

Утверждены Приказом
Генерального директора
ООО «УК Портфельные инвестиции»
(Приказ № 0509/25-01 от 05.09.2025
г., вступают в силу с 08.09.2025 г.)

**Правила доступа и использования
сервиса ООО «УК Портфельные инвестиции» -
Личный кабинет пайщика**

**г. Москва
2025 г.**

Термины и определения

Аккредитованный удостоверяющий центр (Аккредитованный УЦ) - организация, осуществляющая функции по созданию и выдаче сертификатов ключей проверки электронных подписей, получившая аккредитацию в порядке, установленном законодательством Российской Федерации.

Аутентификация - процедура, позволяющая подтвердить путём проверки Аутентификационных данных или УКЭП, что лицо, осуществляющее вход в ЛК, является Пользователем.

Аутентификационные данные – логин и пароль, а также логин и пароль, используемые Пользователем для доступа к portalу государственных услуг www.gosuslugi.ru, при условии, что Пользователь прошел процедуру удалённой идентификации в ЕСИА с подтверждённой учётной записью на portalе государственных услуг www.gosuslugi.ru и согласился с предоставлением в Личный кабинет пайщика своих данных, при этом вход в ЕСИА осуществлен через Личный кабинет пайщика.

Владелец сертификата ключа проверки электронной подписи - Пайщик, которому в установленном порядке Аккредитованным удостоверяющим центром выдан Сертификат ключа проверки электронной подписи (Квалифицированный сертификат ключа проверки электронной подписи).

ЕСИА — Единая система идентификации и аутентификации. Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации и настоящими Правилами, санкционированный доступ к информации, содержащейся в государственных и муниципальных информационных системах

Инвестиционный комитет — собрание членов инвестиционного комитета паевого инвестиционного фонда, порядок формирования которого определяется ПДУ.

Квалифицированный сертификат ключа проверки электронной подписи (Квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный Аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, и являющийся в связи с этим официальным документом.

Компрометация пароля - обстоятельства, прямо или косвенно свидетельствующие о возможности несанкционированного использования Пароля третьими лицами, или наличие у Пользователя или Управляющей компании оснований полагать, что такие обстоятельства существуют.

Компрометация ключа ЭП - утрата доверия к тому, что используемый Ключ ЭП обеспечивает безопасность информации; констатация владельцем сертификата ключа проверки электронной подписи обстоятельств, при которых возможно несанкционированное использование его ключа ЭП неуполномоченными лицами или наличие у него или Управляющей компании оснований полагать, что такие обстоятельства существуют.

Ключ электронной подписи (ключ ЭП) - уникальная последовательность символов, предназначенная для создания Усиленной квалифицированной электронной подписи в Электронном документе. К Ключам электронной подписи также относится логин и пароль, используемые Пользователем для доступа к portalу государственных услуг www.gosuslugi.ru, при условии, что Пользователь прошел процедуру удалённой идентификации в ЕСИА с подтверждённой учётной записью на portalе государственных услуг www.gosuslugi.ru и согласился с предоставлением в Личный кабинет пайщика своих данных, при этом вход в ЕСИА осуществлен через Личный кабинет

пайщика.

Ключ проверки электронной подписи (ключ проверки ЭП) - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности Усиленной квалифицированной электронной подписи.

Личный кабинет пайщика (ЛК) - информационная система ООО «УК Портфельные инвестиции», расположенная на сайте Управляющей компании в информационно-телекоммуникационной сети «Интернет», предназначенная для электронного голосования на Общем собрании или Инвестиционном комитете через информационно-телекоммуникационную сеть «Интернет». Участники системы получают право использования ЛК исключительно в целях использования функционала ЛК в соответствии с Правилами.

Доступ в ЛК осуществляется с любого компьютера или иного устройства, имеющего доступ в информационно-телекоммуникационную сеть «Интернет», с применением процедуры Аутентификации.

Логин (для юридического лица) - имя пользователя, предназначенное для Аутентификации Пользователя и осуществления им доступа к ЛК. Логин является адрес Электронной почты.

Общее собрание - общее собрание владельцев инвестиционных паев закрытого паевого инвестиционного фонда, находящегося под управлением Управляющей компании.

Пароль (для юридического лица) - комбинация символов, известная только Пользователю и служащая для Аутентификации Пользователя в ЛК и осуществления доступа к ЛК.

Пайщик - юридическое или физическое лицо - владелец инвестиционных паев паевого инвестиционного фонда, находящегося под управлением Управляющей компании.

ПДУ – правила доверительного управления паевым инвестиционным фондом, находящегося под управлением Управляющей компании.

Пользователь - Пайщик, Представитель или член инвестиционного комитета, назначенный в соответствии с ПДУ.

