

Утверждено Приказом  
Генерального директора  
Общества с ограниченной ответственностью  
Инвестиционная компания «Фридом Финанс»  
№31052019-02 от 31.05.2019

### **Рекомендации**

**по соблюдению информационной безопасности клиентами Общества с ограниченной ответственностью Инвестиционной компании «Фридом Финанс» в целях противодействия незаконным финансовым операциям.**

Москва, 2019

## 1. Общие положения.

В соответствии с требованиями Положения Банка России от 17.04.2019 № 684-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» Общество с ограниченной ответственностью Инвестиционная компания «Фридом Финанс» (далее по тексту - Общество) доводит до вашего сведения основные рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям.

Рекомендации 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 гарантируют обеспечение конфиденциальности, целостности и доступности информации, но позволяют в целом снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации.

В связи с тем, что требования информационной безопасности так же могут быть отражены в договорах, регламентах, правилах и иных документах Общества, регламентирующих предоставление услуг/сервисов, настоящие Рекомендации действуют в части, не противоречащей положениям внутренних документов.

## 2. Общие рекомендации.

В целях снижения риска реализации инцидентов информационной безопасности (ГОСТ Р 57580.1-2017) – нежелательные или неожиданные события защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов (клиента), технологических процессов Общества и (или) нарушить конфиденциальности, целостности и доступности информации вследствие:

- несанкционированного доступа к вашей информации лицами, не обладающими правом осуществления значимых (критичных) операций (в т.ч. финансовых)
- потери (хищения) носителей ключей электронной подписи, с использованием которых, осуществляются критичные (финансовые) операции;
- воздействия вредоносного кода на устройства, с которых совершаются критичные (финансовые) операции;
- совершения в отношении Вас иных противоправных действий, связанных с информационной безопасностью.

Рекомендуется соблюдать ряд профилактических мероприятий, направленных на повышение уровня информационной безопасности при использовании объектов информатизации (совокупности объектов, ресурсов, средств и систем обработки информации, в т.ч. автоматизированных систем, используемых для обеспечения информатизации бизнес-процессов (ГОСТ Р 57580.1-2017) Общества.

Внимательно изучите договор, приложения к договору и иные документы, связанные с исполнением договора, ознакомьтесь с разделами, посвященными информационной безопасности/конфиденциальности.

### 3. Риск получения третьими лицами несанкционированного доступа к защищаемой информации

При осуществлении критичных (финансовых) операций следует принимать во внимание риск 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 примерами:

- Кража пароля и идентификатора доступа или иных конфиденциальных данных, например, CVV\CVC номера карты, ключей электронной подписи/шифрования посредством технических средств и/или вредоносного кода; и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;
- Установка на устройство вредоносного кода, который позволит злоумышленникам осуществить критичные операции от Вашего имени;
- Использования злоумышленником утерянного или украденного телефона (SIM карты) для получения СМС кодов, которые могут применяться Обществом в качестве дополнительной защиты для несанкционированных финансовых операций, что позволит им обойти защиту;
- Кража или несанкционированный доступ к устройству, с которого Вы пользуетесь услугами/сервисами Общества для получения данных и/или несанкционированного доступа к сервисам Общества с этого устройства;
- 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 сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;
- Перехвата электронных сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если Ваша электронная почта используется для информационного обмена с Обществом. Или в случае получения доступа к вашей электронной почте, отправка сообщений от вашего имени в Общество.

### 4. Снижение риска финансовых потерь.

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

- Использование только лицензионного программного обеспечения, полученного из доверенных источников;
- Запрет на установку программ из непроверенных источников;
- Наличие средств защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран;
- 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, особенно в части обновлений безопасности. Имейте в виду, что обновления снижают риски заражения вредоносным кодом. Злоумышленники часто используют старые уязвимости;
  - Активация парольной или иной защиты для доступа к устройству.
- В. Обеспечьте конфиденциальность:
- Храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Общества: пароли, СМС коды, кодовые слова, ключи электронной подписи/шифрования, а в случае вероятной 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 SVC\CVV 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 Общества.
- С. Проявляйте осторожность и предусмотрительность:
- Будьте осторожны при получении электронных писем со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносным кодом. Вредоносный код, попав к вам через электронную почту или интернет ссылку на сайт, может получить доступ к любым данным и информационным системам на вашем устройстве;
  - Внимательно проверяйте адресата, от которого пришло электронное письмо. Входящее электронное письмо может от злоумышленника, который маскируется под Общество или ее уполномоченных/доверенных лиц;
  - Будьте осторожны при просмотре/работе с интернет-сайтами, так как вредоносный код может быть загружен с сайта;
  - Будьте осторожны с файлами из новых или «недоверенных» источников (в т.ч. архивы с паролем, зашифрованные файлы/архивы, т.к. такого рода файлы не могут быть проверены антивирусным ПО в автоматическом режиме);
  - 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;
  - Следите за информацией в прессе и на сайте Общества о последних критичных уязвимостях и о вредоносном коде;
  - При подаче поручений и/или ином обращении в Общество, осуществляйте звонок только по номеру телефона, указанному в договоре или на официальном сайте Общества. И имейте в виду, 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. Кодовое слово может быть запрошено только, если Вы сами позвонили в Общество;
  - Имейте в виду, что, если Вы передаете ваш телефон и/или иное устройство другим пользователям, они могут установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к сервисам и системам Общества, которыми пользовались Вы. В связи с этим, при утере, краже телефона (SIM карты), используемого для получения СМС кодов или доступа к системам и(или) сервисам Общества с Мобильного приложения: 1) незамедлительно проинформировать Общество, 2) целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить SIM-карту, а также сменить пароли и коды доступа (кодовые слова) в к сервисам и(или) системам Общества;

- 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, если это применимо для вашей услуги – отозвать скомпрометированный ключ электронной подписи/шифрования, в соответствии с правилами, отраженными в договоре, приложениях к договору и иных документах, связанных с исполнением договора;
- D. При работе с ключами электронной подписи необходимо:
- Использовать для хранения ключей электронной подписи внешние носители, настоятельно рекомендуется использовать специальные защищенные носители ключевой информации (ключевые носители), например: e-token, смарт-карта и т.п.;
  - Крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они (ключевые носители) не используются для работы;
  - Использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи/ключевым носителям, не хранить пароли открытым виде на компьютере/мобильном устройстве.
- E. 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.
- F. При работе с Мобильного устройства необходимо:
- Не оставлять свое Мобильное устройство без присмотра, чтобы исключить его 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.
- G. 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 у третьих лиц;

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

**При подозрении в компрометации ключей электронной подписи/шифрования или несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов необходимо незамедлительно обращаться в Общество.**