УПРАВЛЕНИЕ АКТИВАМИ

УТВЕРЖДЕНЫ

приказом
и.о. генерального директора
ООО «ДОМ.РФ Управление активами»

от «06» марта 2020 г.
№ 06-23-нд

РЕКОМЕНДАЦИИ
по соблюдению информационной безопасности клиентами Общества с ограниченной ответственностью «ДОМ.РФ Управление активами» в целях противодействия незаконным финансовым операциям

Москва

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Общество с ограниченной ответственностью «ДОМ.РФ Управление активами» (далее – Организация) в целях противодействия незаконным финансовым операциям и в рамках соблюдения требований 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» разработало настоящие Рекомендации по соблюдению информационной безопасности клиентами Общества с ограниченной ответственностью «ДОМ.РФ Управление активами» в целях противодействия незаконным финансовым операциям (далее – Рекомендации).
Рекомендации разработаны в соответствии с Методическими рекомендациями комитета НАУФОР по экономической и информационной безопасности по ознакомлению клиентов с информацией в целях противодействия незаконным финансовым операциям.
1.2. Под клиентами в целях настоящих Рекомендаций понимаются владельцы инвестиционных паев паевых инвестиционных фондов, находящихся под управлением Организации (далее – Клиенты).
1.3. Настоящие Рекомендации помогают Клиентам обеспечить информационную безопасность от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники.
1.4. Определения, используемые в настоящих Рекомендациях:

Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем[1].
Вредоносный код	Программный код, приводящий к нарушению штатного функционирования средства вычислительной техники.
Соблюдение информационной безопасности	Совокупность мер, применение которых направлено на непосредственное обеспечение защиты информации, процессов, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты[2].
Инциденты информационной безопасности	Нежелательные или неожиданные события защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов (Клиента), технологических процессов организации и (или) нарушить конфиденциальность, целостность и доступность информации вследствие: – несанкционированного доступа к информации Клиентов лицами, не обладающими правом осуществления значимых (критичных) операций (в том числе финансовых);

[1] ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

[2] Здесь и далее термины из ГОСТ Р 57580.1-2017.

	– 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 Клиента иных противоправных действий, связанных с информационной безопасностью.
Объекты информатизации Организации	Совокупность объектов, ресурсов, средств и систем обработки информации, в том числе автоматизированных систем, используемых для обеспечения информатизации бизнес-процессов.

1.4. Рекомендации не гарантируют Клиентам обеспечение конфиденциальности, целостности и доступности информации, но позволяют в целом снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации.
1.5. Рекомендации действуют в части, применимой к текущей деятельности Организации по управлению паевыми инвестиционными фондами. В связи с тем, что требования информационной безопасности также могут быть отражены в договорах, регламентах, правилах и иных документах Организации, настоящие Рекомендации действуют в части, не противоречащей положениям внутренних документов.

2. РЕКОМЕНДАЦИИ

2.1. В целях снижения риска реализации инцидентов информационной безопасности Организация рекомендует Клиентам соблюдать ряд профилактических мероприятий, направленных на повышение уровня информационной безопасности при использовании объектов информатизации Организации.
2.2. Организация рекомендует Клиентам внимательно изучить договор, приложения к договору и иные документы, связанные с исполнением договора, ознакомиться с разделами, посвященными информационной безопасности / конфиденциальности.
2.3. 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:

- кражей у Клиента 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, как следствие, использование злоумышленниками указанных данных с других устройств для несанкционированного доступа);
- установкой на устройство Клиента вредоносного кода, который позволит злоумышленникам осуществить критичные операции от имени Клиента;
- использованием злоумышленником утерянного или украденного телефона Клиента (сим-карты) для получения СМС с кодами, которые могут применяться Организацией в качестве дополнительной защиты для несанкционированных финансовых операций, что позволит злоумышленнику обойти защиту;
- кражей или несанкционированным доступ к устройству, с которого Клиент пользуется услугами/сервисами Организации, для получения данных и/или несанкционированного доступа к сервисам Организации с этого устройства;

- получением клиентского пароля и идентификатора доступа и/или кода из СМС либо кодового слова и прочих конфиденциальных данных, в том числе паспортных данных, номеров счетов и т.д., путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником Организации или техническим специалистом или использует иную легенду и просит Клиента сообщить ему эти секретные данные либо направляет поддельные сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;
- перехватом электронных сообщений и получением несанкционированного доступа
  к выпискам, отчетам и прочей финансовой информации Клиента, если электронная почта Клиента используется для информационного обмена с Организацией, или в случае получения доступа к электронной почте Клиента – отправкой сообщений от имени Клиента в Организацию.

