или партнера передает Участнику комплект ускоренной активации. и бланки заявлений о заключении договоров, на формирование ключей электронной подписи, на выдачу сертификата ключа проверки электронной подписи в двух экземлярах .
3. При получении заявления Участника на выдачу Сертификата ключа УЦ проверяет соответствие идентификационных данных Участника. В случае идентичности указанной информации УЦ изготавливает Сертификат ключа на основании Запроса сертификата.
4. В случае отказа в изготовлении Сертификата ключа Участник уведомляется об этом с указанием причины отказа.
5. Изготовленный Сертификат ключа в виде электронного документа передается Участнику на рабочее место автоматически или по электронной почте.

§ 10. Плановая смена ключей подписи Участника

1. Плановая смена ключей Участников производится в связи с истечением срока действия Сертификата ключа Участника.

2. Сертификат ключа прекращает свое действие в связи с истечением установленного срока его действия, использование соответствующих ключей подписи прекращается.

3. ПО Участника заблаговременно предупреждает его о предстоящей плановой смене ключей. Не ранее, чем за 40 (Сорок) рабочих дней до истечения срока действия текущего Сертификата ключа Участник должен выполнить процедуру плановой смены ключей: сформировать новые ключи и получить Сертификат ключа.

4. Если Участник не успеет получить новый Сертификат ключа до истечения периода действия Сертификата ключа, документы, подписанные ключом, парным Сертификату ключа с истекшим периодом действия, будут блокироваться при проверке электронной подписи.

5. В случае если Участник не успел обновить Сертификат ключа до истечения периода его действия, обновление Сертификата ключа выполняется в порядке, установленном для новых Участников (согласно п.9.1, 9.2. настоящих Правил).

10.1. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ И ОБНОВЛЕНИЕ СЕРТИФИКАТА КЛЮЧА УЧАСТНИКА ПРИ САМОСТОЯТЕЛЬНОМ ФОРМИРОВАНИИ КЛЮЧЕЙ УЧАСТНИКОМ

1. При наличии возможности Участник самостоятельно с помощью ПО, разработанного на базе сертифицированного СКЗИ «Крипто-КОМ 3.2» или «СКЗИ «Крипто-КОМ 3.3» и скопированным им в личном кабинете на странице www.aton.ru в сети «Интернет», выполняет генерацию ключей электронной подписи и формирует Запрос сертификата.
2. Запрос сертификата, сформированный Участником, в электронной форме импортируется в базу данных УЦ при наличии Доверенного канала с УЦ автоматически или по электронной почте.
3. Участник распечатывает и подписывает заявление на выдачу сертификата ключа проверки электронной подписи (по форме Приложения №3) и доставляет его в УЦ:
   - при личном визите в ООО «АТОН»
   - курьером, уполномоченным Участником доставлять, принимать, расписываться в получении документов;
   - по почте России заказным письмом или письмом с объявленной ценностью.
4. При получении заявления на выдачу сертификата ключа проверки электронной подписи УЦ проверяет соответствие идентификационных данных Участника (подробнее Раздел 2, §5, п.5.2.). В случае идентичности указанной информации УЦ изготавливает Сертификат ключа на основании Запроса сертификата.
5. В случае отказа в изготовлении Сертификата ключа Участник уведомляется об этом с указанием причины отказа.
6. Изготовленный Сертификат ключа в виде электронного документа передается Участнику на рабочее место автоматически или по электронной почте.
7. УЦ заполняет заявление на выдачу сертификата ключа проверки электронной подписи на бумажном носителе (по форме Приложения № 3), указывая следующие сведения:
   - регистрационный номер Сертификата ключа,
   - дату начала действия Сертификата ключа,
   - дату окончания действия Сертификата ключа,
   - уполномоченное лицо УЦ,
   - основание полномочий.
8. Уполномоченный представитель УЦ подписывает заполненное заявление на выдачу сертификата ключа проверки электронной подписи, заверяет печатью УЦ.
9. Полученный личный Сертификат ключа Участник помещает на свой ключевой носитель. Сертификат ключа уполномоченного лицам УЦ рекомендуется хранить на ключевом носителе вместе с ключами электронной подписи Участника.

10.2. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ И ОБНОВЛЕНИЕ СЕРТИФИКАТА КЛЮЧА УЧАСТНИКА ПРИ САМОСТОЯТЕЛЬНОМ ФОРМИРОВАНИИ КЛЮЧЕЙ УЧАСТНИКОМ С ИСПОЛЬЗОВАНИЕМ ДЕЙСТВУЮЩЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ.

1. При наличии возможности Участник самостоятельно с помощью ПО, разработанного на базе сертифицированного СКЗИ «Крипто-КОМ 3.2» или «СКЗИ «Крипто-КОМ 3.3» и скопированным им в личном кабинете на странице www.aton.ru в сети «Интернет», выполняет генерацию ключей электронной подписи и формирует Запрос сертификата, который подписывает действующей усиленной неквалифицированной электронной подписью.
2. Сформированный Запрос сертификата в электронной форме автоматически импортируется в базу данных УЦ при наличии Доверенного канала с УЦ.
3. В УЦ выполняется автоматическая проверка электронной подписи, содержащейся в поступившем Запросе сертификата.
4. При отсутствии ошибок в Запросе сертификата, поступившем от Участника, УЦ изготаливает Сертификат ключа.
5. Изготовленный сертификат ключа в виде электронного документа передается Участнику на рабочее место автоматически или по электронной почте.

10.3. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ И ОБНОВЛЕНИЕ СЕРТИФИКАТА КЛЮЧА УЧАСТНИКА ПРИ ОЧНОМ ОБРАЩЕНИИ

1.Изготовление ключей и обновление Сертификата ключа при очном обращении Участника осуществляется УЦ с помощью комплекта быстрой активации

Каждый комплект быстрой активации включает:

- 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 для вычисления контрольной суммы дистрибутивных файлов (контроля целостности);
• Сертификат ключа УЦ;
• Инструкцию по активации.

2.Обновление Сертификата ключа в этом случае выполняется в порядке, установленном для формирования ключей и Сертификата ключа для новых Участников при очном обращении Участника (см.п.9.2 Правил).

§ 11. Внеплановая смена ключей Участников

1. Внеплановой считается замена Сертификатов ключей по инициативе Участника, не связанная с истечением установленного срока действия Сертификата ключа Участника.

Внеплановая смена ключей и обновление Сертификата ключа осуществляются Участником в следующих случаях:

- при компрометации ключа электронной подписи Участника;
- при компрометации ключа электронной подписи уполномоченного лица УЦ;
- при компрометации ключевых носителей;
- в случае иных форс-мажорных обстоятельств.

2. При внеплановой смене ключей Участнику необходимо:

При самостоятельном формировании ключей участником

- при наличии действующей электронной подписи самостоятельно сформировать ключи электронной подписи и Запрос сертификата, подписать Запрос сертификата и заявление на внеплановую замену сертификата ключа проверки электронной подписи действующей электронной подписью. Сформированный Запрос сертификата в электронной форме автоматически импортируется в базу данных УЦ; либо
- самостоятельно сформировать ключи и Запрос сертификата, распечатать, подписать заявление на внеплановую замену ключа электронной подписи и сертификата ключа проверки электронной подписи (Приложение №4) с указанием причины замены и заявление на выдачу сертификата ключа проверки электронной подписи (Приложение №3) и направить их в УЦ.

При очном обращении:

- подписать заявление на внеплановую замену ключа электронной подписи и сертификата ключа проверки электронной подписи с указанием причины замены (Приложение №4), получить комплект быстрой активации, заполнить бланки заявлений на выдачу сертификата ключа проверки электронной подписи (Приложение №3) и заявления на формирование ключей электронной подписи (Приложение №2) и передать заполненные бланки заявлений Сотруднику ООО «АТОН».

§ 12. Аннулирование Сертификата ключа Участника

1. Аннулирование Сертификата ключа Участника осуществляется:
   - по заявлению Участника;
   - по заявлению на отзыв доверенности уполномоченного представителя Участника (для юридических лиц), зарегистрированного в УЦ;
   - по решению УЦ.
2. Заявление на аннулирование Сертификата ключа в бумажной форме подается Участником в УЦ лично, заказным письмом или курьерской связью.
3. Сертификат ключа Участника может быть аннулирован по инициативе УЦ в случае:
   - установленного факта компрометации ключа электронной подписи Участника;
   - по указанию лиц или органов, имеющих такое право в силу закона.
4. УЦ вносит информацию об аннулировании Сертификата ключа в Список аннулированных сертификатов в течение одного рабочего дня со дня наступления обстоятельств, повлекших за собой прекращение действия Сертификата ключа. Действие Сертификата ключа прекращается с момента внесения записи об этом в Список аннулированнных сертификатов.

§ 13. Уведомление о факте аннулирования Сертификата ключа

1. В случаях аннулирования Сертификата ключа УЦ выпускает соответствующие уведомления.

Официальным уведомлением владельца Сертификата ключа о факте аннулирования Сертификата ключа является публикация УЦ Списка аннулированных сертификатов, содержащего сведения об аннулированном Сертификате ключа.

