УТВЕРЖДЕНО

Приказом Генерального директора
ООО ИК «Орлиная река»
_____Сливинская И. Г.
№ 05-01/20-од «09» 01 2020г.

Рекомендации
ООО ИК «Орлиная река» по информационной безопасности к ознакомлению клиентов в целях противодействия незаконным финансовым операциям.

Москва, 2020г.

В соответствие с требованиями 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» ООО ИК «Орлиная река» (далее по тексту - Организация) доводит до 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 обеспечение защиты информации, процессов, ресурсов, технического и организационного обеспечения, необходимого для применения указанных мер защиты (здесь и далее термины из ГОСТ Р 57580.1-2017) позволяют снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их корректной реализации.

В связи с тем, что требования информационной безопасности так же могут быть отражены в договорах, регламентах, инструкциях и иных документах Организации, регламентирующих предоставление услуг/сервисов, 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 информации лицами, не обладающими соответствующими правами на выполнение любых операций, предусмотренных функционалом оператора (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 иных противоправных действий, связанных с информационной безопасностью.

Рекомендуется соблюдать ряд 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)и минимизации рисков:

1) При осуществлении критичных (финансовых) операций следует принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых и иных операций, влекущие негативные последствия, лицами, не обладающими соответствующими правами, такие риски могут быть обусловлены включая, но не ограничиваясь следующими примерами:

a. Использования злоумышленником утерянного или украденного мобильного устройства (планшет, ноутбук, мобильный телефон и пр.) для доступа к личной почте субъекта, получения кодов, которые могут применяться Организацией в качестве дополнительной защиты для несанкционированных финансовых операций;
b. Получение пароля и идентификатора доступа и/или кода из направленных сообщений на электронную почту и/или кодового слова и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, в случаях использования метода социальной инженерии (злоумышленник представляется сотрудником Организации, сотрудником информационной безопасности, техническим специалистом, и иным лицом, руководствуясь нерегламентированными и неправомерными действиями/функциями сотрудника, например, с просьбой сообщить конфиденциальные данные; направляет поддельные сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, приводящее к негативным последствиям (в т.ч. финансовым). Рекомендуется проверять достоверность сотрудника, который выступает от лица Организации и, при возможности, учитывать функциональные возможности данного лица, представившегося сотрудником Организации, а также проверять контакты сотрудника (например, телефон или почтовый адрес, с которого данный сотрудник производит взаимодействие с клиентом);
c. Перехвата электронных сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если электронная почта используется для информационного обмена с Организацией. Так же в случае получения доступа к электронной почте, возможна использование и отправка сообщений от имени пользователя.

2) Для снижения риска финансовых потерь необходимо:

a. Обеспечить защиту устройства, которое используется для взаимодействия с Организацией и пользования услугами/сервисами Организации, к таким мерам включая, но не ограничиваясь могут быть отнесены:
   - Использование только лицензионного программного обеспечения (далее – ПО), полученного из доверенных источников;
   - Использование поддерживаемого производителем системного ПО;
   - Запрет на установку программ из недоверенных источников;
   - Контроль и учет установленного ПО, а также, наличие регламентированного перечня разрешенного ПО на выделенном автоматизированном рабочем месте/сервере;
   - Наличие, настройка, аудит и корректное функционирование средств защиты: Антивирусной защиты, Межсетевого экранирования, Системы обнаружения и предотвращения вторжений, Системы защиты информации от несанкционированного доступа (для корректного и достаточного построения системы защиты, как с организационной, так и с технической части, рекомендуется произвести моделирование угроз и нарушителей для дальнейшего определения необходимости в установке тех или иных средств защиты);
   - Регулярное и своевременное обновление баз средств защиты (например, регулярное обновление сигнатур антивируса и системы обнаружения и предотвращения вторжений);

- Настройка и аудит прав доступа к устройству и помещению, в котором находится устройство, с целью предотвращения несанкционированного доступа и замены/кражи компонентов устройства;
- Соблюдение корректного хранения и использования устройства с целью избежать рисков кражи, несанкционированного доступа и/или утери;
- Использование проверенных/лицензионных «билдов»/версий операционных систем (например, совместимых со средствами защиты)
- При построении системы защиты рекомендуется учитывать совместимость системного и прикладного ПО со средствами защиты.
- Использование паролей не менее 8 символов, содержащих спецсимволы, строчные и заглавные буквы, при необходимости, использование токенов, упраздняющих необходимость ручного ввода паролей, или смешанного типа идентификации и аутентификации. При смене пароля рекомендуется использовать пароль, отличающийся от предыдущего не менее чем на 3 символа.