2.4. Для снижения риска финансовых потерь Организация рекомендует Клиентам:

1) Обеспечить защиту устройства, с которого Клиент пользуется услугами Организации, в том числе путем:
   - использования только лицензионного программного обеспечения, полученного из доверенных источников;
   - запрета на установку программ из непроверенных источников;
   - наличия средств защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран;
   - настройки прав доступа к устройству с целью предотвращения несанкционированного доступа;
   - хранения, использования устройства с целью избежания рисков кражи и/или утери;
   - своевременного обновления операционной системы, особенно в части обновлений безопасности, так как обновления снижают риски заражения вредоносным кодом. Злоумышленники часто используют старые уязвимости;
   - активации парольной или иной защиты для доступа к устройству.

2) Обеспечить конфиденциальность, в том числе путем:
   - хранения в тайне аутентификационных/идентификационных данные и ключевой информации, полученной от Организации: паролей, СМС с кодами, кодовых слов, ключей электронной подписи / шифрования (в случае компрометации необходимо немедленно принять меры для смены и/или блокировки);
   - Соблюдения принципа разумного раскрытия информации о номерах счетов, о паспортных данных Клиента, о номерах кредитных и дебетовых карт, о CVC/CVV кодах, в случае если у Клиента запрашивают указанную информацию, в привязке к сервисам Организации по возможности оценить ситуацию и уточнить полномочия и процедуру через независимый канал, например через телефон контакт-центра Организации.

3) Проявлять осторожность и предусмотрительность:
   - быть осторожными при получении электронных писем со ссылками и вложениями, они могут привести к заражению устройства Клиента вредоносным кодом. Вредоносный код, попав через электронную почту или

интернет-ссылку на сайт, может получить доступ к любым данным и информационным системам на устройстве;
- внимательно проверять адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть направлено злоумышленником, который маскируется под Организацию или иных доверенных лиц;
- быть осторожными при просмотре/работе с интернет-сайтами, так как вредоносный код может быть загружен с сайта;
- быть осторожными с файлами из новых или «недоверенных» источников (в том числе архивами с паролем, зашифрованными файлами/архивами, т.к. такого рода файлы не могут быть проверены антивирусным программным обеспечением в автоматическом режиме);
- не заходить в системы удаленного доступа с «недоверенных» устройств, которые Клиент не контролирует. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;
- следить за информацией в прессе и на сайте Организации о последних критичных уязвимостях и о вредоносном коде;
- иметь в виду, что от лица Организации не могут поступать звонки или сообщения, в которых от Клиента требуют передать код из СМС, пароль, номер карты, кодовое слово и т.д. Кодовое слово может быть запрошено, только если Клиент сам позвонил в контакт-центр по номеру телефона, указанному в договоре или на официальном сайте Организации;
- иметь в виду, что, если Клиент передает телефон и/или устройство другим пользователям, они могу установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам Организации, которыми пользовался Клиент. В связи с этим при утере, краже телефона (сим-карты), используемого для получения СМС с кодами или доступа к системам организации с мобильного приложения, Клиенту следует:
  - незамедлительно проинформировать Организацию через контактный центр;
  - по возможности оперативно (с учетом прочих рисков и особенностей использования телефона) заблокировать и перевыпустить сим-карту, а также сменить пароль в мобильном приложении;
- при подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством, и/или заблокировать доступ, обратившись в Организацию, в отношении ключевой информации, если это уместно для услуги – отозвать скомпрометированный ключ электронной подписи / шифрования в соответствии с правилами, отраженными в договоре, приложениях к договору и иных документах, связанных с исполнением договора;
- помнить, что наличие «эталонной» резервной копии может облегчить и ускорить восстановление устройства Клиента;
- лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у Клиента;
- контролировать телефон, используемый для получения СМС с кодами. В случае выхода из строя сим-карты незамедлительно обратиться к сотовому оператору для уточнения причин и восстановления связи.

4) При работе с ключами электронной подписи:
   - Использовать для хранения ключей электронной подписи внешние носители, настоятельно рекомендуется использовать специальные защищенные носители ключевой информации (ключевые носители), например: e-token, смарт-карту 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 в открытом виде на компьютере / мобильном устройстве.

5) При работе на компьютере:
   - 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 третьих лиц.

6) При работе с мобильным приложением:
   - не оставлять мобильное устройство без присмотра, чтобы исключить несанкционированное использование мобильного приложения;
   - использовать только официальные мобильные приложения;
   - не переходить по ссылкам и не устанавливать приложения / обновления безопасности, пришедшие в СМС-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Организации;
   - установить на мобильном устройстве пароль для доступа к устройству и приложению.

7) При обмене информацией через сеть Интернет:
   - 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 ресурсах;
   - ограничить посещения сайтов сомнительного содержания;
   - не сохранять пароли в памяти интернет-браузера, если к компьютеру возможен доступ третьих лиц;
   - не нажимать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;
   - не открывать файлы, полученные (скачанные) из неизвестных источников.

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