

УТВЕРЖДЕНО
Приказом Директор ООО «УК «СтоунХедж»
№0107-3 от «01» июля 2022г
Мухаметзянова Р.Х.



Рекомендации
по соблюдению информационной безопасности клиентами Общества с
ограниченной ответственностью «Управляющая компания «СтоунХедж» в
целях противодействия незаконным финансовым операциям

Казань, 2022 г.

Настоящие рекомендации разработаны в соответствии с требованиями п.1.13 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».

Общество с ограниченной ответственностью «Управляющая компания «СтоунХедж» (далее по тексту - Организация) 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.

Рекомендации по соблюдению информационной безопасности (совокупности мер, применение которых направлено на непосредственное обеспечение защиты информации, процессов, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты (здесь и далее термины из ГОСТ Р 57580.1-2017) 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.

В связи с тем, что требования информационной безопасности так же могут быть отражены в договорах, регламентах, правилах и иных документах Организации, регламентирующих предоставление услуг, настоящие Рекомендации действуют в части, не противоречащей положениям внутренних документов.

В целях снижения риска реализации инцидентов информационной безопасности (ГОСТ Р 57580.1-2017) – нежелательные или неожиданные события защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов (клиента), технологических процессов организации и (или) нарушить конфиденциальности, целостности и доступности информации вследствие:

- несанкционированного доступа к вашей информации лицами, не обладающими правом осуществления значимых (критичных) операций (в т.ч. финансовых);
- 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 Вас иных противоправных действий, связанных с информационной безопасностью.

Рекомендуется соблюдать ряд профилактических мероприятий, направленных на повышение уровня информационной безопасности при использовании объектов информатизации (совокупности объектов, ресурсов, средств и систем обработки информации, в т.ч. автоматизированных систем, используемых для обеспечения информатизации бизнес-процессов (ГОСТ Р 57580.1-2017) Организации.

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

1. 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 следующими примерами:

- кража пароля и идентификатора доступа или иных конфиденциальных данных, например, 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;
- кража или несанкционированный доступ к устройству, с которого Вы пользуетесь услугами Организации для получения данных и/или несанкционированного доступа к сервисам Организации с этого устройства (при наличии таких сервисов);
- получение пароля и идентификатора доступа 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 сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;
- перехвата электронных сообщений и получения несанкционированного доступа к вашей электронной почте, отправка сообщений от вашего имени в Организацию.

2. Для снижения риска финансовых потерь:

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.

Обеспечьте конфиденциальность:

- храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Организации: пароли, 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, 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, через телефон Организации.

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 и на сайте Организации 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 пароль, кодовое слово и т.д.;
- 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 Организации, которыми пользовались Вы.
- 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.

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 открытым виде на компьютере/мобильном устройстве.

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.

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 денежных средств или иных финансовых активов необходимо незамедлительно обращаться в Организацию.

Пройито и пронумеровано и скреплено печатью
(14/1116) лист 26
Директор ООО «УК «СтоунХедж»

Мухаметзянова Р.Х.

М.П.

