Утвержден
Приказом Генерального директора
АО «ДК РЕГИОН»
№ ДК-17/2ИН от 30 марта 2023г.

Регламент
Электронного документооборота
Системы «Личный кабинет пайщика»
АО «ДК РЕГИОН»

Москва
2023

Термины и определения

ЭДО – электронный документооборот.

Участники – Участниками электронного документооборота являются: Акционерное общество «Депозитарная компания РЕГИОН» (АО «ДК РЕГИОН») и Зарегистрированные лица, присоединившиеся к настоящему регламенту.

Организатор ЭДО – АО «ДК РЕГИОН»**.**

Аккредитованный удостоверяющий центр (УЦ) - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, получившие аккредитацию (признание соответствующим требованиям Федерального закона от 06.04.2011 N 63-ФЗ "Об электронной подписи"), а также удостоверяющий центр федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, удостоверяющий центр федерального органа исполнительной власти, уполномоченного на правоприменительные функции по обеспечению исполнения федерального бюджета, казначейскому обслуживанию исполнения бюджетов бюджетной системы Российской Федерации, и удостоверяющий центр Центрального банка Российской Федерации.

Подлинность электронной подписи в электронном документе – положительный результат проверки средством электронной подписи с использованием сертификата ключа проверки подписи принадлежности электронной подписи в электронном документе владельцу сертификата ключа проверки подписи и отсутствия искажений в подписанном данной электронной подписью электронном документе.

Список отозванных сертификатов – электронный документ, подписанный электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей проверки подписей, которые на момент времени формирования списка отозванных сертификатов были отозваны или действие которых было приостановлено. Момент времени формирования списка отозванных сертификатов определяется по значению поля ThisUpdate списка отозванных сертификатов.

Средство криптографической защиты информации (СКЗИ) - шифровальное (криптографическое) средство, используемое для реализации следующих функций - создание 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 «Об электронной подписи»

Электронный документ (ЭД) – информация, представленная в электронной форме, представляющая собой совокупность структурированных данных, имеющих смысл для Участников и позволяющая обеспечить ее обработку программным и аппаратным обеспечением ЭДО.

Электронный журнал – взаимосвязанный набор электронных записей, отражающих последовательность действий с ЭД в Системе по приему, обработке и отправке ЭД, в том числе содержащий дату, время и содержание операций, производимых в системе.

Система «Личный кабинет пайщика» (ЛКП) – корпоративная информационная система АО «ДК РЕГИОН», предназначенная для удаленного взаимодействия с Зарегистрированным лицом обеспечивающая, защиту, прием, передачу электронных документов с использованием сети «Интернет», доступная по адресу: https://lk.region-dk.ru/shareholder.

Зарегистрированное лицо (пайщик) - лицо (физическое лицо, юридическое лицо и др., за исключением номинального держателя, номинального держателя центрального депозитария), которому открыт лицевой счет в реестре владельцев инвестиционных паев паевого инвестиционного фонда, ведение которого осуществляет АО «ДК РЕГИОН».

1. Общие положения

1.1. Настоящий Регламент электронного документооборота (далее – «Регламент») определяет порядок получения доступа к ЛКП, порядок получения Зарегистрированными лицами документов, предоставляемых АО «ДК РЕГИОН» посредством их размещения в ЛКП при осуществлении деятельности по ведению реестра владельцев инвестиционных паев паевых инвестиционных фондов в соответствии с Правилами ведения реестра владельцев инвестиционных паев паевых инвестиционных фондов специализированного депозитария Акционерного общества «Депозитарная компания «РЕГИОН» (далее – Правила).

1.2. Настоящий Регламент публикуется на сайте АО «ДК РЕГИОН» http://region-dk.ru.

1.3. Правовое регулирование отношений в области использования ЭДО осуществляется в соответствии с Гражданским кодексом Российской Федерации, Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи», другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, а также настоящим Регламентом и заключенными между Участниками соглашениями.

