УТВЕРЖДЕН

Приказом

Генерального директора

ООО «МБ Защита информации»

от «23» октября 2025 г. № МБ-ЗИ/П-2025-18

Регламент

Уполномоченного представителя Удостоверяющего центра

г. Москва, 2025

1. Термины и определения

1.1. В настоящем Регламенте Уполномоченного представителя Удостоверяющего центра (далее – «Регламент»), если из текста прямо не вытекает иное, используются термины, имеющие следующее значение:

«Договор» – договор, заключенный между Уполномоченным представителем и Клиентом, на основании Заявления о присоединении, в порядке, предусмотренном Регламентом.

«Заявитель» – лицо, намеревающееся заключить Договор.

«Заявление» – Заявление на создание сертификата, Заявление на аннулирование сертификата, а также иные заявления, предусмотренные Регламентом.

«Клиент» – лицо, заключившее Договор с Уполномоченным представителем.

«Уполномоченный представитель» – ООО «МБ Защита информации» (ОГРН: 1187746857770), являющееся доверенным лицом Удостоверяющего центра и наделённое полномочиями по приёму Заявлений и вручению Сертификатов от имени Удостоверяющего центра на основании договора, заключённого между Уполномоченным представителем и Удостоверяющим центром в соответствии с частью 4 статьи 13 ФЗ "Об электронной подписи".

«Удостоверяющий центр» или «УЦ» – юридическое лицо, учрежденное и действующее в соответствии с законодательством РФ, в том числе на основании лицензии ФСБ России на осуществление распространения шифровальных (криптографических) средств и информационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств и информационных систем, защищенных с использованием шифровальных (криптографических) средств, выполняющее функции удостоверяющего центра по созданию и управлению сертификатами ключей проверки усиленной неквалифицированной электронной подписи в соответствии с ФЗ "Об электронной подписи"». Сведения об УЦ доводятся до Заявителя/Клиента в письменной форме УП УЦ по запросу Заявителя, Клиента. Сведения об УЦ также содержатся во вручаемом Сертификате.

«Стороны» – Клиент и Уполномоченный представитель. Термин «Сторона» означает любую из Сторон.

«Тарифы» – приложение к Регламенту, определяющее стоимость и порядок оплаты за услуги, оказываемые Уполномоченным представителем.

«Пользователь» – физическое лицо, являющееся полномочным представителем Клиента, сведения о котором указываются в Заявлении о создании сертификата и могут быть указаны в Сертификате. Пользователь является владельцем Сертификата наряду с Клиентом.

«Заявление на создание сертификата» – заявление на создание Сертификата, форма которого приведена в Приложении № 2 к Регламенту.

«Доверенность на владельца сертификата» – доверенность, оформленная Клиентом на Пользователя, предоставляющая Пользователю право использования Сертификата, созданного в УЦ, от имени и в интересах Клиента. Форма доверенности приведена в Приложении № 3 к Регламенту.

«Заявление на аннулирование сертификата» – заявление о прекращении действия (аннулировании) Сертификата, форма которого приведена в Приложении № 4 к Регламенту.

«Сертификат» – сертификат ключа проверки электронной подписи (также – "СКПЭП"), электронный документ, созданный Удостоверяющим центром и подтверждающий принадлежность Ключа ЭП владельцу Сертификата (Пользователю). В рамках Регламентом под СКПЭП понимается СКЭП усиленной неквалифицированной электронной подписи.

«Ключ ЭП» – уникальная последовательность символов, предназначенная для создания электронной подписи.

«КЭП» - усиленная квалифицированная электронная подпись.

«Электронная почта Клиента» – адрес электронной почты Клиента, указанный в Заявлении о создании сертификата.

«Рабочий день УЦ» – промежуток времени с 9 часов 00 минут до 18 часов 00 минут по местному времени часового пояса г. Москвы каждого дня недели за исключением субботы, воскресенья и праздничных нерабочих дней в соответствии с законодательством Российской Федерации.

