ООО УК «Инсайт Кэпитал»
ОГРН 1217700414249, ИНН 9703046439
123242, г. Москва, ул. Зоологическая, д. 8, эт. 1, пом. 9
+ 7 (495) 131-11-01
www.insightcapital.ru

Уведомление клиентов о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц, не имеющим право совершать транзакции от лица клиента. Рекомендации клиентам по защите от противоправного доступа и о рисках вредоносных программ

Уведомление клиентов о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц, не имеющим право совершать транзакции от лица клиента Общества с ограниченной ответственностью Управляющая компания «Инсайт Кэпитал»[1] разработано в соответствии с требованиями Положения 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 (утверждено Банком России 20 апреля 2021 года № 757-П) и подлежит доведению до сведения клиентов Общества, путём размещения на сайте Общества в сети Интернет.

I. Уведомление о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями третьих лиц.

1. Клиенты Общества несут риски возможных финансовых потерь вследствие следующих обстоятельств:
   - получение лицами, не обладающими правом осуществления финансовых операций
   - от лица клиента, несанкционированного доступа к защищаемой информации;
   - утрата (потеря, хищение) носителей ключей электронной подписи, с использованием которых осуществляются финансовые операции;
   - воздействие вредоносного кода на электронные устройства клиента, с которых совершаются финансовые операции (персональный компьютер, ноутбук, планшет, мобильный телефон, прочие электронные устройства, далее по тексту - электронные устройства);
   - совершение в отношении клиента Общества иных противоправных действий.

2. При осуществлении финансовых операций клиентам Общества следует принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами.
   Данные риски могут возникать, помимо прочего, вследствие следующих событий:
   - кража пароля и идентификатора доступа или иных конфиденциальных данных, например, закрытого ключа, посредством технических средств и/или вредоносного

[1] далее - Уведомление и Общество соответственно

кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;

- установка на устройство вредоносного кода, который позволит злоумышленникам осуществить операции от имени клиента Общества;
- использования злоумышленником утерянного или украденного телефона для получения СМС-кодов, которые могут применяться Обществом в качестве элемента простой электронной подписи либо дополнительного способа идентификации клиента, для подтверждения несанкционированных финансовых операций;
- кража или несанкционированный доступ к устройству, с которого клиент Общества пользуется услугами Общества для получения данных и/или несанкционированного доступа к услугам с этого электронные устройства.
- получение злоумышленниками персональных данных клиента Общества, пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих конфиденциальных данных путем обмана и/или злоупотребления доверием. Описанный риск может реализоваться, в том числе, когда злоумышленник представляется сотрудником Общества или техническим специалистом или использует иную легенду и просит клиента сообщить ему указанные конфиденциальные данные или направляет поддельные почтовые сообщения с просьбой предоставить информацию или совершить действие, которое может привести к компрометации электронные устройства;
- перехват почтовых сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если электронная почта клиента используется для информационного обмена с Обществом. В случае получения доступа к электронной почте клиента, отправка сообщений Обществу от его имени.

3. Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) для доступа к информационным системам Общества несёт Владелец учётных данных. Общество не несёт ответственности в случаях финансовых потерь, понесённых клиентами в связи с пренебрежением правилами информационной безопасности.

II. Меры по предотвращению несанкционированного доступа к защищаемой информации.

1. Клиентам Общества следует предпринять все доступные меры для предотвращения несанкционированного доступа к защищаемой информации таких клиентов.
   Для указанных целей клиентам Общества следует принять, помимо прочего, следующие меры:

1.1. Обеспечение надлежащей защиты электронных устройств, с помощью которого клиенты пользуются услугами Общества и обмениваются информацией с Обществом:

- 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 электронного устройства владельцем;
- хранение и использование электронных устройств способом, исключающим риски его кражи и/или потери.
- своевременное обновление операционной системы электронных устройств;
- активация парольной или иной защиты для доступа к устройству;
- незамедлительное изменение учетных данных, используемых для доступа к услугам Общества, после удаления с электронных устройств обнаруженного вредоносного программного обеспечения;
- передача защищаемой информации клиентов только через безопасные беспроводные сети. Работая в общедоступных беспроводных сетях клиентам не следует вводить учетные данные, используемые для доступа к услугам Общества.

