

Утверждено
Приказом Генерального директора
Акционерного общества
«Инвестиционная компания «Горизонт»
Приказ № 20250415-1 от 15.04.2025 г.

Рекомендации

по защите информации от воздействия программных кодов, приводящих к нарушению нормального функционирования вычислительной техники, в целях противодействия незаконным финансовым операциям

В соответствие 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» Акционерное общество «Инвестиционная компания «Горизонт» (далее по тексту - Компания) доводит до вашего сведения основные рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям. Соблюдение этих рекомендаций позволит вам снизить вероятность реализации рисков несанкционированного доступа к защищаемой информации.

Все риски, связанные с утратой и компрометацией данных для доступа к Личному кабинету клиента, к учетным записям на устройствах клиента, к самим устройствам клиента, используемым для совершения финансовых операций и/или для иного взаимодействия с Компанией, несет клиент.

Компания не несет ответственность в случаях финансовых потерь, понесенных клиентами в связи с пренебрежением настоящими рекомендациями и/или правилами информационной безопасности.

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

Несанкционированный доступ к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления может стать причиной реализации различных рисков, в том числе, но не ограничиваясь:

- ✓ риск финансовых потерь в результате совершения финансовых операций лицом, не обладающим правом их осуществления, в том числе путем отправки и формирования от имени клиента поручений на совершение финансовой операции;
- ✓ риск совершения юридически значимых действий лицом, не обладающим правом их осуществления, включая совершение операций с доступными активами, подключение и отключение услуг, внесение изменений в данные клиента, использование счетов и находящихся на них активов для прикрытия иных действий, носящих противоправный характер, совершение иных действий против воли клиента;
- ✓ риск деструктивного воздействия на носители информации и их содержимое, что в свою очередь может привести к воспрепятствованию реализации клиентом своих прав, исполнению клиентом своих обязательств или невозможности использования сервисов Компании;
- ✓ риск разглашения информации конфиденциального характера: сведений об операциях, активах, состоянии счетов, подключенных услугах, персональных данных, иной значимой информации.

Такие риски могут быть обусловлены включая, но не ограничиваясь следующими причинами:

- ✓ потеря (хищение) носителей ключей электронной подписи, с использованием которых, осуществляются критичные (финансовые) операции;
- ✓ пренебрежение клиентом мерами по предотвращению несанкционированного доступа к защищаемой информации;
- ✓ кража 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 использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;
- ✓ установка на устройство вредоносного кода, который позволит злоумышленникам осуществить критичные операции от вашего имени;
- ✓ использования злоумышленником утерянного или украденного телефона (SIM-карты) для получения СМС-кодов, которые могут применяться Компанией в качестве простой электронной подписи или дополнительной защиты для несанкционированных финансовых операций, что позволит им обойти защиту;
- ✓ кража или несанкционированный доступ к устройству, с которого вы пользуетесь услугами/сервисами Компании для получения данных и/или несанкционированного доступа к сервисам Компании с этого устройства;

- ✓ 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 Компании или техническим специалистом, или использует иную легенду и просит вас сообщить ему эти секретные данные; или направляет поддельные сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;
- ✓ перехват электронных сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если ваша электронная почта используется для информационного обмена с Компанией, или в случае получения доступа к вашей электронной почте, отправка сообщений от вашего имени в Компанию.

Меры по предотвращению несанкционированного доступа к защищаемой информации

Для снижения риска финансовых потерь необходимо обеспечить реализацию следующих мер 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. Обеспечьте защиту устройства, с которого вы пользуетесь услугами Компании, 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;
 - ✓ обеспечение защиты устройства от 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.

2. Обеспечьте конфиденциальность:

- ✓ храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Компании: 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 услугам Компании, по возможности, оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон контакт-центра Компании.

3. 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 на ваше устройство через электронную почту или интернет-ссылку, 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 Компанию 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 программным обеспечением 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 и на сайте Компании о последних критичных уязвимостях и о вредоносном коде;

- ✓ при обращении в Компанию осуществляйте звонок только по номеру телефона, указанному в договоре или на официальном сайте Компании. И имейте в виду, что от лица Компании 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 контакт-центр;
- ✓ имейте в виду, что, 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 Компании, которыми пользовались вы. В связи с этим, при утере, краже телефона или SIM-карты, используемых для получения СМС-кодов или доступа к системам Компании с мобильного приложения: 1) незамедлительно проинформировать Компанию через контактный центр, 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 Компанию; в отношении ключевой информации, если это уместно для вашей услуги – аннулировать 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;
- ✓ не отключайте и не взламывайте встроенные механизмы безопасности устройства;
- ✓ не устанавливайте и не используйте программы для удаленного управления устройством;
- ✓ 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;
- ✓ устанавливайте пароль на SIM-карту.

4. 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 не используются для работы;
- ✓ использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи/ключевым носителям, не хранить пароли открытым виде.

5. 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;
- ✓ не записывать пароли на бумажных носителях или в файлах на жестком диске вашего компьютера, не сообщать их другим лицам, в том числе знакомым, друзьям, родственникам;
- ✓ ограничить доступ к компьютеру, исключить либо ограничить возможность дистанционного подключения к компьютеру третьим лицам.

6. При обмене информацией через информационно-телекоммуникационную сеть «Интернет» необходимо:

- ✓ не использовать общедоступные сети Wi-Fi;
- ✓ 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, особенно, 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 Компанию.