

Рекомендации по соблюдению информационной безопасности клиентами ООО УК «Промфинактив» в целях противодействия незаконным финансовым операциям

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» ООО УК «Промфинактив» (далее – Управляющая компания) настоящим доводит до сведения своих клиентов:

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

информации 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.

1. О возможных рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и осуществлением противоправных действий третьими лицами.

1.1. Клиент Управляющей компании несет риски возможных финансовых потерь вследствие следующих обстоятельств:

- получение лицами, не обладающими правом осуществления финансовых операций от лица клиента, несанкционированного доступа к защищаемой информации;
- совершение в отношении клиента Управляющей компании иных противоправных действий.

1.2. При осуществлении финансовых операций клиенту Управляющей компании следует принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций.

Такие риски могут возникать, помимо прочего, вследствие следующих событий:

- кража или несанкционированный доступ к устройству, с которого клиент Управляющей компании осуществляет обмен информацией с Управляющей компанией или пользуется услугами Управляющей компании, для получения данных и/или несанкционированного доступа к услугам с этого устройства; - перехват почтовых сообщений и получение несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если электронная почта клиента используется для информационного обмена с Управляющей компанией.

В случае получения доступа к электронной почте клиента, отправка сообщений Управляющей компании от его имени может осуществляться другим лицом, не обладающим правом осуществления финансовых операций.

1.3. Управляющая компания не несет ответственность за финансовые потери, понесенные Клиентом в связи с пренебрежением им правилами информационной безопасности.

1.4. В случае использования клиентом Управляющей компании систем электронного документооборота с Управляющей компании, с применением информационных систем организаторов этого электронного документооборота, клиенту Управляющей компании следует придерживаться правил информационной безопасности, рекомендованных этим организатором электронного документооборота.

2. О мерах по предотвращению несанкционированного доступа к защищаемой информации.

2.1. Клиенту Управляющей компании следует предпринять все доступные меры для предотвращения несанкционированного доступа к защищаемой информации. Для указанных целей клиенту Управляющей компании следует принять, помимо прочего, следующие меры:

2.1.1. Обеспечение надлежащей защиты устройства, с помощью которого клиент обменивается информацией с Управляющей компании:

- использование только лицензированного программного обеспечения, полученного из доверенных источников;
- запрет на установку программ из непроверенных источников;
- использование средств электронной безопасности и защиты, таких как антивирус, с регулярно и своевременно обновляемыми базами, персональный межсетевой экран, защита накопителя и прочих;
- настройка прав доступа к устройству таким образом, чтобы несанкционированный доступ к информации на таком устройстве был невозможен даже при утрате устройства владельцем;
- хранение и использование устройства способом, исключающим риски его кражи и/или утери;
- своевременное обновление операционной системы устройства;
- активация парольной или иной защиты для доступа к устройству;
- передача защищаемой информации клиентов только через безопасные беспроводные сети.

2.1.2. Клиенту Управляющей компании следует проявлять повышенную осторожность в следующих обстоятельствах:

а) при получении электронных сообщений со ссылками и вложениями, так как они могут привести к заражению устройства клиента вредоносным кодом;

б) при просмотре/работе с сайтами в сети Интернет, так как вредоносный код может быть загружен с сайта;

в) при получении файлов в архиве с паролем, так как в таком файле может быть вредоносный код. Вредоносный код, попав к клиенту через почту или ссылку на сайт в сети Интернет, может получить доступ к любым данным и информационным системам на зараженном устройстве. Клиенту Управляющей компании следует внимательно проверять отправителя электронных сообщений. Входящее сообщение может исходить от злоумышленника, который маскируется под Управляющую компанию или иных доверенных лиц;

- не следует заходить в системы удаленного доступа с устройств, которые клиент не контролирует. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;

- при наличии в средствах массовой информации и на сайте Управляющей компании сведений о последних критичных уязвимостях и о вредоносном коде, рекомендуется принимать такую информацию к сведению;

- необходимо поддерживать в актуальном состоянии контактную информацию, предоставленную Управляющей компании, чтобы в случае необходимости представитель Управляющей компании мог оперативно связаться с клиентом.

2.1.3. В случае работы 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 устройстве.

2.1.4. При работе с защищаемой информацией на персональном 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.

2.1.5. 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 клиенту ресурсах;
- исключить посещение сайтов сомнительного содержания;
- не сохранять пароли в памяти интернет-браузера, если третьи лица имеют доступ к компьютеру;
- не нажимать на баннеры и всплывающие окна, возникающие во время работы в сети Интернет;
- открывать файлы только известных расширений.