2. Временем публикации считается время издания Списка аннулированных сертификатов.

§ 14. Дополнительные положения

14.1. ТРЕБОВАНИЯ К СРЕДСТВАМ ЭЛЕКТРОННОЙ ПОДПИСИ УЧАСТНИКОВ

Средство электронной подписи должно обеспечивать выполнение следующих процедур:

- генерацию ключей электронной подписи и ключей проверки электронной подписи;
- формирование электронной подписи;
- проверку электронной подписи.

Средства электронной подписи должны обеспечивать выполнение мер защиты ключей электронной подписи (см. Раздел 5 § 2).

14.2. СМЕНА КЛЮЧЕЙ УПОЛНОМОЧЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Формирование ключей электронной подписи, ключей проверки электронной подписи и Сертификата ключа УЦ выполняется УЦ с помощью программного обеспечения, разработанного на базе сертифицированного СКЗИ «Крипто-КОМ 3.3» .

Рекомендуемый срок действия Сертификата ключа УЦ составляет 5 (Пять) лет.

Плановая смена ключей уполномоченного лица УЦ выполняется не позднее, чем за 1 (Один) год до окончания периода действия его ключа электронной подписи. Процедура плановой смены ключей уполномоченного лица УЦ (ключей УЦ) осуществляется в следующем порядке:

- УЦ формирует новый ключ электронной подписи и соответствующий ему новый ключ проверки электронной подписи и Сертификат ключа УЦ;
- сформированный новый Сертификат ключа УЦ должен довести до всех Участников по Доверенному каналу;
- до окончания срока действия текущего ключа электронной подписи УЦ Участники должны получить новый Сертификат ключа УЦ и добавить его в справочники сертификатов, не удаляя действующий Сертификат ключа УЦ;
- старый ключ электронной подписи УЦ используется в течение своего срока действия для формирования Списков аннулированных сертификатов, изданных УЦ в период действия старого ключа электронной подписи уполномоченного лица УЦ.

РАЗДЕЛ 3. ПОРЯДОК ИСПОЛЬЗОВАНИЯ ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

§ 1. Аутентификация Участников

1. В Информационной системе при использовании простой электронной подписи возможны следующие способы аутентификации:
   - по идентификатору и паролю;
   - по идентификатору и публичному ключу, зарегистрированному в информационной системе;
   - по идентификатору и одноразовому паролю;
   - по одноразовому паролю и переходу Участника по Уникальной ссылке.
   - по зарегистрированному Номеру мобильного телефона Участника в информационной системе и одноразовому паролю.
2. Для усиления безопасности возможно использование одновременно двух способов аутентификации. Для каждой Информационной системы способы аутентификации определяются ООО «АТОН» с учетом технических возможностей соответствующей Информационной системы.
3. Участник при наличии технической возможности может самостоятельно менять способ аутентификации в Информационной системе. При выборе нового способа аутентификации ООО «АТОН» вправе отключить используемый ранее Участником способ аутентификации в Информационной системе.

§ 2. Формирование пароля и выдача идентификаторов

1. ООО «АТОН» является оператором выдачи идентификаторов аутентификации и паролей к ним, а так же обеспечивает функционирование систем одноразовых паролей и систем аутентификации Информационной системы, осуществляет создание (замену) идентификаторов и паролей к ним, а так же

выполняет все необходимые операции, связанные с обеспечением инициализации и безопасности систем одноразовых паролей и систем аутентификации Информационной системы.

2. ООО «АТОН» вправе наделить полномочиями по выдаче идентификаторов аутентификации и паролей к ним любое юридическое или физическое лицо, при этом их ответственность определяется отдельными соглашениями с ООО «АТОН».

3. Участник или его уполномоченное лицо могут получить идентификаторы аутентификации и пароли к ним в любом офисе ООО «АТОН» или уполномоченного им юридического или физического лица на основании заявления составленного по форме Приложения № 5.

3.1. Участник или его уполномоченное лицо могут зарегистрировать идентификаторы (логин) для iQUIK X на основании заявления, составленного по форме Приложения № 12, и самостоятельно установить пароль к идентификаторам аутентификации по адресу www.aton.ru в сети Интернет.

3.2. По заявлению Участника, в том числе в устной форме, ООО «АТОН» вправе направить на Адрес электронной почты Участника Уникальную ссылку, посредством которой Участник получает доступ на уникальный раздел сайта www.aton.ru, используемый для подписания и обмена в электронной форме документами и информацией между ООО «АТОН» и Участником в соответствии с настоящими Правилами.

4. При наличии технической возможности Участник вправе самостоятельно создать идентификаторы аутентификации и информацию, предназначенную для аутентификации в Информационной системе. Для этого Участнику необходимо подать ООО «АТОН» подписанное простой электронной подписью заявление в электронной форме, расположенное по адресу www.aton.ru.

5. При получении идентификаторов аутентификации и паролей к ним путем подачи заявления в электронной форме ООО «АТОН» обеспечивает Участнику возможность осуществления самостоятельной регистрации идентификаторов в Информационной системе.

6. Участник при наличии технической возможности вправе самостоятельно производить установку, замену паролей к идентификаторам аутентификации, а так же производить любые операции смены информации, предназначенной для его аутентификации согласно инструкций к Информационной системе, Мобильным приложениям.

7. Создаваемый пароль должен соответствовать следующим требованиям:

а) содержать не менее 8 символов;

б) содержать буквенные и (или) цифровые символы.

8. При использовании в Информационной системе в целях аутентификации самостоятельно формируемой Участником ключевой информации (закрытого и публичного ключа) Участник в целях регистрации публичного ключа в Информационной системе направляет ООО «АТОН» в электронной форме подписанное простой электронной подписью заявление по образцу, утвержденному Приложением № 7 к настоящим Правилам.

При получении ООО «АТОН» заявления на регистрацию публичного ключа с указанием ранее зарегистрированного в Информационной системе идентификатора (логина) Участника, публичный ключ, ранее зарегистрированный в Информационной системе с указанием такого идентификатора (логина) Участника, аннулируется.

9. Замена ключей электронной подписи не влияет на юридическую силу электронного документа, если он был подписан действующим на дату подписания ключом электронной подписи в соответствии с настоящими Правилами.

§ 3. Обязанности участника по соблюдению конфиденциальности

1. Участник обязан:
   - хранить в тайне пароли, в том числе одноразовые пароли, полученные посредством СМС-уведомлений на номер мобильного телефона Участника/Адрес электронной почты Участника, PUSH-уведомлений на Мобильное устройство Участника, идентификаторы и информацию, предназначенную для аутентификации в Информационной системе, принимать все возможные меры, предотвращающие нарушение их конфиденциальности;
   - не передавать третьим лицам SIM-карту с Номером мобильного телефона Участника во избежание нарушения конфиденциальности;
   - не передавать третьим лицам Мобильное устройство с установленным на нем Мобильным приложением без завершения активной сессии;
   - осуществлять действия направленные на формирование простой электронной подписи с использованием идентификаторов и паролей аутентификации и информации для аутентификации, полученной в порядке, установленном настоящими Правилами;
   - в случае нарушения конфиденциальности паролей и идентификаторов аутентификации или информации предназначенной для аутентификации в Информационной системе или их утери незамедлительно уведомить об этом ООО «АТОН».
2. Участник несет ответственность:
   - за предоставление некорректного (не существующего или не принадлежащего Участнику) Номера мобильного телефона Участника;
   - за предоставление некорректного (не существующего или не принадлежащего Участнику) Адреса электронной почты Участника;

- за несвоевременное информирование ООО «АТОН», в том числе за возможные последующие негативные события, произошедшие в результате компрометации ключевой информации и/или паролей для доступа в информационную систему;
- за негативные последствия, наступившие в результате несоблюдения обязанностей, установленных пунктом 3.1 § 3 Раздела 4 настоящих Правил.

§ 4. Порядок и правила направления Участнику одноразового пароля

4.1. НАПРАВЛЕНИЕ ОДНОРАЗОВЫХ ПАРОЛЕЙ ПОСРЕДСТВОМ СМС-УВЕДОМЛЕНИЙ/ЭЛЕКТРОННОЙ ПОЧТЫ

1. Одноразовые пароли посредством СМС-уведомления направляются только Участнику, выразившему свое согласие на получение СМС-уведомлений. Факт согласия на получение СМС-уведомлений подтверждается: заявлением Участника (приложения №№ 1, 8), в котором наряду с данными об Участнике и его согласием на получение подобным способом одноразовых паролей указывается номер мобильного телефона, на который оно отправляется, либо запросом на получение одноразового пароля на указанный для направления одноразовых паролей номер мобильного телефона при совершении физическим лицом действий, необходимых для принятия оферты ООО «АТОН» на заключение Соглашения об ЭДО (акцепта).

