РЕКОМЕНДАЦИИ
по соблюдению информационной безопасности клиентами ООО УК «ПРОФИНВЕСТ» в целях противодействия осуществлению незаконных финансовых операций

Настоящие Рекомендации по соблюдению информационной безопасности клиентами ООО УК «ПРОФИНВЕСТ» (далее - Организация) в целях противодействия осуществлению незаконных финансовых операций (далее – Рекомендации) разработаны в соответствии с требованиями Положения Банка России от 20.04.2021 № 757-П «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» и направлены на информирование клиентов

- о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления,
- о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.

Рекомендации подлежат доведению до сведения клиентов Организации путем размещения на сайте Организации в сети Интернет.

Выполнение клиентом Рекомендаций по соблюдению информационной безопасности (совокупности мер, применение которых направлено на непосредственное обеспечение защиты информации, процессов, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты (здесь и далее термины из ГОСТ Р 57580.1-2017)) не гарантирует обеспечение подтверждения подлинности, неизменности, конфиденциальности, целостности и доступности информации, но снижает риски информационной безопасности и направлено на минимизацию возможных негативных последствий в случае их реализации.

В связи с тем, что требования информационной безопасности так же могут быть отражены в договорах, регламентах, правилах и иных документах Организации, регламентирующих деятельность Организации и предоставление ею услуг клиентам, настоящие Рекомендации действуют в части, не противоречащей им.

В случае заключения договора с Организацией клиентам рекомендуется внимательно изучить договор, приложения к договору и иные документы, связанные с исполнением договора, ознакомиться с разделами, посвященными информационной безопасности/конфиденциальности.

Если клиент имеет различные требования и/или рекомендации по информационной безопасности от Организации и иных лиц, то ему следует использовать более строгие требования и/или рекомендации применительно к каждому аспекту выполнения указанных требований и/или рекомендаций.

1. Уведомление о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

1.1. Клиенты Организации несут риски возможных финансовых потерь вследствие получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления. Такие риски могут быть обусловлены включая, но не ограничиваясь следующими событиями:

- осуществление лицами, не обладающими правом осуществления финансовых операций, финансовых операций от лица клиента;
- злоупотребление доверием клиента при совершении финансовых операций от лица клиента лицами, уполномоченными клиентом на совершение таких операций;
- утрата, потеря (хищение) идентификатора(ов) доступа клиента и/или его электронной подписи, необходимых для осуществления финансовых операций;
- разглашение клиентом третьим лицам, в том числе неуполномоченным сотрудникам Организации, информации (персональные данные клиента, кодовые слова и фразы, иная информация, позволяющая идентифицировать клиента) необходимой для создания, изменения, блокирования идентификатора(ов) доступа и/или его электронной подписи;
- доступ третьих лиц с согласия клиента или без него к связанным сервисам аутентификации, которые могут быть использованы Организацией для идентификации клиента, в том числе дополнительной и/или резервной идентификации клиента;
- воздействие вредоносного кода на устройства клиента и каналы связи, с использованием которых совершаются финансовые операции;
- утрата клиентом контроля за устройством, с которого он совершал финансовые операции;
- использование клиентом для совершения операций оборудования, доступ к которому имеют третьи лица, а также несертифицированного оборудования;
- совершение в отношении клиента иных противоправных действий, связанных с информационной безопасностью.

1.2. Риски, напрямую не влекущие финансовые потери:

- Разглашение неопределённому кругу лиц персональных данных и иной конфиденциальной информации клиента;
- Репутационный риск клиента;
- Риски, связанные с нарушением законодательства действиями, произведёнными от имени клиента;
- Репутационный риск Организации.

1.3. Клиентам рекомендуется проводить профилактические мероприятия, направленные на повышение уровня информационной безопасности.

1.4. Организация не несет ответственности в случаях финансовых потерь, понесенных клиентами в связи с пренебрежением правилами информационной безопасности.

2. Меры по предотвращению несанкционированного доступа к защищаемой информации.

2.1. Клиентам Организации следует предпринимать все доступные меры для предотвращения несанкционированного доступа к защищаемой информации, включая, но не ограничиваясь следующими мерами:

2.1.1. Обеспечение надлежащей защиты устройства и канала связи используемого для получения услуг и обмена информацией с Организацией:

- использование только сертифицированных аппаратных и программных средств, доверенных и защищённых каналов связи;
- использование только лицензионного программного обеспечения, полученного из доверенных источников;
- запрет на установку программ из непроверенных источников;
- использование средств защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран и др.;
- настройка прав доступа к устройству с целью предотвращения несанкционированного доступа; создание профилей доступа в соответствии с задачами, для выполнения которых они будут использованы, с предоставлением минимально достаточных для их выполнения прав;
- хранение, использование устройства способом, позволяющим избежать рисков его кражи и/или утери, доступа к нему третьих лиц;
- своевременные обновления операционной системы, системного и прикладного программного обеспечения;
- использование парольной или иной защиты для доступа к устройству, сим-карте, (съёмным) носителям информации, носителям с электронной подписью; использование двухфакторной аутентификации, если есть такая возможность;
- осуществляйте проверку жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода;
- выполнение регламентов в части информационной безопасности производителей и поставщиков оборудования, программ и услуг.

