УТВЕРЖДЕНО
Советом директоров
Общества с ограниченной ответственностью
«Московские партнеры»

Протокол № 31/05 от 31 мая 2019 г.

Декларация о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления

Проведение финансовых операций связано с наличием указанных ниже рисков, которые в равной степени могут реализоваться для Клиента.

Общие причины компрометации информации:

- использование Клиентом ИТС сообщений, полученных от Брокера и содержащих информацию, способную скомпрометировать ключи или пароль Клиента, необходимые для получения доступа к финансовой информации, а также материальные носители указанной информации (далее – Информационный ресурс) не по прямому назначению;
- несоблюдение Клиентом порядка эксплуатации Информационного ресурса до начала его эксплуатации и
  несоблюдение условий технического доступа;
- допуск Клиентом к Информационному ресурсу, его материальным носителям, а также к информации, содержащей коды, логины, пароли, ключи, обеспечивающие доступ к указанному Информационному
  ресурсу, лиц, не уполномоченных Клиентом на совершение финансовых операций, допуск копирования такой информации;
- нарушение целостности Информационного ресурса;
- игнорирование Клиентом информации об изменениях, вносимых провайдерами Информационного ресурса в функционал и условия предоставления доступа к Информационному ресурсу;
- несоблюдение Клиентом рекомендаций о смене полученных паролей на собственные пароли;
- несоблюдение Клиентом процедуры по уведомлению Брокера, удостоверяющего центра о компрометации
  ключа, пароля (в том числе при утрате (потере, хищении) Клиентом устройства, с использованием которого
  им совершались действия в целях осуществления финансовой операции);
- несоблюдение Клиентом рекомендаций по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее -
  вредоносный код), в целях противодействия незаконным финансовым операциям;
- несоблюдение Клиентом рекомендаций по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет.

Способы защиты информации от компрометации:

- использовать Информационные ресурсы по прямому назначению;
- соблюдать порядок эксплуатации Информационного ресурса до начала его эксплуатации и соблюдать
  условия технического доступа;
- не допускать к Информационному ресурсу, его материальным носителям, а также к информации, содержащей коды, логины, пароли, ключи, обеспечивающие доступ к указанному Информационному ресурсу, лиц, не уполномоченных Клиентом на совершение финансовых операций, не допускать копирование такой информации, для указанных целей рекомендуется хранить ключевую информацию на отчуждаемом носителе (USB-накопителе) и хранить его в сейфе или запираемом шкафу, исключив возможность несанкционированного доступа; в случае, если избежать копирования и/или доступа к Информационному ресурсу не удается, сообщать Брокеру, удостоверяющему центру о данном факте;
- не допускать нарушения целостности Информационного ресурса, а в случае, если избежать нарушения целостности не удается, сообщать Брокеру, удостоверяющему центру о данном факте;
- не игнорировать информацию об изменениях, вносимых провайдерами Информационного ресурса в функционал и условия предоставления доступа к Информационному ресурсу;
- соблюдать рекомендации о смене полученных паролей на собственные пароли,
  длина пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и

прописных букв, цифр и символов;

- рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, на которых Клиент вводит конфиденциальные данные;
- в том случае, если Клиент обнаружил, что пароль от Информационного ресурса скомпрометирован, рекомендуется незамедлительно сменить пароль на новый (если такая возможность предусмотрена Информационным ресурсом), известный только Клиенту, удовлетворяющий требованиям, указанным выше;
- если в процессе работы Клиент столкнулся с тем, что ранее действующий пароль не срабатывает и не
  позволяет войти в систему, необходимо как можно быстрее обратиться к Брокеру для получения инструкций по смене пароля;
- Клиент не должен разглашать пароли от Информационного ресурса, Брокер не рассылает электронных писем, SMS или других сообщений с просьбой уточнить конфиденциальные данные Клиента без прохождения процедуры идентификации (то есть без составления анкет на клиента либо без авторизации через систему ЕСИА (Госуслуги) / СМЭВ), Клиенту следует иметь в виду информацию о том, что Брокер ни при каких обстоятельствах не может требовать от Клиента разглашения паролей, в том числе от Информационных ресурсов, предоставленных Клиенту Брокером / при посредничестве Брокера; в любом случае, если у Клиента имеются сомнения, ему рекомендуется связаться с Брокером и уточнить, исходит ли запрос от Брокера,
- Клиент не должен пересылать файлы с конфиденциальной информацией по электронной почте или через
  SMS-сообщения;
- соблюдать процедуру по уведомлению Брокера, удостоверяющего центра о компрометации ключа, пароля (в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им
  совершались действия в целях осуществления финансовой операции);
- рекомендуется незамедлительно обратиться к Брокеру в том случае, если Клиент получил уведомление об операции, которую Клиент не совершал;
- соблюдать следующие рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям:
  - на персональном компьютере Клиента должно быть установлено антивирусное ПО (при наличии технической возможности);
  - антивирусное ПО должно регулярно обновляться, рекомендуется установить по умолчанию максимальный уровень политик безопасности, т. е. не требующий ответов пользователя при обнаружении вирусов, лечение (удаление) зараженных файлов должно производиться антивирусным средством в автоматическом режиме;
  - не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка
    жесткого диска персонального компьютера Клиента на предмет наличия вирусов и вредоносного программного кода, проверка должна осуществляться согласно расписанию, выставленному в настройках антивирусного средства;
  - рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях;
  - при использовании сети Интернет для обмена почтовыми сообщениями необходимо применять антивирусное ПО, разработанное специально для почтовых клиентов;
  - при возникновении подозрения на наличие компьютерного вируса (нетипичная работа ПО, появление
    графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т. п.) рекомендуется приостановить работу с системой до полного устранения неисправностей;
  - рекомендуется не использовать компьютер, с которого Клиент осуществляет запуск информационно-торговой системы, для общения в социальных
    сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы;
  - рекомендуется не открывать файлы, полученные по электронной почте от неизвестных отправителей;
- соблюдать следующие рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет:
  - мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором Клиенту под каким-либо предлогом может предлагаться ввести конфиденциальную информацию, зачастую такие
    web-сайты являются почти точной копией web-сайтов известных компаний, которым Клиент

доверяет, и предназначены для сбора конфиденциальной информации обманным путем;

- перед просмотром электронного письма рекомендуется всегда проверять адрес отправителя, строка
  «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса настоящей компании, изменить адрес электронной почты отправителя очень просто, поэтому необходимо соблюдать бдительность;
- рекомендуется внимательно читать текст электронного письма, электронные письма от известных компаний обычно не содержат орфографических или грамматических ошибок, если в тексте присутствуют слова на иностранном языке, специальные символы и т. д., скорее всего это электронное письмо, отправленное мошенниками;
- следует опасаться безличных обращений, таких как «Уважаемый пользователь», или обращений по адресу электронной почты, типичное фишинговое письмо начинается с обезличенного приветствия;
- рекомендуется сохранять спокойствие, многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Клиента действовать быстро и необдуманно, многие поддельные сообщения электронной почты пытаются убедить Клиента в том, что его счету угрожает опасность, если лицо немедленно не обновите критически важные данные;
- рекомендуется внимательно анализировать ссылки, они могут быть почти точной копией подлинных,
  однако они способны перенаправить Клиента на мошеннический web-сайт, если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не следует переходить по ней;

Указанный выше перечень рисков не является исчерпывающим в виду многообразия ситуаций, которые могут возникать при совершении Клиентом финансовых операций.