1.1. Одноразовые пароли для аутентификации в ТС QUIK посредством электронной почты направляются Участнику, выразившему свое согласие на получение одноразовых паролей посредством электронной почты, в случае получения ООО «АТОН» от Участника или иных третьих лиц информации о невозможности направления Участнику/получения Участником СМС-уведомлений вследствие технических сбоев, в том числе сбоев в работе линий связи, обрыва линий связи, выхода из строя оборудования у телефонного оператора. Факт согласия на получение одноразовых паролей посредством электронной почты подтверждается заявлением Участника (приложение № 9), в котором наряду с данными об Участнике и его согласием на получение подобным способом одноразовых паролей указывается Адрес электронной почты Участника (e-mail).

2. Если иное не указано в настоящих Правилах Участник представляет ООО «АТОН» заявление о согласии на получение одноразовых паролей посредством СМС-уведомлений в письменной форме, заявление о согласии на получение одноразовых паролей посредством электронной почты в электронной форме, подписанное простой электронной подписью.

2.1. В сети Интернет согласие на получение одноразовых паролей посредством СМС-уведомлений может подтверждаться направлением запроса на получение одноразового пароля на указанный для направления одноразовых паролей номер мобильного телефона путем нажатия кнопки «Выслать» в поле «Одноразовый пароль» при совершении действий, необходимых для принятия оферты ООО «АТОН» на заключение Соглашения об ЭДО (акцепта);

2.2. В Мобильном приложении Aton Space согласие на получение одноразовых паролей посредством СМС-уведомлений может подтверждаться направлением запроса на получение одноразового пароля путем нажатия кнопки «Подписать» при совершении действий, необходимых для принятия оферты ООО «АТОН» на заключение Соглашения об ЭДО (акцепта).

3. ООО «АТОН» в обязательном порядке обеспечивает фиксацию фактов отправки и доставки адресату одноразовых паролей посредством СМС-уведомления и сообщений на Адрес элетронный почты Участника. Факт отправки и доставки СМС-уведомления подтверждается детализацией СМС-уведомления (информация о дате и времени отправки СМС-уведомления, текст отправленного СМС-уведомления, дата и время доставки СМС-уведомления Участнику), которая учитывается в технической информационной системе ООО АТОН и может быть предоставлена в случае возникновения спорной ситуации. Факт отправки и доставки сообщений на Адрес электронной почты Участника, подтверждается информацией о дате и времени отправки сообщения, текстом отправленного сообщения. Информация учитывается в технической информационной системе ООО АТОН и может быть предоставлена в случае возникновения спорной ситуации.

4 Подписание (пакета) электронных документов с использованием полученного посредством СМС-уведомления одноразового пароля осуществляется в Личном кабинете (на страницах www.aton.ru, web.atonspace.ru в сети Интернет), в Мобильном приложении Aton Line, Мобильном приложении Aton Space, в уникальном разделе сайта www.aton.ru, в который Участник переходит по Уникальной ссылке, направленной ООО «АТОН» на Адрес электронной почты Участника в порядке, предусмотренном настоящими Правилами.

5. ООО «АТОН» вправе отказать в регистрации Номера мобильного телефона/ Адреса электронной почты Участника в следующих случаях:

- если при проверке реквизитов Участника обнаружено указание Участником несуществующих/некорректных данных (номера телефона, договора, адреса электронной почты) и иных подобных реквизитов;
- если при проверке реквизитов Участника обнаружено, что указанный номер мобильного телефона/ адрес электронной почты уже зарегистрирован в Информационной системе за другим Участником;
- в случае, если указанный номер мобильного телефона зарегистрирован в системах ООО «АТОН» за другим физическим лицом либо у ООО "АТОН" есть иные основания полагать, что другое лицо использует указанный номер телефона;

- в случае ненадлежащего оформления Участником заявления, составленного по форме Приложений №№ 1, 8/Приложения №9;
- в случае нарушения Участником настоящих Правил.

Об отказе принятия документов от Участника, ООО «АТОН» информирует Участника.

5.1. ООО «АТОН» вправе приостановить оказание Участнику предусмотренных настоящими Правилами услуг по направлению одноразовых паролей посредством СМС-уведомлений/ электронной почты в следующих случаях:

- если у ООО "АТОН" появятся основания полагать, что другое лицо использует Номер мобильного телефона/ Адрес электронной почты Участника, включая, но не ограничиваясь наступлением следующих событий:
  - ❖ указанием третьим лицом Номера мобильного телефона/ Адреса электронной почты Участника в качестве контактных данных этого лица в предоставленных им в ООО «АТОН» документах;
  - ❖ отсутствием возможности связаться с Участником по Номеру мобильного телефона/ Адресу электронной почты Участника;
  - ❖ получением ООО «АТОН» звонков/писем с Номера мобильного телефона/ Адреса электронной почты Участника от третьих лиц;
- в случае нарушения Участником настоящих Правил.

Оказание услуг возобновляется после предоставления Участником ООО «АТОН» достоверного подтверждения принадлежности Участнику Номера мобильного телефона/Адреса электронной почты Участника либо заявления, составленного по форме Приложений №№ 8, 9, с указанием принадлежащего Участнику иного Номера мобильного телефона/ Адреса электронной почты Участника, устранения допущенного Участником нарушения настоящих Правил, соответственно.

6. ООО «АТОН» не несет ответственность за корректность (существование и принадлежность Участнику) Номера мобильного телефона/Адреса электронной почты Участника.

7. ООО «АТОН» не несет ответственность за нарушение обязательств вследствие сбоев в работе линий связи, обрыва линий связи, выхода из строя оборудования у телефонного оператора.

4.2. НАПРАВЛЕНИЕ ОДНОРАЗОВЫХ ПАРОЛЕЙ ПОСРЕДСТВОМ PUSH-УВЕДОМЛЕНИЙ

1. Одноразовые пароли посредством PUSH–уведомлений направляются только Участнику, выразившему свое согласие на получение PUSH–уведомлений. Факт согласия на получение PUSH–уведомлений подтверждается заявлением Участника (Приложение №11).

2. Участник предоставляет ООО «АТОН» заявление о согласии на получение одноразовых паролей посредством PUSH – уведомлений, подписанное простой электронной подписью в Мобильном приложении Aton Line или в письменной форме на бумажном носителе.

3. PUSH–уведомление направляется Участнику в виде всплывающего сообщения на экране Мобильного устройства с установленным Мобильным приложением Aton Line, Идентификатор которого зарегистрирован при первичной аутентификации при входе в Мобильное приложение Aton Line.

4. В целях получения Одноразовых паролей посредством PUSH–уведомлений на Мобильное устройство Участник в Мобильном приложении Aton Line, установленном на таком устройстве, должен активировать функцию получения Одноразовых паролей посредством PUSH–уведомлений.

5. Участник вправе отказаться от получения Одноразовых паролей посредством PUSH–уведомлений на Мобильное устройство Участника, дезактивировав функцию получения Одноразовых паролей посредством PUSH–уведомлений в Мобильном приложении Aton Line, установленном на таком устройстве.

6. ООО «АТОН» в обязательном порядке обеспечивает фиксацию фактов отправки и доставки адресату Одноразовых паролей посредством PUSH-уведомления. Факт отправки и доставки PUSH-уведомления подтверждается путем предоставления оператором информационной системы журнала записей из информационной системы на указанную дату и время (информация о дате и времени отправки PUSH-уведомления, текст отправленного PUSH-уведомления, дата и время доставки PUSH-уведомления Участнику), которая учитывается в технической информационной системе ООО «АТОН» и может быть предоставлена в случае возникновения спорной ситуации.

7. Подписание (пакета) электронных документов с использованием полученного посредством PUSH-уведомления Одноразового пароля осуществляется в Мобильном приложении Aton Line.

8. ООО «АТОН» вправе отказать в регистрации Идентификатора устройства Участника/активации функции получения Одноразовых паролей посредством PUSH–уведомлений на Мобильное устройство Участника в следующих случаях:

- в случае если есть подозрения на компрометацию идентификаторов Участника;
- в случае ненадлежащего оформления или отсутствия от Участника заявления, составленного по форме Приложения №11;
- в случае нарушения Участником настоящих Правил.

9. ООО «АТОН» не несет ответственность за нарушение обязательств вследствие сбоев в работе линий связи, обрыва линий связи, выхода из строя оборудования провайдера.

§ 5. Направление Участнику электронных документов посредством электронной почты

1. ООО «АТОН» в порядке, предусмотренном настоящим параграфом, направляет Участнику индивидуальные инвестиционные рекомендации в форме электронного документа, подписанного простой электронной подписью, посредством электронной почты в соответствии со стандартом RFC 2822 (https://www.ietf.org/rfc/rfc2822.txt) с помощью защищенных многоцелевых расширений электронной почты S/MIME (secure/multipurpose internet mail extensions).
2. ООО «АТОН» направляет электронные документы посредством электронной почты с адресов электронной почты, опубликованных на сайте ООО «АТОН» www.aton.ru в разделе «Адреса, предназначенные для отправки инвестиционных рекомендаций», на электронный адрес Участника.
3. Адрес отправителя электронного документа верифицируется с использованием протокола S\Mime и содержится в Сертификате ключа, выданном УЦ.
4. Корневой Сертификат ключа УЦ, используемый для подписи проверяемого Сертификата ключа, размещен на сайте ООО «АТОН» по адресу www.aton.ru.
5. Технические интернет заголовки сообщения электронной почты (электронного документа) содержат сервера отправителей ООО «АТОН», mx.aton.ru. Порядок просмотра технических заголовков устанавливается инструкцией на программное обеспечение, используемое Участником для работы с электронной почтой.

