Утвержден

Генеральным директором
АО «Прайм Брокерский Сервис»

приказ от «23» января 2023 г. № ВнД-09/09

Рекомендации по соблюдению информационной безопасности клиентами АО «Прайм Брокерский Сервис» в целях противодействия незаконным финансовым операциям.

Настоящие Рекомендации по соблюдению информационной безопасности клиентами АО «Прайм Брокерский Сервис» (далее – АО «ПБС» , Компания) в целях противодействия осуществлению незаконных финансовых операций (далее – Рекомендации) разработаны в соответствии 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» и направлены на информирование Инвесторов:

- о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- о мерах 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.

Перед заключением внимательно изучайте документы АО «ПБС», регламентирующие предоставление услуг и сервисов, ознакомьтесь с разделами, посвященными информационной безопасности. Рекомендации подлежат доведению до сведения клиентов Компании путем размещения на сайте в сети Интернет по адресу https://pbsr.ru/ и носят открытый рекомендательный характер.

Выполнение клиентом Рекомендаций 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 гарантирует обеспечение подтверждения подлинности, неизменности, конфиденциальности, целостности и доступности информации, но снижает риски информационной безопасности и направлено на минимизацию возможных негативных последствий в случае их реализации.

В связи с тем, что требования информационной безопасности так же могут быть отражены в договорах, регламентах, правилах и иных документах Компании, регламентирующих деятельность Компании и предоставление ею услуг Клиентам, настоящие Рекомендации действуют в части, не противоречащей им. В случае заключения договора с Компанией Клиентам рекомендуется внимательно изучить договор, приложения к договору и иные документы, связанные с исполнением договора, ознакомиться с разделами, посвященными информационной безопасности и конфиденциальности.

Факт безусловного ознакомления Клиентом с Условиями настоящих Рекомендаций удостоверяется подписанием со стороны Клиента Согласия на присоединение к условиям договоров в сфере брокерской и депозитарной деятельности (далее- Согласие о присоединении) либо Заявления об изменении условий акцепта Регламента сервисов на финансовых рынках и (или) Условий осуществления депозитарной деятельности, в том числе в виде электронного документа с использованием простой электронной подписи.

Под защищаемой информацией понимается:

- персональные данные Клиента;
- информация, необходимая Компании для авторизации Клиента в целях осуществления финансовых операций и удостоверения права распоряжаться денежными средствами, ценными бумагами и (или) иным имуществом;
- информация об осуществляемых финансовых операциях с активами Клиента;
- информация, содержащаяся в Договорах, отчетах и (или) иных документах, составляемых при осуществлении финансовых операций;

Основные риски получения несанкционированного доступа к защищаемой информации:

- риск несанкционированного доступа к информации лицами, не обладающими правом осуществления значимых (критичных) операций (в т.ч. финансовых);
- риск совершения финансовых операций с активами Клиента, в том числе путем формирования и отправки от имени Клиента поручения / распоряжения на проведение финансовой операции;
- риск совершения иных юридически значимых действий, включая внесение изменений в регистрационные данные Клиента, использование счетов и находящихся на них активов для противоправных действий против воли Клиента;
- риск повреждения программного обеспечения Клиента, воздействия вредоносного кода на устройства, с которых совершаются критичные (финансовые) операции, а также риск изменения, искажения, уничтожения или шифрования информации об активах или данных самого Клиента;
- риск разглашения конфиденциальной информации;
- риск совершения иных противоправных действий, связанных с информационной безопасностью.

I. Уведомление Клиента о возможных рисках несанкционированного доступа 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, CVV\CVC номера карты, ключей электронной подписи или шифрования посредством технических средств и(или) вредоносного кода; и
- использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;
- утрата, потеря (хищение) идентификатора(ов) доступа Клиента и (или) его электронной подписи, необходимых для осуществления финансовых операций;
- злоупотребление доверием клиента при совершении финансовых операций от лица клиента лицами, уполномоченными клиентом на совершение таких операций;
- установка на устройство вредоносного кода, который позволит злоумышленникам осуществить критичные операции от имени Клиента.
- 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, утрата Клиентом контроля за устройством с которого он пользуется услугами и(или) 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.
- перехвата электронных сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если электронная почта Клиента используется для информационного обмена с Компанией или в случае получения доступа к электронной почте Клиента при отправке сообщений от имени Клиента в Компанию.