2.1.2. Обеспечение конфиденциальности защищаемой информации:

- хранение в тайне идентификационных данных, электронной подписи, иных конфиденциальных данных, используемых Организацией для идентификации клиента, а при компрометации таких данных клиент обязан немедленно принять меры для их смены и/или блокировки и уведомить Организацию о такой компрометации;
- соблюдение принципа разумного раскрытия идентификационных данных (в том числе персональных данных), а в случае запроса у клиента указанной информации в связи с оказанием услуг Организацией, клиенту рекомендуется по возможности оценить ситуацию и уточнить полномочия запрашивающего лица и процедуру

предоставления запрашиваемой информации через независимый канал связи, например, по контактному телефону Организации;

- исключение повторного использования ранее использовавшихся паролей/ключевых слов, фраз, а также ответов на контрольные вопросы, которые могут быть известны третьим лицам;

- недопущение использования в качестве паролей/ключевых слов, фраз, ответов на контрольные вопросы данных, которые могут быть прямо или косвенно сопоставлены с информацией о клиенте, а также сочетаний, которые могут быть подобраны перебором;
- недопущение публичного доступа к конфиденциальной информации, включая возможность дистанционного наблюдения, видеонаблюдения.

2.1.3. Проявление осторожности и предусмотрительности:

- клиентам Организации рекомендуется проявлять должную осторожность в следующих случаях:
  - при получении электронных писем со ссылками и вложениями, так как они могут привести к заражению устройства клиента вредоносным кодом;
  - при получении электронных писем с вложениями в виде архивов с файлами, защищенных паролем, или зашифрованных файлов/архивов, так как в таких файлах может быть вредоносный код;
  - при просмотре/работе с интернет-сайтами, так как вредоносный код может быть загружен с сайта;
  - использовании сетей связи общего доступа.

  С помощью вредоносного кода, попавшего к клиенту через электронную почту или ссылку в сети Интернет, злоумышленник может получить доступ к данным на зараженном устройстве клиента и/или выполнить на нём произвольные действия.
- клиентам Организации рекомендуется внимательно проверять адресата от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под Организацию или иных доверенных лиц;
- клиентам Организации рекомендуется следить за информацией в прессе и на сайте Организации о последних критичных уязвимостях и о вредоносном коде и принимать такую информацию к сведению;
- клиентам Организации рекомендуется осуществлять звонки и направлять почтовые сообщения (в том числе электронные) в Организацию только по номеру телефона, почтовому и электронному адресам, указанным на сайте Организации в сети Интернет. От лица Организации не могут поступать звонки или сообщения, в которых от клиента требуют предоставить идентификаторы доступа;
- клиентам Организации не следует предоставлять доступ к устройству третьим лицам, так как в этом случае клиент несет риск загрузки такими лицами на устройство вредоносного кода.
- в случае утраты (потери, хищения) устройства клиентам рекомендуется для предотвращения использования злоумышленниками устройства для доступа к услугам Организации от лица клиента:
  - незамедлительно проинформировать Организацию по контактному номеру телефона и/или адресу электронной почты, указанным на сайте Общества в сети Интернет;
  - по возможности оперативно, с учетом прочих рисков и особенностей использования устройства, заблокировать доступ к устройству, к установленной в нём сим-карте (при наличии).

- в случае получения услуг Организации через устройство, клиентам рекомендуется использовать для этих целей отдельное устройство, доступ к которому есть только у клиента;
- клиентам рекомендуется использовать сложный пароль для входа на устройство, и не хранить пароль в открытом виде на компьютере/мобильном устройстве;
- клиентам рекомендуется поддерживать в актуальном состоянии свою контактную информацию, предоставленную Организации, чтобы в случае необходимости представитель Организации мог оперативно связаться с клиентом.

2.1.4. При работе на персональном компьютере клиентам рекомендуется:

- 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 сложный пароль для входа на компьютер, и не хранить пароль в открытом виде на компьютере;
- ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

2.1.5. При работе с мобильным устройством клиентам рекомендуется:

- не оставлять свое мобильное устройство без присмотра, чтобы исключить его несанкционированное использование;
- использовать только официальные мобильные приложения, установленные с помощью магазина приложений;
- не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в SMS-сообщениях, Push-уведомлениях или по электронной почте, в том числе от имени Организации;
- установить на мобильном устройстве сложный пароль для входа и не хранить пароль в открытом виде.

2.1.6. В случае обмена информацией с Организацией через сеть Интернет клиентам рекомендуется:

- проверять информацию об Организации в сертификате сайта;
- 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 клиенту ресурсах;
- не посещать сайты сомнительного содержания;
- не сохранять пароли в памяти интернет-браузера, если к устройству имеют доступ третьи лица;

- не нажимать на баннеры и всплывающие окна, возникающие во время работы в сети Интернет;
- не открывать файлы, полученные (скачанные) из неизвестных источников.

2.2. При подозрении в несанкционированном доступе к защищаемой информации, сервисам Организации, клиенту необходимо незамедлительно обратиться в Организацию по контактному телефону и/или адресу электронной почты, указанным на сайте Организации в сети Интернет http://www.uk.profinwest.com .