§ 6. Особенности обмена электронными документами посредством торговых систем, разработанных clientam.com на основе программного обеспечения Handy Trader

1. ООО «АТОН» осуществляет обмен электронными документами с Участником посредством торговых систем, разработанных clientam.com на основе программного обеспечения Handy Trader, в том числе информационной торговой системы Aton Trading в соответствии с настоящими Правилами с особенностями, предусмотренными настоящим параграфом.
2. Участник (его уполномоченное лицо), подавший в ООО «АТОН» заявление на оказание ему услуг по совершению сделок на международных рынках с использованием торговых систем в соответствии с Приложением № 24 к Регламенту оказания ООО «АТОН» брокерских услуг на рынках ценных бумаг считается подавшим ООО «АТОН» заявление на выдачу Участнику (его уполномоченному лицу) идентификаторов аутентификации и паролей к ним для работы в информационной торговой системе Aton Trading.
3. Идентификаторы для входа в информационную торговую систему Aton Trading направляются на Адрес электронной почты Участника (e-mail), пароль - на Номер мобильного телефона Участника посредством СМС-уведомлений.
4. После получения идентификаторов аутентификации и паролей к ним для работы через информационную торговую систему системыAton Trading, Участник должен самостоятельно согласно полученной вместе с идентификаторами инструкции зарегистрироввать Номер мобильного телефона Участника для получения одноразовых паролей в целях аутентификации Участника при входе в торговую систему. Номер мобильного телефона Участника, зарегистрированный для аутентификации Участника в информационной торговой системеAton Trading, должен совпадать с Номером мобильного телефона Участника для получения СМС – уведомлений, зарегистрированном в ООО «АТОН» в соответствии с заявлением Участника (приложения №№1, 8).
5. При смене Номера мобильного телефона Участника для получения СМС – уведомлений, Участник обязан зарегистрировать новый номер для использования его в целях аутентификации Участника при входе в информационную торговую системуAton Trading.
6. ООО «АТОН» имеет право не предоставлять или приостановить доступ Участника к обмену электронными документами посредством информационной торговой системы Aton Trading в следующих случаях:
   - 6.1. при несовпадении Номера мобильного телефона Участника, зарегистрированного для аутентификации Участника в информационной торговой системеAton Trading, с Номером мобильного телефона Участника для получения СМС – уведомлений, зарегистрированном в ООО «АТОН» в соответствии с заявлением Участника (приложения №№1, 8),
   - 6.2. при неосуществлении Участником регистрации Номера мобильного телефона Участника в соответствии с п.3 настоящего параграфа, а также
   - 6.3. в случаях, указанных в п.п. 5, 5.1 ст.4.1 § 4 Раздела 3 настоящих Правил в отношении Номера мобильного телефона Участника и Адреса электронной почты Участника, используемых в соответствии с настоящим параграфом,
7. Участник при наличии технической возможности вправе самостоятельно производить установку, замену паролей к идентификаторам аутентификации, а так же производить любые операции смены информации, предназначенной для его аутентификации согласно инструкции, которую предоставляет Interactive Brokers.
8. Одноразовые пароли для аутентификации Участника в информационных торговых системах Aton Trading направляются Участнику в соответствии с правилами работы Interacticve Brokers.

РАЗДЕЛ 4. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

§ 1. Основные положения

1. В ходе использования ключей электронной подписи, Сертификатов ключей и аутентификационных данных возможно возникновение конфликтных (спорных) ситуаций, связанных с формированием, доставкой, получением, подтверждением получения электронных документов, а также с использованием электронной подписи в электронных документах.

2.Причиной конфликтной ситуации может служить:

- оспаривание факта формирования электронного документа;
- оспаривание авторства электронного документа (подозрение на нарушение процедуры идентификации владельца ключа подписи, сформировавшего электронный документ);
- оспаривание целостности электронного документа (подозрение на нарушение свойства целостности электронного документа при его передаче по каналу связи);
- оспаривание факта отправления и (или) получения электронного документа;
- оспаривания времени отправления и (или) получения электронного документа;
- иные случаи возникновения конфликтных ситуаций.

3. Конфликтные ситуации разрешаются в рабочем порядке и/или с привлечением экспертной комиссии по разрешению конфликтной ситуации (далее – «Экспертная комиссия») в порядке, установленном настоящими Правилами.

4. Подтверждение подлинности усиленной неквалифицированной электронной подписи и Сертификата ключа в случае возникновения конфликтных ситуаций осуществляется с использованием программного обеспечения «Arbiter-PKI», разработанного ЗАО «Сигнал-Ком» на базе СКЗИ «Крипто-КОМ 3.2» и СКЗИ «Крипто-КОМ 3.3». Процедура подтверждения подлинности усиленной неквалифицированной электронной подписи основывается на математических свойствах алгоритма электронной подписи, реализованного в соответствии с ГОСТ 34.10-2001. Протокол проверки, формируемый указанной программой, является основным документом при разборе конфликтной ситуации.

5. Подтверждение подлинности простой электронной подписи осуществляется проверкой факта получения Участником аутентификационных данных для входа в информационную систему, наличием записей входа в информационную систему с предоставленными Участнику аутентификационными данными, существованием записей о формировании заявки в логе информационной системы, наличием записей о факте отправки и ввода одноразовых паролей.

6. Участники и ООО «АТОН» признают в качестве достаточного доказательства (пригодного также для предъявления при разрешении споров в суде) журнал событий, извлечённых из Информационных систем ООО «АТОН».

7. При разрешении конфликтных ситуаций, связанных с формированием, использованием электронной подписи, отправлением и (или) получением электронных документов посредством ИТС QUIK, Участники и ООО «АТОН» руководствуются документацией к ИТС QUIK разработчика ARQA Technologies.

8. ООО "АТОН" не несет ответственности за убытки, причиненные Участнику в результате неправомерных действий третьих лиц, направленных на незаконное использование ключей пользователя (публичного и секретного ключа) и/или логина и пароля Участника и/или иной конфиденциальной информации, касающейся его, за исключением убытков, причиненных Участнику в результате умышленного нарушения ООО «АТОН» условий настоящих Правил.

9. Участник соглашается с тем, что все заявки и иные электронные документы, направленные с использованием его ключей пользователя (публичного и секретного ключа) и/или логина и пароля, считаются поданными Участником. Электронный документ, направленный с использованием ключей или/и логина и пароля Участника, является достаточным основанием для оказания Участнику услуг на условиях заключенных с Участником договоров.

10. Выписки из электронных журналов и файлов серверной части ПО (в т.ч. серверов ИТС QUIK) (включая журнал операций, который представляет собой совокупность записей в базе данных, содержащих информацию об активных операциях/транзакциях, совершаемых в том числе с использованием ИТС QUIK Участниками (подача, модификация, отмена поручений, иных видов поручений/сообщений)), являются пригодным для предъявления в суде и достаточным доказательством факта совершения действий Участником, в том числе фактов установления (попытки установления) Участником соединения с сервером ИТС QUIK, подачи заявок Участником с использованием ИТС QUIK.

§2. Разрешение конфликтных ситуаций в рабочем порядке

2.1 ПОЛУЧЕНИЕ УВЕДОМЛЕНИЯ О КОНФЛИКТНОЙ СИТУАЦИИ

1. При возникновении обстоятельств, которые свидетельствуют о наличии конфликтной ситуации, Участник незамедлительно направляет в УЦ письменное уведомление о возникновении конфликтной ситуации с изложением обстоятельств и предполагаемых причин ее возникновения.

2. УЦ проверяет наличие указанных в уведомлении обстоятельств, и в случае необходимости осуществляет проверку в том числе подлинности Сертификатов ключей (п.п. 2.2-2.4 Правил), проверкой фактов выдачи Участнику аутентификационных данных (п.2.9 Правил), проверку электронной подписи, содержащейся в оспариваемом электронном документе (п.п. 2.7. – 2.11. Правил), и принимает меры по разрешению конфликтной ситуации (п.2.12. Правил).

3. Срок рассмотрения уведомления Участника УЦ составляет 15 (Пятнадцать) рабочих дней с даты его поступления в УЦ.

2.2. ПРОВЕРКА ПОДЛИННОСТИ СЕРТИФИКАТА КЛЮЧА, ВЫДАННОГО В ФОРМЕ БУМАЖНОГО ДОКУМЕНТА.