1.4. Настоящий Регламент является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

1.5. Факт присоединения к Регламенту является полным принятием условий настоящего Регламента и всех его приложений в редакции, действующей на момент регистрации Заявления о присоединении.

1.6. Внесение изменений и/или дополнений в Регламент производится АО «ДК РЕГИОН» в одностороннем порядке. Внесение изменений и/или дополнений в Регламент осуществляется в форме новой редакции. Изменения и дополнения, вносимые в Регламент, вступают в силу и становятся обязательными для всех участников в дату, определенную при их утверждении.

1.7. Уведомление остальных Участников о внесении изменений и/или дополнений в Регламент осуществляется путем публикации сообщения на сайте АО «ДК РЕГИОН» не позднее 1 (Одного) рабочего дня до даты их вступления в силу.

2. Получение доступа к ЛКК.

2.1. Зарегистрированное лицо может получить доступ к ЛКК при условии присоединения к настоящему Регламенту.

2.2. Присоединение к настоящему Регламенту осуществляется путем подписания и предоставления в АО «ДК РЕГИОН» Заявления о присоединении к Регламенту по форме Приложения №1 настоящего Регламента.

2.3. Получение Зарегистрированным лицом индивидуального логина и пароля к своему личному кабинету осуществляется в офисе по адресу в пределах места нахождения АО «ДК РЕГИОН» при личном присутствии Зарегистрированного лица, являющегося физическим лицом и при личном присутствии уполномоченного представителя Зарегистрированного лица, являющегося юридическим лицом.

Логин и пароль выдаются при предъявлении подлинника документа, удостоверяющего личность Зарегистрированного физического лица, уполномоченного представителя Зарегистрированного юридического лица, а также подлинника или надлежащим образом заверенной копии доверенности представителя Зарегистрированного юридического лица, действующего на основании доверенности.

3. Порядок предоставления документов в ЛКК.

3.1. Перечень электронных документов, предоставляемых АО «ДК РЕГИОН» посредством размещения в ЛКП приведены в Правилах ведения реестра владельцев инвестиционных паев специализированного депозитария Акционерное общество «Депозитарная компания «РЕГИОН»,

3.2. АО «ДК РЕГИОН» подготавливает электронные документы для отправки Зарегистрированному лицу посредством размещения в ЛКП в электронном виде в формате PDF.

3.3. Подготовленные электронные документа АО «ДК РЕГИОН» регистрирует средствами собственной системы регистрации в соответствии с правилами регистрации исходящей корреспонденции.
3.4. Зарегистрированные электронные документы подписываются электронной подписью уполномоченного представителя АО «ДК РЕГИОН».
3.5. Датой получения Зарегистрированным лицом от АО «ДК РЕГИОН» документов и информации, сформированных в электронном виде с помощью ЛКП, является дата размещения АО «ДК РЕГИОН» документов и информации в ЛКП.
3.6. Электронный документ можно скачать в формате PDF.
3.7. Ни один из Участников, ни какие-либо третьи лица не имеют возможность вносить изменения в ЭД, хранящийся в ЛКП.

4. Порядок формирования и проверки электронной подписи АО «ДК РЕГИОН».