Правила - настоящие Правила доступа и использования сервиса ООО «УК Портфельные инвестиции» - Личный кабинет пайщика, включая все приложения и изменения к ним.

Простая электронная подпись (ПЭП) - логин и пароль, используемые Пользователем для доступа к portalу государственных услуг www.gosuslugi.ru, при условии, что Пользователь прошел процедуру удалённой идентификации в ЕСИА с подтверждённой учётной записью на portalе государственных услуг www.gosuslugi.ru и согласился с предоставлением в Личный кабинет пайщика своих данных, при этом вход в ЕСИА осуществлен через Личный кабинет пайщика; используется для определения лица, подписывающего Электронный документ, и подтверждает факт формирования электронной подписи Пайщика - физическим лицом или Представителем такого Пайщика.

Представитель - физическое лицо, имеющее полномочия (права) совершать от имени Пайщика действия, предусмотренные настоящими Правилами и правилами ПДУ. В тексте настоящих Правил во всех случаях подразумевается, что любые действия от имени Пайщика осуществляют только Пайщик или его Представитель.

Регламент удостоверяющего центра (Регламент УЦ) - документ, разработанный и утвержденный Аккредитованным УЦ, обязательный для исполнения любым лицом, вступающим во взаимоотношения с Аккредитованным УЦ по выполнению последним функций удостоверяющего центра, предусмотренных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». Регламент удостоверяющего центра размещается на сайте Аккредитованного УЦ в информационно-телекоммуникационной сети «Интернет».

Сайт Личного кабинета пайщика - сайт в сети Интернет <https://lk.ukpi.ru>, через который осуществляется использование Личного кабинета пайщика.

Сертификат ключа проверки электронной подписи (Сертификат) - электронный документ или документ на бумажном носителе, выданные Аккредитованным удостоверяющим центром и подтверждающие принадлежность ключа проверки электронной подписи Владельцу сертификата ключа проверки электронной подписи.

Сессия (период доступа) - промежуток времени в течение которого Пользователь вправе использовать функционал ЛК без повторного прохождения Аутентификации.

Средство криптографической защиты информации (СКЗИ) - шифровальное (криптографическое) средство, используемое для реализации следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи и имеющее подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ.

Сторона(ы) - Управляющая компания и Пользователь при совместном упоминании в настоящих Правилах.

Уполномоченное лицо удостоверяющего центра - физическое лицо, являющееся сотрудником Аккредитованного удостоверяющего центра и наделенное Аккредитованным удостоверяющим центром полномочиями по заверению от лица Аккредитованного удостоверяющего центра сертификатов ключей проверки подписей и списков отозванных сертификатов.

Управляющая компания - Общество с ограниченной ответственностью «Управляющая компания Портфельные инвестиции».

Усиленная квалифицированная электронная подпись (УКЭП) - электронная подпись, которая соответствует всем признакам Усиленной неквалифицированной электронной подписи и следующим дополнительным признакам:

- 1) ключ проверки электронной подписи указан в Квалифицированном сертификате;
- 2) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ.

Участники ЭДО – Управляющая компания и Пользователи, осуществляющие обмен информацией в электронной форме с использованием ЭП.

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

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию, в том числе простая электронная подпись посредством применения единой системы идентификации и аутентификации.

Электронная почта - адрес электронной почты Пользователя, сведения о котором предоставлены Управляющей компании в Заявлении о предоставлении доступа в Личный кабинет пайщика (Приложение 1 к Правилам).

Электронный документ (ЭД) - сообщение (документ), в котором информация представлена в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах, и соответствует установленному формату.

Электронный журнал - взаимосвязанный набор электронных записей, отражающих последовательность действий с ЭД в ЛК, в том числе содержащий дату, время и содержание операций, производимых в ЛК.

Иные термины и определения, специально не определенные в Правилах, используются в значениях, установленных ПДУ, Федеральным законом № 63-ФЗ, иными нормативными правовыми актами Российской Федерации.

1. Общие положения

1.1. Настоящие Правила устанавливают порядок предоставления доступа и использования Личного кабинета пайщика.

1.2. Правила публикуются на официальном сайте ООО «УК Портфельные инвестиции» в информационно-телекоммуникационной сети «Интернет» по адресу: www.ukpi.ru.

1.3. Правовое регулирование отношений в области использования Участниками ЭДО электронного документооборота осуществляется в соответствии с Гражданским кодексом Российской Федерации, Федеральным законом от 06.04.2011 № 63-ФЗ, Федеральным законом от 29.11.2001 № 156-ФЗ, Положением Банка России от 28.06.2022 N 796-П "О дополнительных требованиях к общему собранию владельцев инвестиционных паев закрытого паевого инвестиционного фонда" другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, а также Правила и ПДУ.