«Сайт» – сайт Уполномоченного представителя в сети «Интернет», доступ к которому осуществляется по ссылке https://me-informationsecurity.com/ru/document.

«Средства электронной подписи» (СЭП) – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

«ФЗ "Об электронной подписи"» – Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ.

Все иные термины, определения которых не даны в настоящем разделе 1 Регламента, применяются в соответствии с их значениями, определенными в ФЗ «Об электронной подписи», а также в соответствии со значениями, изложенными в иных действующих нормативных правовых актах.

2. Общие положения

2.1. Регламент определяет условия оказания услуг Уполномоченным представителем, включая порядок направления и рассмотрения заявлений на создание Сертификата и заявлений на аннулирование Сертификата, а также вручения Сертификатов.

2.2. Отношения между Сторонами по поводу создания Сертификатов в УЦ регулируются Регламентом и иными соглашениями, заключенными между ними, в той степени, в которой такие соглашения не противоречат Регламенту.

2.3. Регламент не является публичным договором в значении, предусмотренном статьей 426 Гражданского кодекса Российской Федерации.

2.4. Регламент является договором присоединения в значении, предусмотренном статьей 428 Гражданского кодекса Российской Федерации.

2.5. Договор, заключенный на основании Заявления о присоединении, носит рамочный характер в значении, предусмотренном статьей 429.1 Гражданского кодекса Российской Федерации.

2.6. Клиент, присоединившийся к Регламенту, считается согласным и обязан соблюдать условия УЦ, определенные в документах УЦ, связанных с порядком выпуска, аннулирования СКПЭП и иными вопросами, возникающими в процессе создания, использования, аннулирования СКПЭП.

3. Внесение изменений в Регламент

3.1. Настоящий Регламент, включая все Приложения, утверждается Уполномоченным представителем. Изменения и дополнения в настоящий Регламент вносятся Уполномоченным представителем в одностороннем порядке. Уполномоченный представитель вправе определять сроки и порядок вступления в силу изменений и дополнений в настоящий Регламент.

3.2. Новая редакция Регламента вступает в силу по истечении 5 (пяти) Рабочих дней со дня её размещения на Сайте.

3.3. Регламент в обновленной редакции считается акцептованным Клиентом, в случае если на дату вступления в силу соответствующей редакции Регламента, Уполномоченным представителем не получено уведомление об отказе от Договора в соответствии с п. 3.2 Регламента.

4. Порядок присоединения к Регламенту

4.1. Заявитель заключает Договор путем предоставления Уполномоченному представителю заявления о присоединении к Регламенту по форме приложения 1 к Регламенту, подписанного лицом, обладающим полномочиями подписать такое заявление от имени Заявителя - юридического лица, что подтверждается копиями документов, представленных Заявителем.

4.2. Договор считается заключенным с даты регистрации договора Уполномоченным представителем, о чём Уполномоченный представитель уведомляет Клиента путем направления Уполномоченным представителем сообщения на адрес электронной почты, указанный Клиентом в заявлении о присоединении к Регламенту.

4.3. После заключения Договора Клиент вправе направлять Заявления на создание сертификатов в адрес УЦ. Такие заявления могут быть поданы одновременно с заявление о присоединении к Регламенту.

4.4. В случае направления Заявления на создание сертификата и сопутствующих документов в электронном виде такой пакет документ может быть направлен для УЦ на адрес электронной почты Уполномоченного представителя: mbzi_inbox@moex.com.

5. Порядок оказания услуг по созданию Сертификатов

5.1. Уполномоченный представитель оказывает услуги по созданию Сертификатов на основании направленных от Клиента Заявлений на создание сертификата. Услуга включает получение и обработку полученного Уполномоченным представителем от Клиента Заявления на создание сертификата, проведение идентификации, передачу Заявления и/или сведений из него в УЦ. Непосредственное создание Сертификата осуществляется УЦ. Если Заявление на создание сертификата подписано не единоличным исполнительным органом Клиента, а представителем, то к Заявлению обязательно прикладывается доверенность, подтверждающая полномочия лица, подписавшего Заявление.