4.1. Все документы в Системе «Личный кабинет пайщика», размещаемые АО «ДК РЕГИОН» подписываются электронными подписями уполномоченного представителя АО «ДК РЕГИОН».
4.2. При подписании электронных документов используется квалифицированная усиленная электронная подпись с поддержкой штампов времени.
4.3. Понятие и признаки квалифицированной электронной подписи определены Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи».
4.4. Для формирования электронной подписи в ЛКП используется сертифицированное ФСБ России СКЗИ.
4.5. Формирование электронной подписи электронного документа может быть осуществлено только уполномоченным представителем АО «ДК РЕГИОН» - владельцем сертификата ключа проверки подписи, ключ электронной подписи которого действует на момент формирования электронной подписи электронного документа.
4.6. Ключ электронной подписи действует на определенный момент времени (действующий ключ), если:
- наступил момент времени начала действия ключа;
- срок действия ключа не истек;
- сертификат ключа проверки подписи, соответствующий данному ключу действует на данный момент времени.
4.7. Сертификат ключа проверки подписи действует (действующий сертификат) на определенный период времени, характеризующийся:
- наступлением момента времени начала его действия;
- не истекшим сроком его действия;
- тем, что он не аннулирован (отозван) и действие его не приостановлено;
- подтверждением подлинности (корректности) электронной подписи Уполномоченного лица удостоверяющего центра в данном сертификате.
4.8. Сертификат ключа проверки электронной подписи считается аннулированным (отозванным) с момента публикации УЦ списка отозванных сертификатов, в котором содержится серийный номер данного сертификата.
4.9. Размещенные в ЛКП электронные документы, подписанные корректной ЭП, имеют равную юридическую силу с документами на бумажном носителе, подписанными и скрепленными оттисками печатей.
4.10. Электронная подпись считается корректной, если получен положительный результат проверки подписи.
4.11. Результат проверки ЭП считается положительным, если:
- подтверждена Подлинность электронной подписи документа
- ключ электронной подписи действителен на момент подписи
4.12. Момент времени подписи определяется из штампа времени электронной подписи

5. Права и Обязанности Участников электронного взаимодействия

5.1. АО «ДК РЕГИОН» имеет право:
5.1.1. В любое время проводить профилактические и иные работы в ЛКП, прекращая доступ Зарегистрированных лиц к данной системе с предварительным уведомление

Зарегистрированного лица путем размещения информации на сайте по адресу: https://lk.region-dk.ru/shareholder

5.1.2. В любое время изменять сервисы ЛКП, программное обеспечение, дизайн, содержание, как с уведомлением Зарегистрированного лица, так и без такового.

5.2. АО «ДК РЕГИОН» обязуется:

5.2.1. Консультировать Зарегистрированное лицо по вопросам функционирования ЛКП, получения ЭД.

5.2.2. Вести электронный журнал, обеспечивать его целостность, а также защиту информации, содержащейся в Электронном журнале, и хранить его не менее 5 (пяти) лет после прекращения настоящего Регламента.

5.2.3. Прекращать доступ Зарегистрированного лица к ЛКП на основании его письменного заявления, поданного в АО «ДК РЕГИОН».

5.2.4. Принимать меры по защите и обеспечению целостности информации, находящейся в Электронном журнале.

5.3. Зарегистрированное лицо имеет право:

5.3.1. Получать консультации по вопросам функционирования ЛКП, получения ЭД.

5.3.2. Требовать предоставление информации о причинах отсутствия ЭД в ЛКП.

5.4. Зарегистрированное лицо обязано:

5.4.1. Не разглашать третьим лицам, за исключением случаев, предусмотренных законодательством конкретные способы защиты информации, реализованные в ЛКП.

5.4.2. Выполнять требования к программно-техническим средствам.

5.4.3. Ознакомиться с уведомлением о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц, являющимся Приложением №2 к настоящему Регламенту.

5.5. Участники совместно обязуются:

5.5.1. Не предпринимать действий, способных нанести ущерб другой Стороне вследствие использования ЛКП.

5.5.2. Незамедлительно уведомить другую Сторону в случае обнаружения возможных угроз безопасности получения ЭД посредством ЛКП, для принятия мер по защите.

6. Учет и хранение электронных документов

6.1. Ответственным за учет и хранение электронных документов является уполномоченный представитель Организатора ЭДО.

6.2. Все документы, переданные с использованием ЛКП, а также соответствующие им по времени использования все сертификаты ключей проверки ЭП должны храниться в течение сроков, предусмотренных действующими нормативными правовыми актами Российской Федерации для хранения соответствующих документов. При этом должны обеспечиваться:

- доступ к электронным документам, информации о датах и времени их получения (отправки), адресатах, а также возможность поиска документов по их реквизитам;
- резервное копирование электронных документов осуществляется Организатором ЭДО в соответствии с его внутренним регламентом;
- архивное хранение электронных документов, их реквизитов, включая информацию о датах и времени получения (отправки) и адресатах осуществляется уполномоченными представителями Участников с использованием компонентов ЭДО;

6.3. Электронные документы должны храниться в архивах электронных документов обеих сторон в том же формате, в котором они были отправлены или получены.