1.2. Обеспечение конфиденциальности защищаемой информации:

- хранение в тайне аутентификационных/идентификационных данных и ключевой информации, полученных от Общества: паролей, СМС-кодов, кодовых слов, закрытых ключей, сертификатов. В случае компрометации указанных данных клиенту следует принять меры для смены таких данных и/или уведомления Общества об их компрометации;
- соблюдение принципа разумного раскрытия информации о номерах счетов, паспортных данных, номерах кредитных и дебетовых карт, CVC/CVV кодах; в случае запроса
- у клиента указанной информации в связи с оказанием услуг Обществом, клиенту следует по возможности оценить ситуацию и уточнить полномочия отправителя запроса и процедуру раскрытия информации через независимый канал связи, например, в контакт-центре Общества.

1.3. Проявление осторожности и предусмотрительности:

- клиенту Общества следует проявлять повышенную осторожность в следующих обстоятельствах:
  - при получении электронных сообщений со ссылками и вложениями, так как они могут привести к заражению электронных устройств клиента вредоносным кодом;
  - при просмотре/работе с сайтами в сети Интернет, так как вредоносный код может быть загружен с сайта;
  - 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 заражённом вирусами и/или вредоносными программами электронном устройстве.
- следует внимательно проверять отправителя электронных сообщений. Входящее сообщение может быть от злоумышленника, который маскируется под Общество или иных доверенных лиц;
- клиентам Общества не следует заходить в системы удаленного доступа с не доверенных устройств, которые клиент не контролирует. На таких электронных

устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;

- при наличии в средствах массовой информации и на сайте Общества сведений о последних критичных уязвимостях и о вредоносном коде, клиентам рекомендуется принимать такую информацию к сведению;
- при обращении в контакт-центр Общества клиенту следует осуществлять звонок только по номеру телефона, указанному на сайте Общества в сети Интернет;
- при предоставлении клиентом доступа к устройству третьим лицам клиент несёт риск загрузки такими лицами на устройство вредоносного кода. В случае утраты электронных устройств злоумышленники могут воспользоваться им для доступа к системам Общества от лица клиента;
- при утрате телефона, используемого для получения СМС-кодов или доступа к системам Общества, клиенту необходимо совершить следующие действия:
  - проинформировать Общество по телефону контакт-центра и/или адресу электронной почты, указанным на сайте Общества в сети Интернет;
  - по возможности оперативно с учетом прочих рисков и особенностей использования телефона клиента заблокировать и перевыпустить сим-карту;
  - сменить пароль, воспользовавшись другим доверенным устройством, и/или заблокировать дистанционный доступ к услугам Общества, обратившись в Общество;
- при подозрении на несанкционированный доступ и/или компрометацию электронных устройств клиенту необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать дистанционный доступ к услугам Общества, обратившись в Общество, в отношении ключевой информации (если это уместно
- для оказываемого клиенту Обществом вида услуг - отозвать скомпрометированный закрытый ключ);
- клиенту рекомендуется использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у клиента;
- в случае выхода из строя сим карты, используемой для получения СМС-кодов, клиенту следует незамедлительно обратиться к своему сотовому оператору для уточнения причин неработоспособности сим-карты и восстановления связи.
- контактная информация, предоставленная клиентом Обществу, должна поддерживаться в актуальном состоянии для того, чтобы в случае необходимости сотрудник Общества мог оперативно связаться с клиентом.

1.4. При работе 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.

1.5. При работе с защищаемой информацией на персональном компьютере необходимо:
- устанавливать и использовать только лицензионное программное обеспечение на электронных устройствах;
- своевременно устанавливать актуальные обновления безопасности на электронные устройства;
- 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 персонального компьютера;
- использовать сложные пароли, с использованием заглавных и прописных букв, цифр и специальных знаков;
- ограничить доступ к персональному компьютеру, исключить (ограничить) возможность дистанционного подключения к персональному компьютеру третьим лицам.