1.4. Доступ в Личный кабинет пайщика предоставляется Пользователю, являющемуся - физическим лицом, при выполнении следующих условий:

- у Пользователя есть право на участие в Общем собрании или Инвестиционном комитете;
- для использования в качестве Ключа электронной подписи логина и пароля для доступа к portalу государственных услуг www.gosuslugi.ru Пользователь должен на Сайте Личного кабинета пайщика нажать на кнопку «Войти через Госуслуги». В этом случае, Пользователь будет переадресован на портал государственных услуг www.gosuslugi.ru для прохождения процедуры удаленной идентификации в ЕСИА. После прохождения процедуры удаленной идентификации в ЕСИА с подтверждённой учётной записью на портале государственных услуг www.gosuslugi.ru и подтверждения согласия Пользователя с предоставлением в Личный кабинет пайщика своих данных, Пользователю предоставляется доступ в Личный кабинет пайщика.

1.5. Доступ в Личный кабинет пайщика предоставляется Пользователю, являющемуся - юридическим лицом, при выполнении следующих условий:

- у Пользователя есть право на участие в Общем собрании или Инвестиционном комитете;
- наличие у Пользователя действующего Ключа электронной подписи;
- предоставление Управляющей Компании Заявления о предоставлении доступа в Личный кабинет пайщика по форме, установленной в Приложении 1 к настоящим Правилам (Заявление о доступе).

1.6. Использование Представителями Участников ЭДО УКЭП требует одновременного предоставления машиночитаемых доверенностей, оформленных с соблюдением требований действующего законодательства Российской Федерации и предоставленных в порядке, предусмотренном ПДУ.

1.7. Настоящие Правила не являются публичным договором, публичной офертой и не обязывают Управляющую компанию предоставить доступ к Личному кабинету пайщика каждому обратившемуся лицу.

2. Функциональные возможности Личного кабинета пайщика

2.1. Функциональные возможности Личного кабинета позволяют Пользователю:

- получать доступ к сообщениям о созыве общего собрания, информации (материалам) общего собрания владельцев инвестиционных паев закрытого паевого инвестиционного фонда, отчетам об итогах проведения заочного голосования для принятия решений общим собранием владельцев инвестиционных паев и иным документам, размещенным Управляющей компанией;
- принимать участие в заочном голосовании при принятии решений общим собранием

владельцев инвестиционных паев закрытого паевого инвестиционного фонда путем заполнения и представления (направления) электронного бюллетеня и подписания его Электронной подписью.

2.2. Функциональные возможности Личного кабинета позволяют Пользователю (члену инвестиционного комитета):

- получать доступ к уведомлениям о проведении инвестиционного комитета, материалам инвестиционного комитета закрытого паевого инвестиционного фонда, протоколам инвестиционного комитета и иным документам, размещенным Управляющей компанией;
- принимать участие в заочном голосовании на инвестиционном комитете закрытого паевого инвестиционного фонда путем заполнения и представления (направления) электронного бюллетеня и подписания его Электронной подписью.

2.3. Функциональные возможности Личного кабинета позволяют Управляющей компании:

- размещать информацию о проведении заочного голосования для принятия решений общим собранием владельцев инвестиционных паев закрытого паевого инвестиционного фонда, включая материалы к общему собранию владельцев инвестиционных паев;
- размещать информацию о проведении заочного голосования на инвестиционном комитете закрытого паевого инвестиционного фонда, включая материалы к инвестиционному комитету;
- размещать электронные бюллетени для заочного голосования на общем собрании владельцев инвестиционных паев паевого инвестиционного фонда, инвестиционном комитете закрытого паевого инвестиционного фонда;
- предоставлять Пользователям, имеющим право голоса при принятии решений общим собранием владельцев инвестиционных паев закрытого паевого инвестиционного фонда, доступ к отчетам об итогах проведения заочного голосования для принятия решений общим собранием владельцев инвестиционных паев и иным документам, размещенным Управляющей компанией;
- предоставлять Пользователям (членам инвестиционного комитета) доступ к протоколам инвестиционного комитета и иным документам, размещенным Управляющей компанией.

2.4. Управляющая компания вправе в одностороннем порядке изменять перечень документов (информации), доступных Пользователю посредством ЛК.

3. Процедура получения доступа в ЛК

3.1. Для предоставления доступа в ЛК заинтересованное лицо – юридическое лицо предоставляет Управляющей компании Заявление о предоставлении доступа в Личный кабинет пайщика (Форма для юридических лиц) по форме Приложения 1 (далее – Заявление) в одном экземпляре. Заявление подается в Управляющую компанию. Заявления, направленные почтой (в том числе электронной), факсом или курьером, не принимаются.

После получения Управляющей компанией Заявления, Управляющая Компания отправляет на Электронную почту Пайщика уникальную ссылку с ограниченным сроком действия, при переходе по которой Пайщик устанавливает Пароль. Пайщик подтверждает установление Пароля Усиленной электронной подписью. Логинем является адрес Электронной почты.