Проверка подлинности Сертификата ключа, выданного в форме бумажного документа, состоит в проверке следующих сведений, указанных в Сертификате ключа:

- паспортных данных владельца Сертификата ключа, серийного номера Сертификата ключа, ключа проверки электронной подписи, подписи владельца Сертификата ключа, подписи уполномоченного лица УЦ путем визуального сличения с имеющимися у УЦ образцами соответствующих подписей – для Участника, являющегося физическим лицом;
- наименования, место нахождения юридического лица, ФИО, паспортных данных, доверенности или учредительных документов юридического лица, на основании которых действует уполномоченный представитель Участника, подписи уполномоченного предствителя Участника, подписи уполномоченного лица УЦ путем визуального сличения с имеющимися у УЦ образцами соответствующих подписей – для Участника, являющегося юридическим лицом.

Подлинность Сертификата ключа, выданного в форме бумажного документа, считается установленной, если все указанные в Сертификате ключа сведения соответствуют, сведениям, имеющимся у УЦ.

2.3 ПРОВЕРКА ПОДЛИННОСТИ СЕРТИФИКАТА КЛЮЧА, ВЫДАННОГО В ФОРМЕ ЭЛЕКТРОННОГО ДОКУМЕНТА.

Проверка подлинности Сертификата ключа, выданного в форме электронного документа, осуществляется с помощью программного обеспечения «Arbiter-PKI» и включает в себя выполнение следующих действий:

- определение Сертификата ключа, необходимого для проверки;
- проверка Сертификата ключа уполномоченного лица УЦ,
- проверка отсутствия Сертификатов ключей в списке аннулированных сертификатов.

Подлинность Сертификата ключа, выданного в форме электронного документа, считается подтвержденной, если по итогам проверки с использованием программного обеспечения «Arbiter-PKI» формируется следующее сообщение: «Сертификат действителен».

2.4. ПРОВЕРКА ПОДЛИННОСТИ СЕРТИФИКАТА КЛЮЧА, СОЗДАННОГО ПРИ ИСПОЛЬЗОВАНИИ ДЕЙСТВУЮЩЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ ПО ИНИЦИАТИВЕ УЧАСТНИКА.

1.Проверка подлинности Сертификата ключа, созданного на основании электронного запроса Участника и подписанного действующей электронной подписью Участника, включает в себя следующие действия:

- Проверка электронной подписи, которой был подписан Запрос сертификата
- Определение цепочки Запросов сертификатов в электронном виде и Сертификатов ключей (каждый следующий Запрос сертификата подписан с использованием Сертификата ключа, изданного на основании предыдущего Запроса и имеет только электронную форму)
- Определение Сертификата ключа, который имеет электронную и бумажную форму, подписанную собственноручной подписью Участника.

2.Подлинность Сертификата ключа считается установленной, если

- электронная подпись под каждым Запросом сертификата действительна на момент подписания Запроса сертификата и издания Сертификата ключа на основании данного запроса,
- Сертификат ключа проверки электронной подписи, которой подписан каждый Запрос сертификата, действителен на момент подисания запроса,
- Сертификат ключа, который имеет бумажную форму, подписан собсвенноручной подписью Участника.

2.5. ПРОВЕРКА ФАКТА ОТПРАВЛЕНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТА.

Проверка факта отправления или получения электронного документа заключается в определении статуса электронного документа в реестре электронных документов.

Отправка электронного документа считается подтвержденной, если электронный документ подписан электронной подписью Участника и в реестре электронных документов имеет статус «опубликован».

Получение электронного документа считается подтвержденным, если электронный документ подписан электронной подписью Участника и в реестре электронных документов имеет статус «получен» или «в обработке».

2.6. ПРОВЕРКА ВРЕМЕНИ СОЗДАНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТА

Проверка времени создания электронного документа состоит в определении времени создания электронного документа в информационной системе.

2.7. ПРОВЕРКА ПОДЛИННОСТИ УСИЛЕННОЙ НЕКВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ В ЭЛЕКТРОННОМ ДОКУМЕНТЕ.

1. Проверка подписанного электронной подписью электронного документа включает в себя выполнение следующих действий:

- Определение электронного документа, содержащего электронную подпись. подлежащую проверке.
- Расшифровка электронного документа, выделение текста документа и электронной подписи (в случае необходимости).
- Определение даты формирования каждой электронной подписи, содержащейся в электронном документе
- Определение Сертификата ключа или нескольких Сертификатов ключей, необходимых для проверки электронной подписи в документе.
- Проверка данных, указанных в Сертификате ключа, выданного в форме бумажного документа.
- Проверка действительности Сертификата ключа (или нескольких сертификатов) на момент подписания электронного документа.
- Проверка действительности Сертификата ключа уполномоченного лица УЦ на момент подписания электронного документа.
- Проверка отсутствия Сертификатов ключей в списке аннулированных сертификатов.
- Проверка электронной подписи, содержащейся в электронном документе с использованием Сертификата ключа (или нескольких Сертификатов).

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

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

3. Если Сертификат ключа, необходимый для проверки подлинности электронной подписи, содержащейся в электронном документе, на дату проверки аннулирован или истек, УЦ принимает решение о действительности электронной подписи, содержащейся в электронном документе, используя дату создания документа и дату аннулирования Сертификата ключа в списке аннулированных сертификатов или дату окончания действия Сертификата.

2.8. ПРОВЕРКА ФАКТА ПОЛУЧЕНИЯ УЧАСТНИКОМ АУТЕНТИФИКАЦИОННЫХ ДАННЫХ ДЛЯ ВХОДА В ИНФОРМАЦИОННУЮ СИСТЕМУ И СОЗДАНИЯ ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

1. Проверка факта получения Участником аутенфикационных данных включает в себя выполнение следующих действий:

- установление наличия заявления Участника на получение логина\пароля (Приложение №5 к настоящим Правилам, Приложения № 3 к Регламенту оказания ООО «АТОН» брокерских услуг на рынках ценных бумаг);
- установление наличия заявления Участника о согласии на получение одноразовых паролей посредством СМС -уведомлений (Приложение №1, 8 к настоящим Правилам)/PUSH-уведомлений (Приложение № 11 к настоящим Правилам);
- установление наличия заявления на регистрацию публичного ключа пользователя для системы QUIK (Приложение №7 к настоящим Правилам);
- установление наличия заявления на регистрацию идентификаторов для iQUIK X (Приложение №12 к настоящим Правилам);
- установление наличия зарегистрированного Адреса электронной почты Участника и направления Участнику Уникальной ссылки.

2. Факт получения Участником аутенфикационных данных считается подтвержденным, если установлено наличие подписанного заявления участником либо его уполномоченным лицом, которое понадобится для проведения проверки.

2.9. ПРОВЕРКА ФАКТА НАЛИЧИЯ ЗАПИСЕЙ ВХОДА В ИНФОРМАЦИОННУЮ СИСТЕМУ, ОТПРАВКИ ОДНОРАЗОВЫХ ПАРОЛЕЙ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

1. Проверка осуществляется путем предоставления оператором информационной системы выгрузки журнала записей из информационной системы на указанную дату и время.

2. ООО «АТОН» запрашивает у Interactive Brokers выгрузки журнала записей из систем, которые предоставляет InteractiveBrokers на указанную дату и время.

2.10. ПРОВЕРКА ПОДЛИННОСТИ ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСИ В ЭЛЕКТРОННОМ ДОКУМЕНТЕ

1. Проверка подлинности простой электронной подписи, которой подписаны электронные документы, происходит следующим образом:

1) Определяется Участник.

2) Определяется Информационная система, в рамках которой была сформирована простая электронная подпись.

3) Определяются реквизиты Участника, предназначенные для его аутентификации в Информационной системе (идентификаторы аутентификации и информация, предназначенная для аутентификации Участника/ определяется Уникальная ссылка, направленная на Адрес электронной почты Участника и факт перехода Участника по Уникальной сслке).

4) Определяется электронный документ и его реквизиты.

5) Делается запрос в Информационную систему по реквизитам электронного документа.

6) В случае использования систем, предоставленных Interactive Brokers, ООО «АТОН» создает запрос InteractiveBrokers по реквизитам электронного документа и идентификаторам Участника.

7) Электронный документ должен быть сформирован в соответствии с Правилами и требованиями Информационной системы и проверяемый электронный документ должен быть подписан Участником Системы ЭДО

8) Осуществляется проверка извлечённого из Информационной системы электронного документа.

Подлинность простой электронной подписи в электронном документе считается подтвержденной, если по итогам проверки извлечённый из Информационной системы электронный документ содержит рекзвизиты Участника, предназначенные для его аутентификации в Информационной системе.

2. При проверке подлинности простой электронной подписи в случае использования одноразовых паролей, осуществляется сопоставление одноразового пароля, введенного Участником Информационной системы при подписании электронного документа, и пароля, направленного Участнику СМС – уведомлением на номер мобильного телефона, зарегистрированный в ООО «АТОН»/PUSH-уведомлением на Мобильное устройство Участника, Идентификатор которого с установленным на нем Мобильным приложением Aton Line зарегистрирован в ООО «АТОН». При положительном результате проверки идентичности указанных одноразовых паролей и положительной аутентификации Участника, использовавшего данный индентификатор для подписания электронного документа, подлинность простой электронной подписи считается подтвержденной.

3. При проверке подлинности простой электронной подписи в случае использования систем, предоставленных InteractiveBrokers ООО «АТОН» руководствуется информацией, которую предоставляет Interactive Brokers из своих информационных систем при получении запроса.

