Эссет
Менеджмент

Исх. № 1162 от 26.03.2020

Общество с ограниченной ответственностью «Эссет Менеджмент» (Лицензия на осуществление деятельности по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами № 21-000-1-00987 от 30 января 2015 года, выдана Банком России, без ограничения срока действия) (далее – Организация) доводит до сведения клиентов рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям, в том числе:

- информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- информацию о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате 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.

При этом под защищаемой информацией понимается:

- информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками Организации и (или) клиентами Организации (далее - электронные сообщения);
- информация, необходимая Организации для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом;
- информация об осуществленных Организацией и её клиентами финансовых операциях;
- ключевая информация средств криптографической защиты информации, используемая Организацией и её клиентами при осуществлении финансовых операций.

Организация рекомендует соблюдать ряд профилактических мероприятий, направленных на повышение уровня информационной безопасности при использовании объектов информатизации Организации.

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

1) При осуществлении 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:

Общество с ограниченной ответственностью «Эссет Менеджмент»
123001, г. Москва, ул. Садовая Б., дом 5, корпус 1, этаж 6
ОГРН 5147746030581, ИНН 7708820892, КПП 771001001
телефон: +7 (495) 137-51-32, эл. почта: am@assetmng.ru

a. Кража пароля и идентификатора доступа или иных конфиденциальных данных и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;
b. Установка на устройство вредоносного кода, который позволит злоумышленникам осуществить финансовые операции от вашего имени;
c. Использования злоумышленником утерянного или украденного телефона (SIM-карты) для получения СМС-кодов, которые могут применяться Организацией в качестве дополнительной защиты для несанкционированных финансовых операций, что позволит им обойти защиту;
d. Кража или несанкционированный доступ к устройству, с которого вы пользуетесь услугами/сервисами Организации для получения данных и/или несанкционированного доступа к сервисам Организации с этого устройства;
e. 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 Организации или техническим специалистом или использует иную легенду и просит вас сообщить ему эти секретные данные; или направляет поддельные электронные сообщения или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;
f. Перехвата электронных сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если ваша электронная почта используется для информационного обмена с Организацией. Или в случае получения доступа к вашей электронной почте, отправка электронных сообщений от вашего имени в Организацию.

Несанкционированный доступ к защищаемой информации может повлечь разглашение данной информации, деструктивное воздействие на носители информации и их содержимое, совершение юридически значимых действий против воли клиента, иной ущерб.

2) Для снижения риска ущерба:

a. Обеспечьте защиту устройства, с которого вы пользуетесь услугами Организации, 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 средства 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.

b. Обеспечьте конфиденциальность:

- Храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Организации: пароли, СМС-коды, кодовые слова, ключи электронной подписи/шифрования, а в случае 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 CVC\CVV кодах, в случае если у вас запрашивают указанную информацию, в привязке к сервисам Организации, по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, по номеру телефона, указанному на официальном сайте Организации.

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 быть от злоумышленника, который маскируется под Организацию или иных 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 о последних критичных уязвимостях и о вредоносном коде;
- Осуществляйте звонок только по номеру телефона, указанному в договоре или на официальном сайте Организации. И имейте в виду, что от лица Организации 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 Организацию;
- Имейте в виду, если вы передаете ваш телефон и/или устройство другим пользователям, они могут установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам Организации, которыми пользовались вы. В связи с этим при утере, краже телефона (SIM-карты), используемого для получения СМС-кодов или доступа к системам Организации с мобильного приложения: 1) незамедлительно проинформировать Организацию, 2) целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить SIM-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 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;

- Помните, что наличие «эталонной» резервной копии может облегчить и ускорить восстановление вашего устройства;
- Лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у вас;
- Контролируйте свой телефон, используемый для получения СМС-кодов. В случае выхода из строя SIM-карты, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи.

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 открытом 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 мобильным приложением необходимо:
- Не оставлять свое 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 SMS-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Организации;
- Установить на мобильном устройстве пароль для доступа к устройству и приложению.

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 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 Организацию.

Предложенные рекомендации 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.

Настоятельно советуем соблюдать предложенные рекомендации.

Обращаем внимание, что стоимость инвестиционных паев может увеличиваться и уменьшаться, результаты инвестирования в прошлом не определяют доходы в будущем, государство не гарантирует доходность инвестиций в паевые инвестиционные фонды.

Прежде чем приобрести инвестиционный пай, следует внимательно ознакомиться с правилами доверительного управления паевым инвестиционным фондом.

Получить подробную информацию о паевых инвестиционных фондах, находящихся под управлением ООО «Эссет Менеджмент», а также ознакомиться с правилами доверительного управления такими фондами и иными документами, предусмотренными в Федеральном законе от 29.11.2001 № 156-ФЗ «Об инвестиционных фондах», «Положении о требованиях к порядку и срокам раскрытия информации, связанной с деятельностью акционерных инвестиционных фондов и управляющих компаний паевых инвестиционных фондов, а также к содержанию раскрываемой информации», утвержденном Приказом ФСФР России от 22 июня 2005 г. № 05-23/пз-н, и иных нормативных актах в сфере финансовых рынков можно в офисе ООО «Эссет Менеджмент» по адресу: 123001, г. Москва, ул. Садовая Б., дом 5, корпус 1, этаж 6; по телефону: +7 (495) 137-51-32. Информация, подлежащая в соответствии с Федеральным законом от 29.11.2001 № 156-ФЗ «Об инвестиционных фондах» и нормативными актами в сфере финансовых рынков раскрытию путем опубликования на сайте управляющей компании паевого инвестиционного фонда в информационно-телекоммуникационной сети «Интернет», публикуется на сайте ООО «Эссет Менеджмент» по адресу www.assetmng.ru. Информация, подлежащая в соответствии с Федеральным законом от 29.11.2001 № 156-ФЗ «Об инвестиционных фондах», нормативными актами в сфере финансовых рынков и правилами доверительного управления Фондом раскрытию путем опубликования в печатном издании, публикуется в «Приложении к Вестнику Федеральной службы по финансовым рынкам».

Инвестиционные паи паевых инвестиционных фондов, находящихся под управлением ООО «Эссет Менеджмент», предназначены для квалифицированных инвесторов.

Сообщаем, что в соответствии с пунктом 3 статьи 51 Федерального закона от 29.11.2001 № 156-ФЗ «Об инвестиционных фондах» не допускается распространение информации о паевом инвестиционном фонде, инвестиционные паи которого предназначены для квалифицированных инвесторов, за исключением случаев ее раскрытия в соответствии с данным Федеральным законом и иными федеральными законами.

Генеральный директор
ООО «Эссет Менеджмент» В.А. Голиков