3.2. С момента выполнения Пайщиком всех действий, указанных в пункте 3.1. Правил доступ в ЛК считается предоставленным.

3.3. Пайщик или Представитель - физическое лицо может самостоятельно пройти регистрацию в качестве Пользователя на странице в информационно-телекоммуникационной сети Интернет по адресу: <https://lk.ukpi.ru> (при наличии подтвержденной учетной записи в ЕСИА).

При этом физическое лицо для получения доступа в ЛК обязано:

- пройти процедуру удаленной идентификации через Единый портал государственных и муниципальных услуг www.gosuslugi.ru (посредством ЕСИА);
- дать согласие на передачу Управляющей компании своих персональных данных из ЕСИА.

3.4. Полномочия Представителя при получении доступа в ЛК должны быть подтверждены надлежащим образом выданной доверенностью в соответствии с требованиями, предусмотренными ПДУ. Оригинал вышеуказанной доверенности должен быть предоставлен в Управляющую компанию до начала использования ЛК.

3.5. Представитель для осуществления действий от имени Пайщика в ЛК не вправе использовать

Аутентификационные данные Пайщика.

3.6. Пользователь обязуется обеспечить хранение своих Аутентификационных данных способом, обеспечивающим их недоступность для третьих лиц, а также немедленно уведомлять Управляющую компанию о подозрении, что Аутентификационные данные могут быть известны и/или использованы третьими лицами. В случае Компрометации пароля или при подозрении на Компрометацию пароля Пользователь обязуется незамедлительно установить новый Пароль и сообщить об этом Управляющей компании.

3.7. Участники ЭДО признают и подтверждают, что:

- Успешная Аутентификация Пользователя на основании Логина и Пароля, а также ввода и отправки ключа Усиленной квалифицированной электронной подписи являются достоверными и достаточными доказательствами входа Пользователя в ЛК;
- Успешная Аутентификация Пользователя на основании результата прохождения Пользователем процедуры удалённой идентификации в ЕСИА с подтверждённой учётной записью на портале государственных услуг www.gosuslugi.ru является достоверным и достаточным доказательством входа Пользователя в ЛК;
- выписки из электронных журналов (журнал операций, реестр электронных подписей и иные), лог-файлов, электронных баз данных, данные почтовых серверов, копии отправленных электронных писем, протоколов соединений, архивов Электронных документов и других документов, подписанные Управляющей компанией и/или предоставленные в компетентные органы в электронном виде, являются достоверными и достаточными доказательствами для предъявления при разрешении конфликтных ситуаций и/или споров в досудебном порядке и/или в суде, подтверждающими дату, время Авторизации Пользователя в ЛК, факт и время подписания Электронных документов с использованием ЭП, доказательством содержания Электронных документов, а также доказательством иных фактов, имеющих значение в связи с исполнением Правил.

3.8. Максимальное время Сессии (периода доступа) в ЛК устанавливается Управляющей компанией.

3.9. Плата за подключение Пользователей (предоставление доступа) к ЛК не взимается.

4. Аккредитованный удостоверяющий центр и сертификаты (квалифицированные сертификаты) ключей проверки Усиленной квалифицированной электронной подписи

4.1. При организации и функционировании электронного документооборота ЛК применяются: квалифицированные сертификаты ключа проверки электронной подписи. Квалифицированный сертификат подлежит созданию с использованием средств аккредитованного удостоверяющего центра.

4.2. Квалифицированный сертификат признается изданным Аккредитованным удостоверяющим центром, если подтверждена подлинность электронной подписи этого сертификата, сделанной Уполномоченным лицом удостоверяющего центра.

4.3. Порядок регистрации Представителей, изготовления квалифицированных сертификатов, замены ключей, отзыва квалифицированных сертификатов устанавливается в соответствующих документах Аккредитованного УЦ, являющихся обязательными для Участников ЭДО.

4.4. Сертификат ключа проверки электронной подписи считается аннулированным (отозванным) с момента публикации Аккредитованным удостоверяющим центром списка отозванных сертификатов, в котором содержится серийный номер данного сертификата.

4.5. В случае аннулирования или досрочного прекращения действия квалифицированного сертификата, выданного аккредитованному удостоверяющему центру, выдавшему квалифицированный сертификат заявителю, либо в случае досрочного прекращения или истечения срока аккредитации удостоверяющего центра квалифицированный сертификат, выданный аккредитованным удостоверяющим центром заявителю, прекращает свое действие.

4.6. Владелец квалифицированного сертификата обязан не использовать ключ электронной подписи и немедленно обратиться в аккредитованный удостоверяющий центр, выдавший квалифицированный сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена.