2.11. ПРОВЕРКА ПОДЛИННОСТИ ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСИ В ЭЛЕКТРОННОМ ДОКУМЕНТЕ, НАПРАВЛЕННОМ ПОСРЕДСТВОМ ЭЛЕКТРОННОЙ ПОЧТЫ

1. Проверка включает в себя выполнение следующих действий:

1) Определяется электронный документ (электронное почтовое сообщение), содержащее подлежащую проверке электронную подпись;

2) Осуществляется проверка наличия электронного адреса в списке Адресов, предназначенных для отправки инвестиционных рекомендаций, опубликованном на сайте www.aton.ru;

3) Определяется дата формирования каждой электронной подписи, содержащейся в электронном документе;

4) Определяется наличие подписи в соответствии с протоколом S\MIME в электронном документе. Наличие подписи по протоколуу S\MIME определяется в соответствии с инструкцией на программное обеспечение используемым участником для работы с электронной почтой (в частности, для Microsoft Outlook, это символ  в сообщении электронной почты);

5) Осуществляется проверка факта подписания Сертификата ключа, используемого для формирования электронной подписи (далее – «Сертификат ключа подписи»), корневым Сертификатом ключа УЦ;

6) Осуществляется проверка действительности Сертификата ключа подписи (или нескольких сертификатов ключа подписи) на момент подписания электронного документа;

7) Осуществляется проверка действительности корневого Сертификата ключа УЦ на момент подписания электронного документа;

8) Осуществляется проверка отсутствия Сертификатов ключей подписи в списке аннулированных сертификатов;

9) Определяется содержание сервера отправителей ООО «АТОН» в технических интернет заголовках сообщения электронной почты (проверяемого электронного документа).

2. Подлинность электронной подписи в электронном документе считается подтвержденной, в случае соответствия указанным выше требованиям.

2.12. МЕРЫ ПО РАЗРЕШЕНИЮ КОНФЛИКТНОЙ СИТУАЦИИ, ПРИНИМАЕМЫЕ УЦ ПО ИТОГАМ ПРОВЕРКИ

1. По результатам проверки УЦ составляет акт разбора конфликтной ситуации (далее – «Акт»), который должен содержать:

- дату и место составления Акта;
- действия, выполненные в результате проверки;
- основные выводы;
- подпись уполномоченного лица УЦ.

2. УЦ извещает доступными способами Участника, инициировавшего разбор конфликтной ситуации, о результатах проверки и, при необходимости, о мерах, принятых для разрешения конфликтной ситуации.

3. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если Участник, инициировавший разбор конфликтной ситуации, удовлетворен информацией, предоставленной ему, и не имеет к УЦ претензий по итогам проведенной проверки.

4. В случае если Участник не удовлетворен полученной информацией, и ситуация не была решена в рабочем порядке, формируется Экспертная комиссия для рассмотрения конфликтной ситуации.

§3. Разрешение конфликтных ситуаций Экспертной комиссией

3.1.ФОРМИРОВАНИЕ ЭКСПЕРТНОЙ КОМИССИИ.

1. Экспертная комиссия созывается на основании письменного заявления Участника.

Указанное заявление должно содержать:

- предмет конфликтной ситуации
- возможные причины и последствия конфликтной ситуации
- список предлагаемых для участия в работе Экспертной комиссии уполномоченных представителей Участника с указанием их фамилий, имен, отчеств, должностей, их контактной информации (телефоны, факсы, электронная почта).

2. Заявление составляется в форме бумажного документа, подписывается Участником и передается в УЦ в порядке, который обеспечивает подтверждение вручения корреспонденции.

Заявление может быть составлено и направлено в форме электронного документа. При этом факт доставки должен быть подтвержден.

3.В течение 3 (трех) рабочих дней после получения заявления УЦ формирует Экспертную комиссию.

4.Если Участники не договорятся об ином, в состав Экспертной комиссии входит равное количество уполномоченных представителей Участников, участвующих в разрешении конфликтной ситуации (но не больше четырех от каждого Участника). При этом в состав Экспертной комиссии в обязательном порядке включаются представители служб информационно-технического обеспечения, а также служб обеспечения информационной безопасности Участников.

В состав Экспертной комиссии в обязательном порядке входит уполномоченный представитель УЦ.

5. К работе Экспертной комиссии для проведения технической экспертизы могут быть привлечены независимые эксперты, из числа представителей поставщиков средств защиты информации, используемых в качестве средства электронной подписи при электронном взаимодействии Участников.

6. В случае если представитель(и) одного из Участников не явился(лись) для участия в проведении экспертизы, экспертиза проводится без их участия, а об отсутствии представителей составляется акт, который подписывается всеми присутствующими участниками Экспертной комиссии.

7. Основная задача Экспертной комиссии установить на организационно-техническом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о наличии конфликтной ситуации, ее причинах и последствиях, а также способах и методах ее разрешения.

3.2. ПРОВЕДЕНИЕ ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ.

1. Для проведения технической экспертизы в связи с использованием Участником усиленной неквалифицированной электронной подписи УЦ предоставляет аттестованный специальный персональный компьютер.

2. В присутствии членов Экспертной комиссии производится проверка оборудования и программного обеспечения, а также тестирование их работоспособности. Эта процедура проводится путем создания пробной электронной подписи в электронном документе и проверки этой подписи.

3. Проверка подлинности электронной подписи в электронном документае выполняется согласно п.2.7 Раздела 4 настоящих Правил

4.Если Сертификат ключа, необходимый для проверки электронной подписи. содержащейся в электронном документе, на данный момент времени уже не действителен, то Экспертная комиссия принимает решение о действительности электронной подписи, содержащейся в электронном документе, используя дату создания документа и дату окончания действия Сертификата ключа или его отзыва.

При положительном результате проверки электронной подписи, содержащейся в электронном документе подпись под документом считается подтвержденной.

5.Протокол проверки электронной подписи, формируемый с использованием программного обеспечения «Arbiter-PKI» (далее – «Протокол проверки»), является основным документом, закрепляющим результаты работы Экспертной комиссии и должен быть подписан всеми членами Экспертной комиссии.

6.Положительный результат проверки, зафиксированный в Протоколе проверки, означает, что электронный документ имеет юридическую силу. Неподтверждение подлинности электронного документа, зафиксированное в Протоколе проверки, будет означать, что представленный электронный документ не имеет юридической силы.

3.3 ПРОТОКОЛЫ И ОТЧЕТЫ РЕЗУЛЬТАТОВ РАБОТЫ КОМИССИИ

1. По всем действиям, предпринимаемым Экспертной комиссией, для выяснения фактических обстоятельств конфликтной ситуации составляется протокол работы Экспертной комиссии (далее – «Протокол»).

2.Протокол должен содержать следующие данные:

- дату и место составления Протокола;
- состав Экспертной комиссии с указанием фамилий, имен, отчеств, контактной информации;
- краткое изложение обстоятельств, свидетельствующих, по мнению Участника, о возникновении и/или наличии конфликтной ситуации;
- установленные Экспертной комиссией фактические обстоятельства конфликтной ситуации;
- наименование мероприятия, проводимого Экспертной комиссией, с указанием даты, времени и места его проведения;
- выводы, к которым пришла Экспертная комиссия в результате проведенного мероприятия;
- подписи всех членов Экспертной комиссии.

3.4 МЕРЫ ПО РАЗРЕШЕНИЮ КОНФЛИКТНОЙ СИТУАЦИИ, ПРИНИМАЕМЫЕ ПО ИТОГАМ РАБОТЫ ЭКСПЕРТНОЙ КОМИССИИ

1. По результьатам проверки, проведенной Экспертной комиссией, составляется Акт, который должен содержать следующую информацию:

- состав Экспертной комиссии;
- дату и место составления Акта;
- даты и время начала и окончания работы Экспертной комиссии;
- краткий перечень мероприятий, проведенных Экспертной комиссией;
- выводы, к которым пришла Экспертная комиссия в результате проведенных мероприятий;
- подписи членов Экспертной комиссии.

2. К Акту может прилагаться особое мнение члена или членов Экспертной комиссии, не согласных с выводами комиссии, указанными в Акте. Особое мнение составляется в произвольной форме, подписывается членом или членами Экспертной комиссии, чье мнение оно отражает.

3. Акт составляется в форме бумажного документа по одному экземляру каждому Участнику.

4.Конфликтная ситуация признается разрешенной по итогам работы Экспертной комиссии в случае, если Участники удовлетворены выводами, полученными Экспертной комиссией, и не имеют взаимных претензий в связи с разрешаемой конфликтной ситуацией.

В этом случае Участники в срок не позднее пяти рабочих дней со дня окончания работы Экспертной комиссии на основании ее выводов принимают соответствующие меры по разрешению конфликтной ситуации.

В случае невозможности разрешения конфликтной ситуации согласно установленному в настоящих Правилах порядку, Участники разрешают конфликтную ситуацию в суде согласно § 2 Раздела 6 настоящих Правил.

