Информация 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 реализовываться для клиента.

Общие причины компрометации информации:

- использование клиентом личного кабинета на сайте микрофинансовой организации и/или электронной подписи и/или сообщений, полученных от микрофинансовой организации 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 микрофинансовой организации, 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 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 микрофинансовой организации, удостоверяющему центру о данном факте;
- не допускать нарушения целостности информационного ресурса, а в случае, если избежать нарушения целостности не удается, сообщать микрофинансовой организации, 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, рекомендуется регулярно менять пароль в личном кабинете на сайте микрофинансовой организации, длина пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр;

- рекомендуется использовать различные уникальные пароли для различных веб-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 микрофинансовой организации для получения инструкций по смене пароля;
- клиент не должен разглашать пароли от информационного ресурса, микрофинансовая организация не рассылает электронных писем, СМС 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 микрофинансовая организация ни при каких обстоятельствах не может требовать от клиента разглашения паролей, в том числе от информационных ресурсов, предоставленных клиенту микрофинансовой организацией; в любом случае, если у клиента имеются сомнения, ему рекомендуется связаться с микрофинансовой организацией и уточнить, исходит ли запрос от микрофинансовой организации,
- клиент не должен пересылать файлы с конфиденциальной информацией по электронной почте или через СМС-сообщения;
- соблюдать процедуру по уведомлению микрофинансовой организации, 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 микрофинансовой организации 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 доступ к сайту личного кабинета на сайте микрофинансовой организации и 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 веб-сайт – это небезопасный веб-сайт, на котором Клиенту под каким-либо предлогом может предлагаться ввести конфиденциальную информацию, зачастую такие веб-сайты являются почти точной копией веб-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 веб-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 ввиду многообразия ситуаций, которые могут возникать при совершении клиентом финансовых операций.