5. Порядок проверки электронной подписи, условия равнозначности электронной подписи собственноручной

- 5.1. Все документы в ЛК подписываются Электронными подписями Пользователей или Представителей.
- 5.2. Перед подписанием Электронного документа Пользователь обязан ознакомиться с ним и быть согласным с его содержанием в полном объеме. Пользователь не вправе предъявлять претензии к содержанию Электронного документа после его подписания Электронной подписью.
- 5.3. При подписании Электронных документов Участники ЭДО используют ПЭП или УКЭП. При этом ПЭП вправе использовать только Пользователи - физические лица или их Представители.
- 5.4. Для проверки Усиленной квалифицированной электронной подписи в ЛК используется СКЗИ, имеющее сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности.
- 5.5. Ключ Усиленной квалифицированной электронной подписи действует на определенный момент времени, если Квалифицированный сертификат, соответствующий данному ключу ЭП, действует на данный момент времени, срок действия ключа не истек, наступил момент времени начала действия ключа.
- 5.6. Квалифицированный сертификат действует на определенный период времени, если наступил момент начала его действия; не истек срок его действия; он не аннулирован (не отозван); подтверждена подлинность (корректность) Электронной подписи Уполномоченного лица удостоверяющего центра в данном Сертификате/Квалифицированном сертификате.
- 5.7. Квалифицированный сертификат считается аннулированным (отозванным) с момента публикации Аккредитованным УЦ списка отозванных сертификатов, в котором содержится серийный номер данного Сертификата/Квалифицированного сертификата.
- 5.8. Усиленная квалифицированная электронная подпись считается корректной, если:
- получен положительный результат проверки Средством криптографической защиты информации с использованием Квалифицированного сертификата принадлежности Электронной подписи в Электронном документе Владельцу сертификата ключа проверки электронной подписи и отсутствия искажений в подписанном данной Электронной подписью Электронном документе;
 - ключ ЭП действителен на момент проверки ЭП.
- 5.9. Момент времени подписи определяется из штампа времени электронной подписи.
- 5.10. Электронные документы, подписанные ПЭП, являются документами (доказательством) при рассмотрении спорных ситуаций, в том числе в суде.
- 5.11. Определение лица, подписавшего Электронный документ ПЭП, при авторизации посредством ЕСИА, осуществляется в соответствии с данными о Пользователе, полученными из ЕСИА.
- 5.12. Пользователь, подписавший ЭД ПЭП считается определенным (идентифицированным), в случае если одновременно выполняются следующие условия:
- установлен факт входа под Логинем Пользователя в ЛК, предшествующий подписанию Электронного документа в ЛК;
 - установлен факт подписания Электронного документа.
- 5.13. Факт подписания в ЛК Электронного документа, подписанного ЭП Пользователя и иные действия Управляющей компании и Пользователя фиксируются в электронных журналах. Электронные журналы могут быть использованы в качестве доказательств при разрешении споров.
- 5.14. Участники ЭДО, до начала обмена ЭД в ЛК, признают и подтверждают, что используемые при обмене Электронными документами в рамках Правил методы обеспечения Аутентификации Участников ЭДО, конфиденциальности и целостности сообщений являются достаточными для обеспечения надежной, эффективной и безопасной работы и защиты от несанкционированного доступа, а также подтверждения авторства и подлинности Электронных документов.
- 5.15. Все Электронные документы, направленные Участниками ЭДО, подписанные корректной Электронной подписью, являются подлинными и целостными документами, исходящими от соответствующего Участника ЭДО, и являются основанием для совершения юридически значимых действий.
- 5.16. Все Электронные документы, подписанные корректной электронной подписью (в том числе ПЭП) имеют ту же юридическую силу, что и идентичные по смыслу и содержанию документы на бумажном носителе, подписанные собственноручной подписью Участника ЭДО или его Представителя.

5.17. Если в соответствии с законодательством Российской Федерации либо условиями ПДУ документ должен быть заверен печатью, Электронный документ, направленный Участником ЭДО, подписанный электронной подписью и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью.

6. Права и обязанности Участников ЭДО

6.1. Управляющая компания имеет право:

6.1.1. В любое время изменять сервисы ЛК, программное обеспечение, дизайн, содержание, как с уведомлением Пользователя, так и без такового.

6.1.2. В одностороннем порядке ограничить доступ к ЛК, все или часть операций или функциональных возможностей ЛК без объяснения причин такого ограничения.

6.1.3. Отказать в приеме Электронных документов, если есть основания считать, что такие документы отправлены от имени Пользователя другим лицом, не имеющим соответствующих полномочий от Пайщика, в том числе злоумышленником.

6.1.4. Отказать в доступе к ЛК в случае получения сообщения от Пользователя о Компрометации ключа ЭП, или Компрометации пароля.