b. Обеспечение конфиденциальности:
   - Соблюдать принцип разумного раскрытия информации о номерах счетов, паспортных данных, номерах кредитных и дебетовых карт, о CVC\CVV кодах, и иных данных, в случае если запрашивают указанную информацию, в привязке к сервисам Организации, по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон/электронную почту Организации.

c. Проявлять осторожность и предусмотрительность:
   - Рекомендуется проявлять осторожность при получении электронных писем со ссылками и вложениями, т.к. они могут привести к заражению устройства вредоносным кодом или направить на «фишинговую» страницу, замаскированную под сайт Организации, при входе в который субъект имеет вероятность активировать скрытую/открытую ссылку на скачивание и последующую активацию вредоносного кода. При занесении вредоносного кода на устройство и отсутствии эффективных антивирусных средств защиты, злоумышленник может получить доступ к любым данным и информационным системам на устройстве, а также продолжить заражение иных устройств через зараженное;
   - Рекомендуется внимательно проверять адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть направленно от злоумышленника, который маскируется под Организацию или иных доверенных лиц;
   - Рекомендуется проявлять осторожность при просмотре/работе с интернет-сайтами, так как вредоносный код может быть загружен с сайта;
   - Рекомендуется пользоваться доверенным списком интернет-ресурсов, исключая риск заражения, через иные интернет-ресурсы.
   - Рекомендуется проявлять осторожность с файлами из недоверенных источников в т.ч. архивы с паролем, зашифрованные файлы/архивы;
   - Рекомендуется избегать системы удаленного доступа с недоверенных устройств, которые не контролируются субъектом входа или доверенным администратором субъекта. На устройствах возможен вредоносный код,

собирающий идентификационные и аутентификационные, или иные данные, или способный подменить операцию;

- Рекомендуется проявлять осведомленность за информацией в прессе, информационных ресурсах о последних/актуальных уязвимостях (например, «Банк данных угроз безопасности информации ФСТЭК»);
- При взаимодействии с сервисом контакт центра Организации, рекомендуется осуществлять контакт только по номеру телефона/электронной почте, указанному(ой) в договоре или на официальном сайте Организации.
- Рекомендуется учитывать, что от лица Организации производятся звонки или сообщения, в которых от требуют передать, например, коды, пароли, номера карт, аутентификационные данные, кодовые слова.
- При компрометации аутентификационных данных или подозрении на несанкционированный доступ и/или компрометацию устройства рекомендуется сменить пароль, сообщить, при наличии, в отдел информационной безопасности, заблокировать доступ, обратившись в Организацию, в отношении ключевой информации,– отозвать скомпрометированный ключ электронной подписи/шифрования, в соответствии с правилами, отраженными в договоре, приложениях к договору и иных документах, связанных с исполнением договора;
- Рекомендуется производить резервирование данных, в виду скорейшего восстановления устройства в рабочее состояние;
- Для осуществления финансовых операций рекомендуется использовать отдельное, защищенное устройство, доступ к которому есть только у пользователя;

d. При работе на автоматизированном рабочем месте 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 средства защиты информации, рассмотренные в 5 пункте 2), а) настоящей рекомендации (межсетевые экраны и средства защиты от несанкционированного доступа, антивирусы, средства контроля конфигурации устройств и пр.), регулярно обновляя базы средств защиты;
   - Использовать сложные пароли, рассмотренные в 11 пункте 2), а);
   - Ограничить доступ к автоматизированному рабочему месту, мобильному устройству, в т.ч. в помещение, в котором находятся используемые устройства, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

e. При работе с мобильным устройствами рекомендуется:
   - Не оставлять мобильное устройство без присмотра, исключая несанкционированное использование мобильного устройства и входа в используемые сервисы/ресурсы;
   - Установить на Мобильном устройстве пароль для доступа к устройству и сервису.

f. При обмене информацией через сеть Интернет рекомендуется:

- 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/аутентификационную информацию на подозрительных сайтах и других неизвестных ресурсах;
- Ограничить посещения сайтов сомнительного содержания, используя доверенный «пул» интернет-ресурсов;
- Не сохранять пароли в памяти интернет-браузера;
- 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 аутентификационных данных доступа, несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов необходимо незамедлительно сообщить Организации.