6.4. Каждая из сторон самостоятельно обеспечивает защиту собственных архивов электронных документов от несанкционированного доступа, изменения, уничтожения.

7. Разрешение споров

7.1. Все споры, разногласия, требования, возникающие из настоящего Регламента или касающиеся его нарушения, прекращения недействительности подлежат путем переговоров.

7.2. В случае невозможности разрешения разногласий путем переговоров, споры разрешаются в Арбитражном суде г. Москвы в порядке, установленном действующим законодательством РФ, с обязательным соблюдением досудебного претензионного порядка.
7.3. Претензия оформляется в письменном виде и направляется заказным письмом с уведомлением, с приложением копий документов подтверждающих обоснование заявленной претензии.
7.4. Срок ответа на претензию устанавливается в 15 (пятнадцать) дней с момента ее получения.

8. Обстоятельства непреодолимой силы (Форс-мажор)

8.1. АО «ДК РЕГИОН» не несет ответственность в случае невыполнения, несвоевременного или ненадлежащего выполнения какого-либо из обязательств настоящего Регламента, если это обусловлено исключительно наступлением и/или действием обстоятельств непреодолимой силы (форс-мажор).
8.2. К обстоятельствам непреодолимой силы относятся: военные действия, стихийные бедствия, пожары, забастовки, массовые беспорядки, изменения гражданского или налогового законодательства, изменение или введение новых нормативных актов, существенно ухудшающих условия выполнения настоящего Регламента или делающих невозможным выполнение настоящего Регламента полностью или частично.

9. Ответственность сторон за несоблюдение настоящего Регламента

9.1. За несоблюдение настоящего Регламента Участники несут имущественную ответственность в соответствии с действующим законодательством Российской Федерации.
9.2. Участники не несут ответственности за любые убытки других Участников, не связанные с нарушением сторонами своих обязательств по настоящему Регламенту.

10. Заключительные положения

10.1. Все изменения, дополнения и приложения к настоящему Регламенту, оформленные надлежащим образом, являются его неотъемлемой частью.
10.2. Участники не вправе передавать права и обязанности, связанные с исполнением настоящего Регламента, третьим лицам.
10.3. Во всем остальном, что не предусмотрено настоящим Регламентом, Участники руководствуются действующим законодательством РФ.
10.4. Начало действия настоящего Регламента 01.04.2023 г.

Приложение № 1
К Регламенту электронного документооборота
Системы «Личный кабинет пайщика»

Заявление о присоединении

Сведения о заявителе – Участнике ЭДО			
Полное наименование/ФИО			
ОГРН/наименование и реквизиты документа, удостоверяющего личность			
ИНН (для юридического лица)		КПП (для юридического лица)	
Место нахождения/адрес регистрации по месту жительства или пребывания			
Почтовый адрес (для юридических лиц)			

Настоящим заявитель полностью и безусловно присоединяется согласно ст. 428 ГК РФ к Регламенту электронного документооборота Системы «Личный кабинет пайщика» АО «ДК РЕГИОН» (далее – Регламент), а также всем приложениям к ним, заключая тем самым договор на использование системы «Личный кабинет пайщика» электронного документооборота АО «ДК РЕГИОН». Заявитель подтверждает, что полностью прочитал, ознакомлен и согласен с содержанием и условиями Регламента и приложениями к ним, обязуется полностью, своевременно и в полном объеме выполнять принятые на себя обязательства и соблюдать положения Регламента. Заявитель заявляет, что намерен осуществлять обмен электронными документами в системе «Личный кабинет пайщика», порядок которого устанавливает Организатор ЭДО.

После подачи настоящего заявления заявитель не может ссылаться на то, что он не ознакомился с вышеуказанными документами (полностью или частично) либо не признает их обязательность при осуществлении электронного документооборота.