6.2. Управляющая компания обязуется:

6.2.1. Консультировать Пользователя по вопросам функционирования ЛК, приема-передачи Электронных документов, информации и технологий их обработки в рамках технической поддержки приема/передачи Электронных документов посредством ЛК.

6.2.2. Осуществлять прием Электронных документов Пользователя согласно условиям организации и проведения электронного документооборота, установленного Правилами.

6.2.3. Поддерживать в работоспособном состоянии оборудование и программное обеспечение, предназначенное для предоставления Пользователям доступа в Личный кабинет пайщика.

6.3. Пользователь имеет право:

6.3.1. Получать консультации по вопросам функционирования ЛК, приема-передачи Электронных документов, информации и технологий их обработки в рамках технической поддержки приема/передачи Электронных документов посредством ЛК.

6.3.2. Осуществлять подписание Электронных документов согласно порядку, установленному Правилами.

6.3.3. Получать доступ к уведомлениям, информации (материалам) для проведения общего собрания, предоставляемым лицам, включенным в список лиц, имеющих право на участие в общем собрании.

6.3.4. Получать доступ к уведомлениям, информации (материалам) для проведения инвестиционного комитета, предоставляемым лицам, включенным в список лиц, имеющих право на участие в инвестиционном комитете.

6.4. Пользователь обязан:

6.4.1. Эксплуатировать средства Электронной подписи в соответствии с правилами их использования.

6.4.2. Обеспечивать (соблюдать) конфиденциальность Ключей электронной подписи.

6.4.3. Обеспечить установку и функционирование на рабочем месте Пользователя Средства криптографической защиты информации.

6.4.4. Прикладывать наилучшие усилия для недопущения несанкционированного использования Электронной подписи.

6.4.5. Уведомить Аккредитованный удостоверяющий центр, выдавший квалифицированный сертификат ключа проверки электронной подписи, и Управляющую компанию о нарушении конфиденциальности Ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении, за исключением случаев использования ПЭП.

6.4.6. Не использовать ключ УКЭП в случае Компрометации ключа ЭП.

6.4.7. Соблюдать условия организации и проведения электронного документооборота, установленные Правилами.

6.4.8. Не разглашать третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации, конкретные способы защиты информации, реализованные в ЛК.

6.4.9. Немедленно уведомлять Управляющую компанию о Компрометации пароля или Компрометации ключа ЭП.

6.4.10. Соблюдать Рекомендации по безопасному использованию ЛК приведенные в Приложении 2 к настоящим Правилам (далее - Рекомендации).

6.5. Участники ЭДО совместно обязуются:

6.5.1. Не предпринимать действий, способных нанести ущерб другой стороне электронного документооборота вследствие использования ЛК.

6.5.2. Незамедлительно уведомить другую сторону электронного документооборота в случае обнаружения возможных угроз безопасности обмена Электронными документами посредством ЛК, для принятия мер по защите.

7. Порядок обмена электронными документами

7.1. Если специально не указано иное, в каждом случае указания времени в тексте Правил приведены ссылки на московское время.

7.2. Датой получения Пользователем от Управляющей компании документов и информации, сформированных в электронном виде с помощью ЛК, является дата размещения Управляющей компании документов и информации в ЛК.

7.3. Подписание в ЛК Электронных документов Пользователем допускается в сроки, установленные ПДУ при условии, что проверка на подлинность ЭП дала положительный результат.

7.4. Пользователь уведомляется об отказе в подписании документов в форме Электронного документа путем изменения статуса Электронного документа в ЛК с указанием причины.

7.5. Ни один из Участников ЭДО, ни какие-либо третьи лица не имеют возможность вносить изменения в ЭД, хранящийся в ЛК.

8. Ответственность. Разрешение споров

8.1. Стороны несут ответственность за неисполнение или ненадлежащее исполнение требований и условий настоящих Правил в порядке, предусмотренном законодательством Российской Федерации.

8.2. Управляющая компания не несет ответственность за любые последствия использования Личного кабинета третьими лицами, возникшие, в том числе, вследствие компрометации Пароля Пользователя, несвоевременного уведомления Пользователем Управляющей компании о компрометации Пароля. Пользователь самостоятельно несет ответственность за безопасность и сохранность своего Пароля от ЛК.

8.3. Пользователь самостоятельно несет полную ответственность за сохранность и конфиденциальность Ключа электронной подписи и его использование.

8.4. Управляющая компания не несет ответственность за убытки, возникшие у Пользователя вследствие поломки, сбоев в работе, несанкционированного доступа, взлома, копирования, уничтожения и иных подобных событий, произошедших в отношении техники, устройств, носителей информации на стороне Пользователя.

8.5. Сторона не несет ответственность за любые последствия, возникшие в результате сбоев в работе каналов связи, и (или) оборудования, и (или) программного обеспечения другой Стороны, предназначенные для доступа и использования Личного кабинета.

