

«УТВЕРЖДЕНО»

Генеральный директор
Невский Кэпитал Партнерс (ООО)

_____ А.М. Щетров

Приказ № 37 от 05.07.2021 г.

**Рекомендации по защите информации
в целях противодействия незаконным финансовым операциям**

Настоящие рекомендации по защите информации в целях противодействия незаконным финансовым операциям разработаны Невский Кэпитал Партнерс (ООО), осуществляющим доверительное управление паевыми инвестиционным фондами (лицензия на осуществление деятельности по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами предоставлена Банком России 17.12.2009 за № 21-000-1-00680), далее - Управляющая компания, 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 защиту информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям.

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

Клиенты Управляющей компании несут риски негативных последствий вследствие следующих обстоятельств:

- получение третьими лицами доступа к персональным данным и иной значимой информации конфиденциального характера, а также их разглашение;

- утрата, потеря (хищение) идентификаторов доступа клиента (в случае их применения), с использованием которых осуществляются финансовые операции;

- воздействие вредоносного кода на устройства клиента, с которых совершаются финансовые операции;

- совершение в отношении клиента иных противоправных действий, связанных с информационной безопасностью.

2. В целях предотвращения 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, для контроля конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременного обнаружения воздействия вредоносного кода рекомендуем принимать следующие меры:

1) использовать и хранить устройство таким образом, чтобы исключить возможность его хищения и несанкционированного использования;

2) использовать современные и актуальные методы блокировки устройств (TouchID, FaceID, Пин-код и др.);

3) устанавливать надежные пароли и не использовать один пароль ко всем системам, регулярно менять пароли, хранить пароли в тайне от всех лиц, без исключения;

4) обязательное блокирование устройства;

5) при утрате (потере, хищении) устройства позаботиться о смене паролей доступа к системам;

6) проверять реквизиты и не сообщать третьим лицам информацию, полученную для проведения финансовой операции в СМС-сообщениях;

7) использовать только лицензионное программное обеспечение;

8) выполнять правила, требования, положения, установленные эксплуатационной документацией на программное обеспечение, информационную систему (ресурс), средства защиты информации, включая средства электронной подписи, используемые при обмене информацией;

9) настроить автоматическое обновление программного обеспечения;

10) устанавливать приложения, скачанные только с официальных магазинов приложений (App Store или Google Play) или с сайтов производителей;

11) использовать антивирусное программное обеспечение и встроенные средства межсетевого экранирования (брандмауэр);

12) настроить автоматическую полную проверку устройств на предмет наличия вирусов и вредоносного программного кода не реже одного раза в месяц;

13) при возникновении подозрения на наличие вируса (признаки - значительное замедление работы, увеличение исходящего/входящего трафика, нетипичная работа устройства, частое появление сообщений о системных ошибках и сбоях и т.п.) провести

дополнительные проверки и приостановить работу с финансовой информацией до устранения проблем;

14) не посещать неофициальные и подозрительные Интернет-ресурсы, а также не использовать неофициальные и подозрительные мобильные приложения;

15) 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.;

16) 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;

17) не разглашать посредством средств связи (например, по телефону или электронной почте) информацию, которая может повлечь несанкционированный доступ к системам, конфиденциальной информации или финансовым операциям;

18) не использовать подключение к публичным сетям связи (WiFi) для осуществления финансовых операций или передачи конфиденциальной информации;

19) соблюдать принцип разумного раскрытия идентификационных данных, в том числе персональных данных (в случае запроса у клиента указанной информации в связи с оказанием услуг Управляющей компанией, клиенту рекомендуется по возможности оценить ситуацию и уточнить полномочия запрашивающего лица и процедуру предоставления запрашиваемой информации через независимый канал связи, например, по контактному телефону Управляющей компании);

20) при подозрении в несанкционированном обращении третьего лица от имени клиента для получения услуг Управляющей компании, Клиенту необходимо незамедлительно обратиться в Управляющую компанию;

21) осуществлять звонки и направлять почтовые сообщения (в том числе электронные) в Управляющую компанию только по номеру телефона, почтовому и электронному адресу, указанным на сайте Управляющей компании в информационно-телекоммуникационной сети Интернет по адресу www.nevskycsp.ru (от лица Управляющей компании не могут поступать звонки или сообщения, в которых от клиента требуют предоставить идентификаторы доступа).

Настоящие рекомендации подлежат доведению до сведения клиентов путем размещения на официальном сайте Управляющей компании в информационно-телекоммуникационной сети Интернет по адресу www.nevskycsp.ru.