РАЗДЕЛ 5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

§ 1. Система обеспечения информационной безопасности

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

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

3. Соблюдение требований информационной безопасности при организации ЭДО обеспечивает:

- конфиденциальность информации (при передаче данных конфиденциальность обеспечивается использованием функций шифрования);
- целостность передаваемой информации (целостность защищаемых данных обеспечивается использованием функций усиленной неквалифицированной 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 ключа проверки электронной подписи 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 ЭДО;
- 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 ПО, используемого для получения услуг. Для проведения контроля целостности используется утилита *rush*, входящая в состав СКЗИ «Крипто-КОМ 3.2» и СКЗИ «Крипто-КОМ 3.3».

§ 2. Меры защиты ключей электронных подписей

1. Ключи электронных подписей при их генерации должны записываться на отчуждаемые носители ключевой информации.

2. Участник должен обеспечить надежное хранение в тайне ключа электронной подписи. Личные ключевые носители Участников должны храниться в сейфе. Участник несет персональную ответственность за хранение личных ключевых носителей.

3. Ключи электронной подписи на отчуждаемом носителе необходимо защищать паролем. Пароль формирует лицо, выполняющее процедуру генерации ключей.

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

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

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

7. Хранение 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, защищающий ключ электронной подписи.

8. Пересылка (передача) 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 wipe, входящая в состав СКЗИ «Крипто-КОМ 3.2» и СКЗИ «Крипто-КОМ 3.3», предназначенная для удаления файлов с ключевых носителей с предварительным их физическим затиранием.

§ 3. Компрометация ключевых носителей уполномоченного лица УЦ

1. В случае компрометации ключа электронной подписи уполномоченного лица УЦ выполняется аннулирование Сертификата ключа УЦ.

2. Информация о факте компрометации ключей уполномоченного лица УЦ размещается на странице www.aton.ru в сети Интренет, а Участники оповещаются о компрометации путем соответствующей рассылки по электронной почте.

3. Процедура внеплановой смены скомпрометированных ключей уполномоченного лица УЦ осуществляется в соответствии с порядком, установленным в п.14.2 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 ключа электронной подписи уполномоченного лица УЦ, считаются аннулированными и подлежат внеплановой смене.

§ 4. Компрометация ключевых носителей Участников

1. Участник (юридическое или физическое лицо) самостоятельно принимает решение о факте или угрозе компрометации своего ключа усиленной неквалифицированной электронной подписи и простой электронной подписи.

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;
- доступ, в том числе временный, посторонних лиц к файлу закрытого ключа или к информации о пароле для защиты закрытого ключа;
- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа третьих лиц к файлу закрытого ключа или паролю для защиты закрытого ключа, в том числе передача файла закрытого ключа или его пароля по незащищенным каналам связи.

3. К событиям неявной компрометации ключевой информации могут быть отнесены следующие подозрения:

- возникновение подозрений на утечку информации или ее искажение на оборудовании, содержащем ключевую информацию (например, в случае обнаружения вирусного заражения средствами антивирусной защиты, установки нелицензионного программного обеспечения и т.д.);
- нарушение печати на сейфе, хранилище ключевого носителя, содержащего ключ электронной подписи;
- доступ третьих лиц к оборудованию, содержащему ключевую информацию;
- другие случаи, когда нельзя достоверно установить, что произошло с ключевым носителем, содержащим ключ электронной подписи (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 ключевой информации, владельцу необходимо произвести оценку ситуации и самостоятельно принять решение по дальнейшему использованию ключевого носителя, содержащего ключ электронной подписи.

4. В случае компрометации или угрозы компрометации ключа электронной подписи Участник прекращает его использование, обращается в УЦ с заявлением об аннулировании Сертификата ключа, соответствующего скомпрометированному ключу и об аннулировании ключа простой электронной подписи . Ответственность за несвоевременное информирование УЦ, в том числе за возможные последующие негативные события, произошедшие в результате компрометации ключа электронной подписи, возлагается только на Участника. УЦ помещает соответствующий Сертификат ключа в Список аннулированных сертификатов с указанием причины «Компрометация ключа» и публикует Список аннулированных сертификатов в сетевом справочнике сертификатов.

5. В случае выявления УЦ обстоятельств, которые могут свидетельствовать о наступлении событий, отнесенных к явной и/или неявной компрометации ключевой информации, УЦ вправе аннулировать ключи, используемые Участником в Информационной системе.

6. ООО «АТОН» не несет ответственность за любые убытки, понесенные Участником, причиной которых является использование третьими лицами ключевой информации в случае ее компрометации.

§ 5. Компрометация пароля и личных идентификаторов Участника для доступа в Информационные системы

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

2. К событиям, относящимся к явной компрометации, 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»);
- выбытие из владения помимо воли Участника мобильного телефона, используемого Участником для получения СМС-уведомлений;
- выбытие из владения помимо воли Участника Мобильного устройства, на котором активирована функция получения Одноразовых паролей посредством PUSH–уведомлений;
- информация, получаемая на номер мобильного телефона Участника, стала доступна третьим лицам (в случае направления Участнику СМС-уведомлений);
- информация, получаемая на Мобильное устройство Участника, стала доступна третьим лицам (в случае направления Участнику PUSH-уведомлений).

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

3. К неявной компрометации 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 нелицензионного 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, владельцу необходимо произвести оценку ситуации и самостоятельно принять решение по дальнейшему использованию пароля и идентификаторов Участника.

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

5. В случае выявления УЦ обстоятельств, которые могут свидетельствовать о наступлении событий, отнесенных к явной и/или неявной компрометации пароля или идентификаторов Участника, УЦ вправе приостановить оказание Участнику услуг, связанных с использованием пароля или идентификаторов Участника, а также услуг по направлению Участнику одноразовых паролей посредством СМС или PUSH-уведомлений.

§ 6. Меры по защите информации предпринимаемые Участником при работе с Мобильными приложениями

1. Участник должен:

- на Мобильное устройство, с которого планируется осуществлять подключение, установить Мобильное приложение из официальных источников iOS - AppStore, Android;
- на Мобильном устройстве установить парольную защиту;
- установить антивирусное програмное обеспечение на Мобильное устройство, используемое для работы с Мобильными приложениями;
- завершать работу с Мобильным приложением через завершение сессии (осуществив выход из Мобильного приложения);
- при утрате Мобильного устройства, на который ООО «АТОН» отправляет СМС/PUSH - уведомления с Одноразовыми паролями, немедленно обратиться к своему оператору сотовой связи для блокировки абонентского номера или замены СИМ-карты, а также сообщить ООО «АТОН» об утрате Мобильного устройства для выявления возможных несанкционированных операций.

2. Ответственность за непринятие Участником мер, указанных в настоящем параграфе, несвоевременное информирование ООО «АТОН», за возможные последующие негативные события, произошедшие в результате компрометации данных, возлагается только на Участника.

РАЗДЕЛ 6. ОБМЕН СООБЩЕНИЯМИ, ДОКУМЕНТООБОРОТ

§ 1. Предоставление документов на бумажных носителях

1. Если иное не установлено настоящими Правилами любые документы могут предоставляться Участником на бумажных носителях лично в офис ООО «АТОН».
2. Документы, предоставленные Участником на бумажных носителях, должны быть подписаны от имени Участника.
3. Участник вправе направить в ООО «АТОН» почтой следующие документы:
   - Заявление на получение идентификатора (логина) и пароля (приложение №5);
   - Заявление о замене логина и пароля для входа в информационную систему (приложение №5А);
   - Заявление на регистрацию публичного ключа (приложение №7);
   - Заявление о согласии на получение одноразовых паролей посредством СМС-уведомлений (Приложение №8);
   - Заявление о согласии на получение одноразовых паролей посредством электронной почты (Приложение №9);
   - Заявление на регистрацию идентификаторов (логина) для iQUIK X (приложение №12).
4. Участник, отправивший в ООО «АТОН» документ по почте, должен посредством телефонной связи, подтвердить отправку документа. Для идентификации и аутентификации Участника Участником должны быть названы:
   a) наименование или фамилия и инициалы Участника;
   b) кодовое слово, установленное в рамках договора о брокерском обслуживании на рынке ценных бумаг, заключенного между Участником и ООО «АТОН».

В случае неисполнения данной обязанности, ООО «АТОН» вправе по своему усмотрению отказать Участнику в приеме полученного документа.
5. Подтверждения отправки документа в порядке, предусмотренном п.4 настоящего параграфа, не требуется в случае направления документа, подлинность подписи Участника на котором засвидетельствована нотариусом.
6. ООО «АТОН» вправе не принимать от Участника документы, не соответствующие типовым формам, установленным приложениями к настоящим Правилам.

РАЗДЕЛ 7. ПРОЧИЕ ПОЛОЖЕНИЯ

§ 1. Тарифы на услуги. Порядок расчетов

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

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

2) Если иное не предусмотрено Тарифами на услуги ООО «АТОН» расходы ООО «АТОН» подлежат возмещению по мере их возникновения при условии их предварительного согласования с Участником.

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 ООО «АТОН».