8.6. В связи с осуществлением электронного документооборота между Участниками ЭДО возможно возникновение конфликтных ситуаций, связанных с получением, подписанием, подтверждением получения Электронных документов, а также использованием в данных документах электронной подписи.

Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

- оспаривание факта идентификации владельца сертификата Ключа проверки электронной подписи, подписавшего документ;
- заявление Участника ЭДО об искажении Электронного документа;
- оспаривание факта подписания Электронного документа;
- оспаривание времени подписания Электронного документа;
- иные случаи возникновения конфликтных ситуаций, связанных с функционированием ЛК.

8.7. В случае возникновения конфликтной ситуации Сторона, предполагающая возникновение конфликтной ситуации, должна незамедлительно, но не позднее 5 (пяти) рабочих дней после возникновения конфликтной ситуации направить уведомление о конфликтной ситуации второй Стороне.

Уведомление о конфликтной ситуации должно содержать информацию о существовании конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии конфликтной ситуации, а также в нем должны быть указаны фамилия, имя и отчество, должность, контактные телефоны, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации, с предоставлением (в случае отсутствия ранее данного этим лицом) согласия на обработку персональных данных.

8.8. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от Стороны, которой было направлено уведомление.

8.9. В случае, если конфликтная ситуация не урегулирована в рабочем порядке, и Сторона считает, что ее права при осуществлении электронного документооборота в рамках ЛК были нарушены, она обязана направить Стороне, которая, по его мнению, нарушила его права, претензию.

Претензия должна содержать:

- изложение существа требований Стороны;
- изложение обстоятельств, на которых основываются требования Стороны, и доказательства, подтверждающие их, со ссылкой на нормы законодательства;
- иные документы, имеющие значение, по мнению заявителя претензии;
- перечень прилагаемых к претензии документов и других доказательств, а также иные сведения, необходимые для урегулирования разногласий по претензии.

8.10. Порядок направления претензии, а также последующего судебного урегулирования споров осуществляется в порядке, размещенном на официальном сайте Управляющей компании в информационно-телекоммуникационной сети «Интернет» по адресу: www.ukpi.ru, в разделе - Информация для получателей финансовых услуг, обращения (жалобы).

9. Заключительные положения

9.1. Внесение изменений и/или дополнений в Правила производится Управляющей компанией в одностороннем порядке. Внесение изменений и/или дополнений в Правила осуществляется путём утверждения новой редакции Правил. Изменения и дополнения, вносимые в Правила, вступают в силу и становятся обязательными для всех Участников ЭДО в дату, определенную при их утверждении, если иное не предусмотрено Правилами.

Указанные изменения и/или дополнения доводятся до сведения Пользователя путем публикации сообщения на официальном сайте Управляющей компании не позднее чем за один день до даты их вступления в силу, если иное не предусмотрено настоящими Правилами.

При внесении в Условия изменений и/или дополнений Управляющий вправе установить иную дату вступления их в силу, чем указано в абзаце первом настоящего пункта. В этом случае одновременно с указанными изменениями и/или дополнениями на Сайте Управляющего размещается информация о дате их вступления в силу.

9.2. Стороны не вправе передавать права и обязанности, связанные с исполнением настоящих Правил, третьим лицам.

9.3. В случае принятия нормативного правового акта, устанавливающего иные обязательные правила для Участников ЭДО, чем предусмотренные Правилами, Правила применяются в части, не противоречащей указанным нормативным правовым актам.

9.4. Пользователь принимает на себя обязательство регулярно обращаться к официальному сайту Управляющей компании в целях ознакомления с возможными изменениями и/или дополнениями Правил, и несет все риски в полном объеме, связанные с неисполнением или ненадлежащим исполнением указанной обязанности.

9.5. Во всем остальном, что не предусмотрено Правилами, Стороны руководствуются действующим законодательством Российской Федерации.

ПРИЛОЖЕНИЯ:

Приложение 1: Заявление о предоставлении доступа в Личный кабинет пайщика (Форма для юридических лиц).

Приложение 2: Рекомендации по безопасному использованию Личного кабинета пайщика.

Форма для юридических лиц

ЗАЯВЛЕНИЕ
о предоставлении доступа в Личный кабинет пайщика

«__» _____ 20__ г.

Пайщик:

Полное наименование: _____

ОГРН: _____

ИНН: _____

адрес: _____

в лице: _____

просит ООО «УК Портфельные инвестиции» предоставить доступ в Личный кабинет пайщика в качестве Пользователя.