5.2. Документы, предусмотренные пунктом 5.1 Регламента, могут быть предоставлены только в Рабочий день. В случае предоставления Уполномоченному представителю соответствующих документов в Рабочий день после 17.00 по московскому времени, указанные документы считаются полученными и принимаются в работу на следующий Рабочий день.

5.3. Для получения услуги по созданию СКПЭП лицо, указанное в качестве Пользователя в Заявлении на создание сертификата, обязано пройти идентификацию, которая проводится с учётом положений ФЗ «Об электронной подписи», в порядке, определенном разделом 6 Регламента.

5.4. По итогам проведения идентификации Уполномоченный представитель вправе принять одно из следующих решений:

– о принятии Заявления на создание сертификата к исполнению;

– о приостановлении рассмотрения Заявления на создание сертификата и запросе дополнительных документов;

– об отказе в удовлетворении Заявления о создании сертификата.

5.5. Уполномоченный представитель вправе запрашивать у Клиента документы для подтверждения предоставленных им сведений, а также дополнительные документы, подтверждающие достоверность предоставленных сведений.

6. Порядок создания Сертификата

6.1. Клиент вправе предоставить Заявление на создание сертификата как в бумажной форме, так и в виде электронного документа, подписанного КЭП.

Если для подтверждения каких-либо сведений, вносимых в СКПЭП, действующим законодательством установлена определенная форма документа, Заявитель представляет Уполномоченному представителю документ с соблюдением соответствующей формы.

Вместе с Заявлением на создание сертификата Клиент обязуется предоставить следующие документы:

– копия паспорта (страница с фотографией и страница с адресом регистрации) Пользователя (либо в бумажной форме – заверенная нотариально или руководителем организации (или уполномоченным лицом), либо в электронной форме – заверенная с помощью КЭП единоличного исполнительного органа Клиента, либо с помощью КЭП уполномоченного Клиентом лица);

– скан-копия свидетельства государственного пенсионного страхования (СНИЛС) Пользователя;

– если Заявление подаётся лицом, не являющимся руководителем организации, - доверенность на Пользователя в бумажной (либо оригинал, либо нотариально заверенная копия) или в электронной форме (в виде электронного документа, подписанного КЭП единоличного исполнительного органа Клиента);

– если Заявление подаётся лицом, являющимся руководителем организации, - заверенная копия документа, подтверждающего право заявителя действовать от имени юридического лица без доверенности (либо в виде бумажного документа, либо в виде электронного документа, подписанного КЭП уполномоченного лица Клиента).

Уполномоченный представитель оставляет за собой право запросить иные документы от Клиента в целях разрешения спорных ситуаций, связанных с подтверждением правоспособности Клиента и полномочий его представителя, в том числе лица, которое вправе действовать от имени Клиента без доверенности.

Перечисленные выше документы либо их надлежащим образом заверенные бумажные копии предоставляются только в случае, если они не были предоставлены Клиентом Уполномоченному представителю ранее.

В случае изменения ранее представленных сведений, Клиент обязуется предоставить документы, подтверждающие такие изменения, в той же форме, в которой документы предоставлялись первоначально.

6.2. В соответствии с ФЗ «Об электронной подписи» Уполномоченный представитель обязан идентифицировать заявителя-будущего владельца СКПЭП (Пользователя).

В целях получения создания СКПЭП в УЦ Клиенту доступны следующие способы идентификации:

– при его личном присутствии;

– без личного присутствия, с использованием квалифицированной электронной подписи (при наличии действующего квалифицированного сертификата Пользователя);

– без личного присутствия Пользователя, посредством идентификации с использованием услуг нотариуса, связанных с идентификацией личности по фотографии;

– без личного присутствия Пользователя, посредством его идентификации руководителем организации, от имени которой он будет получать и использовать СКПЭП;

– без личного присутствия Пользователя, с использованием простой электронной подписи, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации, и при условии организации взаимодействия удостоверяющего центра с ЕСИА (единой системой идентификации и аутентификации);

– иным способом, не противоречащим нормам ФЗ "Об электронной подписи", согласованным Сторонами.