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

3. За исключением случаев, предусмотренных в п.9 настоящего параграфа, если Участник не является клиентом ООО «АТОН», то Участник обязан с 5 (Пятого) по 10 (Десятый) рабочий день по окончании календарного месяца, в котором между Участником и ООО «АТОН» заключено Соглашение об ЭДО, получить в ООО «АТОН» счет-фактуру, содержащую сведения о подлежащем уплате вознаграждении. Уплата вознаграждения должна быть осуществлена Участником единовременно в течение 30 (Тридцати) календарных дней по окончании календарного месяца, в котором между Участником и ООО «АТОН» заключено Соглашение об ЭДО.

4. Если Участник одновременно является клиентом ООО «АТОН», то размер и порядок оплаты услуг и возмещения расходов ООО «АТОН» устанавливаются Регламентом оказания ООО «АТОН» брокерских услуг на рынке ценных бумаг (далее – «Регламент ООО «АТОН») и Тарифными планами ООО «АТОН», являющимися Приложением №23 к Регламенту ООО «АТОН».

5. Если Участник одновременно является депонентом ООО «АТОН» по депозитарному договору, то размер и порядок оплаты услуг и возмещения расходов ООО «АТОН» устанавливаются Условиями осуществления

депозитарной деятельности Общества с ограниченной ответственностью «АТОН» (далее – «Условия») и Тарифами на услуги Депозитария ООО «АТОН», являющимися Приложением №19 к Условиям.

6. Если Участники осуществляют ЭДО в области, не связанной с оказанием ООО «АТОН» услуг на рынках ценных бумаг, на основании заключенного с ООО «АТОН» отдельного соглашения об оказании услуг по обеспечению ЭДО, то размер и порядок оплаты услуг и возмещения расходов ООО «АТОН» устанавливаются в соответствии с соглашением об оказании услуг по обеспечению ЭДО.

7. Если Участник одновременно является клиентом ООО «АТОН» по договору комиссии на совершение сделок с иностранной валютой на организованных торгах ПАО Московская Биржа (далее – «Договор комиссии»), то размер и порядок оплаты услуг и возмещения расходов ООО «АТОН» устанавливаются Договором комиссии и Тарифами ООО «АТОН» на услуги по совершению сделок с иностранной валютой на организованных торгах ПАО Московская Биржа, являющимися Приложением №5 к Договору комиссии.

8. Если Участник одновременно является клиентом ООО «АТОН» по договор об осуществлении учета иностранных финансовых инструментов, не квалифицированных в качестве ценных бумаг (далее – «Договор ИФИ»), то размер и порядок оплаты услуг и возмещения расходов ООО «АТОН» устанавливаются Договором ИФИ и Тарифами ООО «АТОН» на оказание услуг по учету иностранных финансовых инструментов, не квалифицированных в качестве ценных бумаг, являющимися Приложением №4 к Договору ИФИ.

9. Если Участник одновременно является лицом, оказывающим ООО «АТОН» услуги по сопровождению/обслуживанию клиентов в рамках Партнерского соглашения об организации обслуживания на рынке ценных бумаг (договор об оказании услуг) (далее – «Партнерское соглашение»), то Участник обязан оплатить предусмотренные параграфом 3.1 раздела 6 настоящих Правил услуги ООО «АТОН» в течение 15 (Пятнадцати) рабочих дней по окончании каждого календарного года. Суммы, подлежащие уплате Участником, указываются в предоставляемых Участнику актах об оказании услуг и счетах-фактурах.

§ 2. Арбитражное соглашение

1. Споры, возникающие из Соглашения об ЭДО, или прямо или косвенно связанные с ним, в том числе касающиеся его заключения, существования, изменения, исполнения, нарушения, расторжения, прекращения и действительности, подлежат разрешению в порядке арбитража (третейского разбирательства), администрируемого Арбитражным центром при Российском союзе промышленников и предпринимателей (РСПП) в соответствии с его правилами, действующими на дату подачи искового заявления.
2. Вынесенное третейским судом решение будет окончательным, обязательным для сторон и не подлежит оспариванию.

§ 3. Порядок электронного документооборота при заключении договоров с ООО «АТОН»

1. В целях заключения договора о брокерском обслуживании, депозитарного договора, договора об осуществлении учета иностранных финансовых инструментов, не квалифицированных в качестве ценных бумаг (ИФИ), договора на ведение индивидуального инвестиционного счета (ИИС), депозитарного договора для ИИС, договора об учете ИФИ для ИИС (далее – «Договоры»), Участник вправе направлять в ООО «АТОН» следующие документы в электронном виде, подписанные электронной подписью через сеть «Интернет» или посредством Мобильного приложения Aton Space в соответствии с Правилами электронного документооборота ООО «АТОН»:
   1.1. заявление о заключении договоров по образцу приложения № 1 к Регламенту ООО «АТОН», Условиям, приложения №5 к Договору ИФИ;
   1.2. анкету физического лица по образцу, опубликованному на сайте ООО «АТОН», включающую согласие на обработку персональных данных;
   1.3. поручение по образцу приложения № 10.1. к Регламенту ООО «АТОН».
2. Участник, являющийся физическим лицом (далее – «Клиент»), при заключении с ООО «АТОН» Договоров вправе предоставить ООО «АТОН» и/или другому Участнику, оказывающему ООО «АТОН» услуги по сопровождению/обслуживанию клиентов ООО «АТОН» в рамках Партнерского соглашения (далее – «Исполнитель»), согласие на обработку его персональных данных (далее – «Согласие»), направив ООО «АТОН» Согласие в электронной форме, подписанное электронной подписью, через сеть «Интернет» в соответствии с настоящими Правилами.
3. Заключая с ООО «АТОН» Соглашение об ЭДО Клиент и Исполнитель соглашаются признать Согласие, подписанное электронной подписью Клиента, направленное Клиентом в порядке, предусмотренном настоящими Правилами, равнозначным документу на бумажном носителе, подписанному собственноручной подписью Клиента.
4. Клиент и Исполнитель признают, что копия Согласия на бумажном носителе, удостоверенная подписью уполномоченного лица ООО «АТОН», допускается в качестве письменного доказательства при разрешении конфликтных ситуаций и/или споров в досудебном порядке и/или суде, третейском суде, государственных и муниципальных органах, иных организациях.

§ 3.1 Порядок оказания ООО «АТОН» услуг Участнику (Исполнителю), заключившему с ООО «АТОН» Партнерское соглашение

1. В связи с предоставлением Клиентом при заключении Договоров с ООО «АТОН» в порядке, установленном в параграфе 3 раздела 6 настоящих Правил, Согласия, адресованного Исполнителю, ООО «АТОН» оказывает Исполнителю следующие услуги:
   1.1. ООО «АТОН» передает Исполнителю информацию о Клиентах, предоставивших Согласие, на адрес электронной почты Исполнителя не позднее 10 (десяти) рабочих дней следующих за днем получения Согласия;
   1.2. ООО «АТОН» передает Исполнителю копии полученных Согласий по письменному требованию Исполнителя не позднее 10 (десяти) рабочих дней, следующих за датой получения ООО «АТОН» требования о предоставлении копий документов, в указанной Исполнителем форме:
      1.2.1. в электронном виде на адрес электронной почты Исполнителя; либо
      1.2.2. на бумажном носителе. Верность копии Согласия на бумажном носителе удостоверяется подписью уполномоченного лица и печатью ООО «АТОН»,
   1.3. ООО «АТОН» осуществляет ежедневное резервное копирование и архивное хранение полученных от Клиентов Согласий, их реквизитов, включая информацию о датах и времени получения (отправки) в течение не менее 5 (пяти) лет с даты прекращения отношений с Клиентом.
   1.4. ООО «АТОН» осуществляет хранение журналов регистрации событий аппаратных средств (средств вычислительной техники) и программного обеспечения, подтверждающих факт проставления Клиентом аналога собственноручной подписи Клиента и подачи Согласия Клиентом в рамках электронного документооборота ООО «АТОН» в течение не менее 5 (пяти) лет с даты прекращения отношений с Клиентом.

§ 4. Приложения к настоящим Правилам

К настоящим Правилам прилагаются и являются их неотъемлемой частью:

Приложение №1, 1А. Заявление о заключении договоров;

Приложение №2. Заявление на формирование ключей электронной подписи;

Приложения №№3, 3А. Заявление на выдачу сертификата ключа проверки электронной подписи;

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

Приложение №5. Заявление на получение идентификатора (логина) и пароля;

Приложение №5А. Заявление о замене логина и пароля для входа в информационную систему;

Приложение №6. Тарифы на услуги ООО «АТОН»;

Приложение №7. Заявление на регистрацию публичного ключа пользователя для ИТС QUIK.

Приложение №8. Заявление о согласии на получение одноразовых паролей посредством СМС-уведомлений.

Приложение №9. Заявление о согласии на получение одноразовых паролей посредством электронной почты.

Приложение №10. Акт об оказанных услугах.

Приложение №11. Заявление о согласии на получение одноразовых паролей посредством PUSH – уведомлений.

Приложение №12. Заявление на регистрацию идентификаторов (логина) для iQUIK X.