Е-mail (будет использоваться в качестве Логина): _____

1. Для проверки и использования в ЛК Вашей подписи нужно отправить ЭЦП (открытый ключ) на адрес info@ukpi.ru , ключ должен быть в архиве.
2. Пользователь ознакомлен с условиями Правил доступа и использования сервиса ООО «УК Портфельные инвестиции» - Личный кабинет пайщика, принимает условия данных правил и обязуется их выполнять.

(должность руководителя)

(инициалы, фамилия)

(подпись) М.П

Рекомендации по безопасному использованию ЛК.

1. Обеспечьте защиту устройства, с которого вы пользуетесь услугами ЛК, к таким мерам включая, но не ограничиваясь могут быть отнесены:

- Использование только лицензированного программного обеспечения, полученного из доверенных источников.
- Запрет на установку программ из непроверенных источников.
- Наличие средства защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран, защита накопителя.
- Настройка прав доступа к устройству с целью предотвращения несанкционированного доступа.
- Хранение, использование устройства с целью избежать рисков кражи и/или утери.
- Своевременные обновления операционной системы.
- Активация парольной или иной защиты для доступа к устройству.
- В случае обнаружения злонамеренного программного обеспечения на компьютере после его удаления незамедлительно смените логин и пароль.
- Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины.

2. Обеспечьте конфиденциальность:

- Храните в тайне аутентификационные/идентификационные данные и ключевую информацию: пароли, закрытые ключи, сертификаты, а в случае компрометации немедленно примите меры для смены и/или блокировки.
- Соблюдайте принцип разумного раскрытия информации о номерах счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVC кодах, в случае если у вас запрашивают указанную информацию, в привязке к сервисам Управляющей компании по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон Управляющей компании.

3. Проявляйте осторожность и предусмотрительность:

- Будьте осторожны при получении писем со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносным кодом. Вредоносный код, попав к Вам через почту или интернет ссылку на сайт, может получить доступ к любым данным и информационным системам на вашем устройстве.
- Внимательно проверяйте адресата, от которого пришло письмо. Входящее письмо может быть от злоумышленника, который маскируется под Управляющую компанию или иных доверенных лиц. Это можно сделать, проверив доменное имя или позвонив по телефону вашего контактного лица или лица, указанного на официальном сайте.
- Будьте осторожны при просмотре/работе с интернет сайтами, так как вредоносный код может быть загружен с сайта.
- Будьте осторожны с файлами в архиве с паролем, так как в таком файле может быть вредоносный код.
- Не заходите в системы удаленного доступа с недоверенных устройств, которые вы не контролируете. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию.
- Анализируйте информацию в прессе и иных общедоступных специализированных источниках о последних известных критичных уязвимостях и вредоносных кодах.
- Важно учесть, что от лица Управляющей компании не могут поступать звонки или сообщения, в которых от Вас требуют передать СМС-код, пароль, номер карты, кодовое

слово и т. д.

- Имейте в виду, что если Вы передаете ваш телефон и/или устройство другим пользователям, они могут установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам Управляющей компании, которыми пользовались Вы.
- При подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Управляющую компанию, в отношении ключевой информации, если это уместно для Вашей услуги — отозвать скомпрометированный закрытый ключ, в соответствии с правилами, отраженными в договорных и/или процедурных документах.
- Помните, что наличие резервной копии может облегчить и ускорить восстановление Вашего устройства.
- Лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у Вас.
- Регулярно выполняйте резервное копирование важной информации.
- Поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.

4. При работе с ключами электронной подписи необходимо:

- В случае хранения секретных ключей электронной подписи на внешнем ключевом носителе крайне внимательно относиться к внешнему ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они не используются для работы.
- Использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи, не хранить пароли в текстовых документах на компьютере.

5. При работе на компьютере необходимо:

- Использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и т. д.).
- Своевременно устанавливать актуальные обновления безопасности (операционные системы, офисные пакеты и т. д.).
- Использовать антивирусное программное обеспечение, регулярно обновлять антивирусные базы.
- Использовать специализированные программы для защиты информации (персональные межсетевые экраны и средства защиты от несанкционированного доступа), средства контроля конфигурации устройств.
- Использовать сложные пароли.
- Ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

6. При работе с мобильным устройством необходимо:

- Не оставлять свое мобильное устройство без присмотра, чтобы исключить несанкционированное использование.
- Использовать только официальные мобильные приложения.
- Не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в SMS-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Управляющей компании.
- Установить на мобильном устройстве пароль для доступа к устройству.

7. При обмене информацией через сеть Интернет необходимо:

- Не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам.

- Не вводить персональную информацию на подозрительных сайтах и других неизвестных Вам ресурсах.
- Ограничить посещения сайтов сомнительного содержания.
- Не сохранять пароли в памяти интернет-браузера, если к компьютеру есть доступ третьих лиц.
- Не нажимать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет.
- Открывать файлы только известных Вам расширений (docx, png, xlsx и т. д.).