1.6. При работе с мобильным устройством необходимо:
- не оставлять устройство без присмотра, чтобы исключить его несанкционированное использование;
- использовать только официальные мобильные приложения, загруженные при помощи официального магазина приложений;
- 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 Общества;
- установить на устройстве пароль для доступа к устройству.

1.7. 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.

2. При подозрении в компрометации ключей или несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов необходимо обращаться в Общество по телефону контакт-центра и/или адресу электронной почты, указанным на сайте Общества в сети Интернет.

3. Рекомендации по защите информации от противоправного доступа.
- не сообщайте посторонним лицам персональные данные или информацию через Интернет, включая логины и пароли доступа к клиентским ресурсам Общества,

историю операций, так как эти данные могут быть перехвачены злоумышленниками и использованы для получения доступа к вашим активам;

- не записывайте логин и пароль на бумаге, мониторе или клавиатуре;
- не используйте функцию запоминания логина и пароля в браузерах;
- не используйте одинаковые логин и пароль для доступа к различным системам;
- не пользуйтесь системами, требующими ввода логина и пароля, на компьютерах, которые находятся в общедоступных местах и в конфигурации, которых вы не уверены, по возможности совершайте операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и (или) информации о доступе к клиентским ресурсам Общества;
- в случае если операция совершается с использованием чужого компьютера, не сохраняйте на нем персональные данные и другую информацию, а после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились (загрузив в браузере иную web-страницу), после возвращения к своему средству доступа обязательно смените логин и пароль;
- не открывайте ссылки, указанные в сомнительном письме, в котором вас просят указать конфиденциальные данные, не звоните по телефонам, указанным в подобных письмах, и не отвечайте на них;
- не открывайте приложения к письмам от незнакомых отправителей, так как письма могут быть вирусы (вредоносное программное обеспечение), способные украсть ваши идентификационные данные и информацию;
- не используйте в качестве пароля имена, памятные даты, номера телефонов;
- при использовании простой электронной подписи не позволяйте третьим лицам производить за вас генерацию ключей;
- используйте межсетевой экран, брандмауэр, firewall, блокирующий передачу нежелательной информации;
- не храните незашифрованные личные данные на жестком диске, так как эти данные могут быть похищены злоумышленниками и использованы для получения доступа к Вашим активам;
- поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться;
- не передавайте свою личную информацию через общедоступные Wi-Fi сети, работая в общедоступных Wi-Fi сетях, желательно не вводить пароли доступа, логины;
- для обеспечения конфиденциальности операций пользуйте только защищённое соединение через HTTPS: защищённое соединение предотвращает перехват или фальсификацию передаваемых данных;
- в случае утраты устройства необходимо изменить пароли доступа к ресурсам, на которые производился вход;
- проверяйте новые файлы: будьте осторожны при получении сообщений с файлами-вложениями, обращайте внимание на расширение файла: вредоносные файлы часто маскируются под обычные графические, аудио и видео файлы: для того, чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения расширений файлов, подозрительные сообщения лучше немедленно удалять. При открытии ссылок, полученных по электронной почте, скопируйте ссылку, вставьте в адресную строку используемого браузера и убедитесь, что адрес соответствует интересующему вас ресурсу, никогда не устанавливайте и не сохраняйте без

предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Проверяйте все новые файлы, сохраняемые на компьютере, периодически проверяйте компьютер полностью, подозрительные файлы лучше немедленно удалять, особую опасность могут представлять файлы со следующими расширениями: ade, adp, bas, bat, chm, cmd, com, cpl, crt, eml, exe, hlp, hta, inf, ins, isp, jse, lnk, mdb, mde, msc, msi, msp, mst, pcd, pif, reg, scr; sct, shs, url, vbs, vbe, wsf, wsh, wsc. Если Ваше электронное устройство подверглось заражению, рекомендуется обратиться к квалифицированным IT специалистам, а также сменить пароли от доступа в кабинет, электронной почты, учётных записей в социальных сетях и т.п. с помощью не заражённого электронного устройства.

- не посещайте сайты, которые могут иметь незаконное и/или вредоносное содержание;
- проверяйте все съёмные носители информации (USB-Flash, CD/DVD-диски, карты памяти SD и т.п.) до начала их использования.
- регулярно выполняйте резервное копирование важной информации.