6.3. Уполномоченный представитель проверяет правильность оформления предоставленных документов. В случае если Клиент предоставил документы, форма которых не соответствует формам, установленным настоящим Регламентом, Уполномоченный представитель вправе отказать Клиенту в предоставлении услуг до момента предоставления Клиентом надлежаще оформленных в соответствии с настоящим Регламентом документов.

6.4. В случае соответствия предоставленных Клиентом документов требованиям по составу пакета документов, оформлению документов, наличию полномочий у подписантов предоставленных документов, Уполномоченный представитель передаёт их в УЦ, который создаёт Сертификат.

6.5. Срок действия для Ключа электронной подписи владельца СКПЭП устанавливается в УЦ при формировании СКПЭП равным 1 (одному) году, срок действия СКПЭП – 10 (десяти) годам.

6.6. Выдача Клиенту средств электронной подписи, обеспечивающих возможность создания Ключа электронной подписи и ключа проверки электронной подписи, осуществляется УЦ через Уполномоченного представителя.

7. Порядок прекращения действия (аннулирования) Сертификата

7.1. Сертификат прекращает свое действие в следующих случаях:

7.1.1. в случае прекращения действия Договора;

7.1.2. в случае прекращения действия Доверенности на владельца Сертификата;

7.1.3. по заявлению Пользователя или Клиента (форма Заявления на аннулирование сертификата приведена в Приложении № 4 к Регламенту);

7.1.4. по истечении срока действия Сертификата;

7.1.5. в иных случаях, предусмотренных действующим законодательством РФ или правилами УЦ.

7.2. Клиент обязан направить Заявление на аннулирование Сертификата в случае нарушении или угрозы нарушения конфиденциальности Ключа ЭП, а также если данные, указанные в Сертификате, утратили свою актуальность и (или) являются недостоверными.

7.3. Клиент не вправе использовать Ключ ЭП и связанный с ним Сертификат с момента направления Заявления о на аннулирование сертификата.

7.4. Действие СКПЭП прекращается с момента внесения записи об этом в реестр сертификатов.

8. Иные условия

8.1. Клиент обязуется:

8.1.1. оплачивать услуги Уполномоченного представителя путем перечисления денежных средств на его расчетный счет в течение 5 (пяти) рабочих дней с даты получения счета на оплату услуг Уполномоченного представителя (в случае исполнения третьим лицом обязательств по оплате услуг, в Заявлении о присоединении к Регламенту указываются следующие данные: фирменное наименование и основной государственный регистрационный номер плательщика);

8.1.2. обеспечить конфиденциальность Ключа ЭП, в том числе принимать все возможные меры для предотвращения его утраты, раскрытия и несанкционированного использования;

8.1.3. не использовать Ключ ЭП, связанный с Сертификатом, действие которого прекращено в соответствии с разделом 7 Регламента;

8.1.4. извещать Уполномоченного представителя об изменении любой информации, предоставляемой Уполномоченному представителю, в том числе содержащейся в Заявлении о создании Сертификата или Сертификате;

8.1.5. следить за сроками действия Сертификатов и в случае необходимости получения нового Сертификата заблаговременно подавать Заявление на создание Сертификата.

8.2. Клиент заверяет, что им получены необходимые письменные согласия физических лиц на обработку их персональных данных Уполномоченным представителем и Удостоверяющим центром.

8.3. В том, что не предусмотрено настоящим Регламентом, Стороны руководствуются положениями внутренних документов УЦ, описывающих порядок выдачи и аннулирования Сертификатов, а также нормами ФЗ «Об электронной подписи».

8.4. В случае противоречия между положениями настоящего Регламента и правилами Удостоверяющего центра, приоритет имеют правила Удостоверяющего центра.

9. Прекращение Договора

9.1. Каждая из Сторон вправе отказаться от исполнения Договора посредством направления другой Стороне соответствующего уведомления. Отказ от исполнения Договора вступает в силу по истечении 5 (пяти) Рабочих дней с даты получения другой Стороной такого уведомления.