Контактная информация			
Контактный телефон			
Адрес электронной почты (e-mail)			
Должность руководителя (для юридических лиц)		ФИО Руководителя (для юридических лиц)	
Дата заявления		Подпись заявителя/уполномоченного лица заявителя	

М.П.

Приложение №2
к Регламенту электронного документооборота
Системы «Личный кабинет пайщика»

Уведомление Зарегистрированного лица (пайщика) о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями третьих лиц. Рекомендации Зарегистрированным лицам (пайщикам) по защите от противоправного доступа и о рисках вредоносных программ

I. Уведомление о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями третьих лиц,

В соответствии с требованиями Положения об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций (утв. Банком России 20.04.2021 N 757-П) **Акционерное общество «Депозитарная компания «РЕГИОН»** (далее – «Общество») настоящим **уведомляет** Зарегистрированных лиц (пайщиков) Общества о возможных рисках финансовых потерь из-за:

- несанкционированного доступа к Вашей информации третьими лицами;
- совершения в отношении Вас иных противоправных действий.

Следует принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления противоправных действий. Такие риски могут быть обусловлены включая, но не ограничиваясь следующими примерами:

a. Кража пароля и идентификатора доступа или иных конфиденциальных данных, например, закрытого ключа посредством технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа.

b. Установка на устройство вредоносного кода.

c. Использования злоумышленником утерянного или украденного телефона для получения СМС кодов, которые могут применяться Обществом в качестве дополнительной защиты от несанкционированных действий.

d. Кража или несанкционированный доступ к устройству, с которого Вы пользуетесь услугами/сервисами Общества для получения данных и/или несанкционированного доступа к сервисам с этого устройства.

e. Получение пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником Общества или техническим специалистом или использует иную легенду и просит Вас сообщить ему эти секретные данные; или направляет поддельные почтовые сообщения или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привес к компрометации устройства;

f. Перехвата почтовых сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если Ваша почта используется для информационного обмена с Обществом. В случае получения доступа к вашей почте, отправка сообщений от Вашего имени в Общество.

Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) для доступа к информационным системам Общества несет владелец учётных данных (Зарегистрированное лицо (пайщик).

Общество не несет ответственность в случаях финансовых потерь, понесенных Зарегистрированными лицами (пайщиками) в связи с пренебрежением правилами информационной безопасности.

II. Меры по предотвращению несанкционированного доступа к защищаемой информации.

1. Обеспечьте защиту устройства, с которого вы пользуетесь услугами Общества, 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, полученные от Общества: пароли, СМС коды, кодовые слова, 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 Общества по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон контакт центра Общества.
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 Общество или иных доверенных лиц.
   - 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 на сайте Общества о последних критичных уязвимостях и о вредоносном коде.
   - При наличии в рамках вашего продукта сервиса контакт центра, осуществляйте звонок только по номеру телефона, указанному в договоре. Важно учесть, что от лица Общества 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 могу установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам Общества, которыми пользовались Вы.

- При утере, краже телефона, используемого для получения СМС кодов или доступа к системам Общества необходимо:
    a. незамедлительно проинформировать Общество через контактный центр;
    b. целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить сим карту;
    c. сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Общество.
- При подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Общество, в отношении ключевой информации;
- Помните, что наличие резервной копии может облегчить и ускорить восстановление Вашего устройства;
- Лучше всего использовать максимально защищенное устройство, доступ к которому есть только у Вас;
- Контролируйте свой телефон, используемый для получения СМС кодов. В случае выхода из строя сим карты, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи.
- 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:
    - Использовать для хранения секретных ключей электронной подписи внешние носители.
    - Крайне внимательно относиться к 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 Общества;
    - 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 (pdf, docx, png, xlsx и т.д.).

При подозрении в компрометации пароля доступа, ключей или несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов необходимо незамедлительно обращаться в Общество (тел. +7 (495) 777-29-64, e-mail: depo@region.ru)

Ознакомлен
Зарегистрированное лицо (пайщик) _____
«__»_____20__г.