9.2. Отказ Стороны от исполнения Договора является также отказом такой Стороны от услуг, оказываемых на основании Заявлений о создании сертификата, если к моменту отказа Стороны от исполнения Договора услуги по таким по таким Заявлениям не оказаны в полном объеме.

10. Ответственность

10.1. Во избежание сомнений Уполномоченный представитель не несет ответственности за любые убытки, возникшие у Клиента вследствие:

10.1.1. истечения сроков действия Ключа ЭП и (или) Сертификата;

10.1.2. нарушении или угрозы нарушения конфиденциальности Ключей ЭП, их утраты или несанкционированного доступа к ним и их использования третьими лицами;

10.1.3. нарушения Клиентом Регламента.

10.2. Ответственность Уполномоченного представителя по Договору всегда ограничивается исключительно прямым реальным документально подтверждённым ущербом для Клиента.

11. Конфиденциальность

11.1. Сведения, передаваемые Уполномоченному представителю, но не включаемые в Реестр Сертификатов, являются конфиденциальными.

11.2. Уполномоченный представитель и Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством РФ и Договором.

11.3. Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

12. Разрешение споров

12.1. Все споры, разногласия и претензии, которые могут возникнуть в связи с заключением, исполнением или расторжением Договора, признанием Договора

недействительным или незаключенным, Стороны будут стремиться решить путем переговоров. Сторона, у которой возникли претензии и/или разногласия, направляет другой Стороне сообщение с указанием возникших претензий и/или разногласий с приложением документов, обосновывающих заявленные требования.

12.2. В случае если ответ на сообщение не будет получен направившей сообщение Стороной в течение 10 (десяти) Рабочих дней с даты направления соответствующего сообщения, либо если Стороны не придут к соглашению по возникшим претензиям и/или разногласиям в течение указанного срока, спор подлежит разрешению в Арбитражном суде города Москвы.

Приложение № 1
к Регламенту Уполномоченного представителя Удостоверяющего центра

Форма заявления о присоединении к договору

Заявление о присоединении
к Регламенту Уполномоченного представителя УЦ

г. Москва «____» _____ 202__ г.

_____
(полное наименование заявителя, ОГРН)

в лице _____,

действующего на основании _____,

в соответствии со статьей 428 Гражданского кодекса Российской Федерации полностью и безусловно присоединяется к Регламенту Уполномоченного представителя УЦ, текст которого определен на сайте по ссылке: https://me-informationsecurity.com/ru/document (далее – «Регламент»), с даты регистрации Уполномоченным представителем УЦ настоящего Заявления о присоединении.

Термины, используемые в заявлении, толкуются в соответствии с Регламентом.

Заявитель ознакомлен с условиями Регламента и согласен, что Регламент и Тарифы на Услуги Уполномоченного представителя могут быть изменены Уполномоченным представителем в одностороннем порядке.

Реквизиты и контактные данные Уполномоченного представителя указаны в Регламенте.

Исполнение обязательств по оплате услуг Уполномоченного представителя

☐ будет осуществляться Заявителем самостоятельно;

☐ возложено на: _____.
(фирменное наименование, ОГРН)

_____

Адрес эл. почты Подпись Расшифровка подписи

Заполняется Уполномоченным представителем	
Дата регистрации заявления о присоединении	«____» _____ 202__ г.
Присвоенный номер договора	_____
Подпись и расшифровка	_____ / _____
Реквизиты доверенности представителя (поле заполняется, если подписывает не ЕИО)	от «____» _____ 202__ г. № _____

Приложение № 2
к Регламенту Уполномоченного представителя Удостоверяющего центра

Форма

Заявление
на создание сертификата ключа проверки электронной подписи

1. _____

(полное наименование организации, включая организационно-правовую форму)

в лице _____
(ФИО заявителя, действующего от имени юридического лица)

просит создать СКПЭП в соответствии с указанными в настоящем заявлении данными:

Атрибуты имени субъекта (DN) для создаваемого СКПЭП Пользователя:

INN*	ИНН организации
OGRN/OGRNIP**	ОГРН организации
SNILS***	Страховой номер индивидуального лицевого счета (СНИЛС) владельца СКПЭП
title (T)	Должность владельца СКПЭП
commonName (CN)	Фамилия, имя и отчество владельца СКПЭП
organizationUnitName (OU)	Подразделение организации
organizationName (O)	Наименование организации
localityName (L)	Наименование населенного пункта
stateOrProvinceName (ST)	Наименование территориального субъекта (например, 77 г. Москва)

* Поле заполняется только для лица, поставленного на учет в налоговом органе РФ

** Поле заполняется только для лица, зарегистрированного на территории РФ

*** Поле заполняется только для владельца СКПЭП, являющегося гражданином РФ

2. Порядок идентификации Пользователя:[1]

☐ при личном присутствии;

☐ без личного присутствия, с использованием действующей квалифицированной электронной подписи Пользователя;

☐ без личного присутствия Пользователя, посредством его идентификации руководителем организации, от имени которой он будет получать и использовать СКПЭП;

☐ без личного присутствия Пользователя, с использованием услуг нотариуса.

3. Заявитель действует на основании:

☐ учредительных документов (Устава); ☐ является ИП; ☐ доверенности

4. Заявитель будет использовать СКЗИ:

☐ на территории РФ; ☐ за пределами территории РФ

[1] Заполняется только в случае первичного создания СКПЭП с указанными в заявлении данными

5. Тариф (вариант создания СКПЭП) для внесения изменений в действующий СКПЭП:[2]

   ☐ создание СКПЭП;

   ☐ замена действующего СКПЭП в связи с внесением изменений.

6. Контактное лицо Заявителя:

   ФИО: . . . . . .

   Телефон: . . . . . .

   E-Mail: . . . . . .

_____ _____

(подпись) (фамилия, инициалы)

«_____» _____ 202__ г.

[2] Заполняется только в случае внесения изменений в действующий СКПЭП

Приложение № 3
к Регламенту Уполномоченного представителя Удостоверяющего центра

Форма

Доверенность № _____

_____ _____
(место выдачи) (дата выдачи)

_____,
(полное наименование организации, включая организационно-правовую форму)

далее – Клиент, в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании Устава, уполномочивает

_____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан)

1. Подписать Заявление о присоединении к Регламенту Уполномоченного представителя Удостоверяющего центра, утверждённому ООО «МБ Защита информации»[3].

2. Представлять интересы Клиента в качестве владельца СКПЭП (сертификата ключа проверки электронной подписи) и создавать в Удостоверяющем центре (УЦ) сертификаты ключей проверки электронных подписей с целью последующего их использования в интересах Клиента.

2. В рамках поручения, указанного в п. 1 настоящей доверенности, подписывать заявление на создание сертификата ключа проверки электронной подписи или заявление на аннулирование сертификата ключа проверки электронной подписи, владельцем которого является указанное доверенное лицо, сертификат ключа проверки электронной подписи в форме документа на бумажном носителе для последующего использования сертификата и соответствующего ему криптографического ключа в течение срока действия, указанного в сертификате, от имени Клиента и по его указанию.

Настоящая доверенность действительна по "_____" _____ 202__ года.

_____
Должность, фамилия и инициалы руководителя организации

_____
Подпись руководителя организации

[3] Полномочие необходимо, если присоединение к Регламенту осуществляется Пользователем, а не руководителем Клиента.

Приложение № 4
к Регламенту Уполномоченного представителя Удостоверяющего центра

Форма

Заявление
на аннулирование сертификата ключа проверки электронной подписи

1. _____

(полное наименование организации, включая организационно-правовую форму)

в лице _____
(должность уполномоченного представителя организации)

_____,
(фамилия, имя, отчество уполномоченного представителя организации)

действующего на основании ☐ устава; ☐ доверенности _____,

в связи с _____
(причина аннулирования СКПЭП)

просит аннулировать СКПЭП, содержащий следующие данные:

serialNumber	*Серийный номер СКПЭП*
имя издателя СКПЭП (DN)	*INN=007702077840,OGRN=1027739387411,CN=Корневой УЦ,O=ПАО Московская Биржа,L=Москва,ST=77 г.Москва,C=RU*

использующийся владельцем СКПЭП _____
(ФИО владельца СКПЭП)

Данный СКПЭП прошу аннулировать с "_____" _____ 202__ г.

_____
Должность, фамилия и инициалы представителя Клиента

_____
Подпись представителя Клиента

«_____» _____ 202__ г.

М.П.

Приложение № 5
к Регламенту Уполномоченного представителя Удостоверяющего центра

Тарифы на Услуги

Наименование Услуги	**Тариф[2]** (в рублях, без учета НДС)	**Тариф[2]** (в рублях, с учетом НДС)
Создание СКПЭП	3 166,67	3800,00
Предоставление права использования средств электронной подписи сроком действия 1 год [1]	1 250,00	1500,00
Итого стоимость услуги	**4 416,67**	**5300,00**

[1] Данная услуга предоставляется одновременно с услугой «Создание СКПЭП». Срок предоставления права использования Программного обеспечения (срок действия лицензии) устанавливается равным сроку действия ключа электронной подписи.

[2] С 01.04.2025 по 31.12.2025 действует маркетинговая программа, в рамках которой плата за услуги не взимается.

Приложение № 6
к Регламенту Уполномоченного представителя Удостоверяющего центра

РУКОВОДСТВО
по обеспечению безопасности использования электронной подписи и средств электронной подписи

1. Общие положения

Настоящее руководство регламентирует вопросы обеспечения безопасности при использовании усиленной неквалифицированной электронной подписи, а также соответствующих средств усиленной неквалифицированной электронной подписи, выданных Удостоверяющим центром.

Положения данного руководства распространяются, в первую очередь, на усиленную квалифицированную подпись и средства усиленной квалифицированной электронной подписи. В отношении усиленной неквалифицированной электронной подписи и средств усиленной неквалифицированной электронной подписи данное руководство может быть также применено в полном объеме, за исключением требований, которые не могут быть применены в силу отсутствия реализации указанных в настоящем руководстве возможностей в средствах усиленной неквалифицированной электронной подписи (например, возможности использования ключевых носителей).

С целью унификации, далее по тексту настоящего руководства используются обобщенные термины "электронная подпись" и "средства электронной подписи".

Помимо данного руководства, Клиент для обеспечения безопасности использования электронной подписи и средств электронной подписи должен руководствоваться требованиями эксплуатационной документации и формуляров (при их наличии) на средства электронной подписи, а также требованиями федерального органа исполнительной власти, уполномоченного в сфере использования шифровальных (криптографических) средств.

2. Требования по размещению

При размещении средств вычислительной техники с установленными на них средствами электронной подписи должны быть приняты меры по недопущению несанкционированного доступа в помещения, в которых размещены средства электронной подписи, посторонних лиц, не имеющих допуска к работе в этих помещениях. В случае необходимости присутствия посторонних лиц, в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты информации и передаваемую информацию.

Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

3. Требования по установке средств электронной подписи, общесистемного и специального программного обеспечения

3.1. При использовании средств электронной подписи должны выполняться следующие меры по защите информации от несанкционированного доступа:

3.1.1. Необходимо разработать и применять политику назначения и смены паролей (для входа в ОС, BIOS и т.д.), использовать пароли в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 символов;

- в составе пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

- пароль не должен представлять собой легко вычисляемые сочетания букв и цифр (например, имена, фамилии, наименования, общепринятые сокращения, имя учетной записи, почтовый адрес, слова из словаря, сленга, диалекта, жаргона);

- пароль не должен содержать более двух повторяющихся символов;

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- пароль должен быть изменен при первом входе в АРМ, а также регулярно меняться (один раз в квартал).

3.1.2. При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

- не использовать нестандартные, измененные или отладочные версии операционных систем;

- исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;

- исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;

- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);

- режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;

- всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для штатной работы права;

- необходимо предусмотреть меры, максимально ограничивающие доступ к:
    - системному реестру;
    - файлам и каталогам;
    - временным файлам;
    - журналам системы;
    - файлам подкачки;
    - кэшируемой информации (пароли и т.п.);
    - отладочной информации.

3.1.3. На используемых АРМ необходимо:

- исключить попадание в АРМ программ, позволяющих использовать ошибки операционной системы для повышения предоставленных привилегий;

- регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

3.1.4. В случае подключения технических средств с установленными средствами электронной подписи к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов.

3.1.5. Необходимо организовать и использовать:

- систему аудита, организовать регулярный анализ результатов аудита;

- комплекс мероприятий по антивирусной защите.

3.2. Запрещается:

- осуществлять несанкционированное копирование информации с ключевых носителей;

- разглашать содержимое информации с ключевых носителей или передавать сами ключевые носители лицам, не допущенным к данной информации, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;

- использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;

- вносить какие-либо изменения в программное обеспечение средств электронной подписи;

- записывать на ключевые носители постороннюю информацию;

- оставлять средства вычислительной техники с установленными средствами электронной подписи без контроля после ввода ключевой информации;

- удалять ключевую информацию с ключевого носителя до истечения срока действия или аннулирования сертификата ключа проверки электронной подписи.

4. Требования по обеспечению безопасности при обращении с ключевой информацией и ключевыми носителями, содержащими ключи электронной подписи

4.1. Меры защиты ключей электронной подписи.

Ключи электронной подписи при создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством электронной подписи согласно технической и эксплуатационной документации.

Ключи электронной подписи на ключевом носителе, при наличии технической возможности, должны быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей в соответствии с эксплуатационной документацией на используемое средство электронной подписи.

Ответственность за обеспечение сохранности в тайне пароля (ПИН-кода) возлагается на владельца ключа электронной подписи.

При наличии технической возможности пароль (ПИН-код) должен удовлетворять требованиям, приведенным в разделе 3 настоящего руководства.

4.2. Обращение с ключевой информацией и ключевыми носителями.

Недопустимо пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме открытых ключей).

Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами электронной подписи способствует реализации сценариев совершения мошеннических действий злоумышленниками.

Владелец ключа электронной подписи обязан сохраняться в тайне ключи электронной подписи, не передавать их третьим лицам и принимать меры для предотвращения их компрометации.

Носители ключевой информации должны использоваться только их владельцами и храниться в месте, недоступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами электронной подписи операций формирования и проверки электронной подписи, шифрования и расшифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации неуполномоченными лицами.

На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

5. Обеспечение безопасности АРМ с установленными средствами электронной подписи.

С целью контроля исходящего и входящего трафика, технические средства с установленными средствами электронной подписи должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования.

Для технических средств с установленными средствами электронной подписи должны выполняться следующие требования:

- для учетных записей пользователей операционной системы должны применяться пароли, удовлетворяющие требованиям, приведенным в разделе 3 настоящего руководства;

- должно быть установлено только лицензионное программное обеспечение;

- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных, при этом функционирование антивирусного программного обеспечения должно осуществляться в постоянном, автоматическом режиме;

- должны быть отключены все неиспользуемые службы и процессы операционной системы (в том числе, службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);

- на технических средствах не должны использоваться средства разработки и отладки программного обеспечения;

- должны регулярно устанавливаться обновления операционной системы;

- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами электронной подписи и средствами криптографической защиты информации для неуполномоченных лиц;

- должна быть активирована регистрация событий информационной безопасности;

- должна быть включена автоматическая блокировка экрана после покидания пользователем своего рабочего места.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства электронной подписи, необходимо гарантированно удалить всю информацию, использование которой неуполномоченными лицами может нанести вред Клиенту, в том числе средства электронной подписи, журналы работы систем обмена электронными документами и т.п.