II. Риски, напрямую не влекущие финансовые потери:

- разглашение неопределённому кругу лиц персональных данных и иной конфиденциальной информации Клиента;
- репутационный риск Клиента;
- риски, связанные с нарушением законодательства действиями, произведёнными от имени Клиента;
- репутационный риск Компании.

III. Для снижения риска финансовых потерь рекомендуется:

- Обеспечить защиту устройства, с которого Клиент пользуетесь услугами Компании, к таким мерам включая, но не ограничиваясь могут быть отнесены:
    a) использование только лицензионного программного обеспечения, полученного из доверенных источников. Необходимо ввести запрет на установку программ из непроверенных источников;
    b) наличие средства защиты, таких как: антивирус, с регулярно и своевременно обновляемыми базами), персональный межсетевой экран, настройка прав доступа Клиента к устройству с целью предотвращения несанкционированного доступа. Хранение, использование устройства с целью избежать рисков кражи и/или утери. Своевременные обновления операционной системы в части обновлений безопасности, обновления снижают риски заражения вредоносным кодом. Активация парольной или иной защиты для доступа к устройству.
- Обеспечить конфиденциальность:
    a) хранить в тайне аутентификационные и(или)идентификационные данные и ключевую информацию, полученные от Компании: пароли, СМС коды, кодовые слова, ключи

электронной подписи (шифрования), в случае компрометации незамедлительно контактировать с Компанией для смены и (или) блокировки.

b) соблюдать принцип разумного раскрытия информации о номерах счетов, о паспортных данных Клиента, о номерах кредитных или дебетовых карт, о CVC\CVV кодах, в случае если третьи лица запрашивают указанную информацию, в привязке к сервисам Компании необходимо уточнять полномочия и процедуру через независимый канал Компании, например, телефон контакт центра Компании.

- проявлять осторожность и предусмотрительность при получении электронных писем со ссылками и вложениями, которые могут привести к заражению устройства Клиента вредоносным кодом. Вредоносный код, попав в устройство через электронную почту или интернет-ссылку на сайт, может получить доступ к любым данным и информационным системам на устройстве. Необходимо проверять адресата, от которого пришло электронное письмо. вредоносный код может быть загружен с сайта, необходимо проверять осторожность при работе с интернет-сайтами, а также при просмотре/работе 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 заходить в системы удаленного доступа с недостоверных и(или) неизвестных устройств, которые Клиент не контролирует. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа, способные подменить операцию.
- следить за информацией на сайте Компании и(или) других информационных источниках о последних критичных уязвимостях и о вредоносном коде.
- при наличии в рамках продукта Клиента необходимости совершать звонки в колл центр Компании необходимо использовать только контакты, указанные в Договоре или на официальном сайте АО «ПБС» в сети Интернет https://pbsr.ru/.
- необходимо понимать, что от лица Организации не могут поступать звонки или сообщения, в которых от Клиента требуют передать СМС-код, пароль, номер карты, кодовое слово и т.д.
- в случае, если Клиент передает принадлежащий ему телефон и/или устройство другим пользователям, они могу установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам Компании, которыми пользуются Клиент.

В связи с этим при утере, краже телефона (SIM карты), используемого для получения СМС кодов необходимо:

a) незамедлительно проинформировать Компанию через службу поддержки Клиентов ;

b) целесообразно 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 – отозвать скомпрометированный ключ электронной подписи (шифрования), в соответствии с правилами, отраженными в договоре, приложениях к договору и иных документах, связанных с исполнением договора и соблюдением конфиденциальности. Наличие «эталонной» резервной копии может облегчить и ускорить восстановление устройства Клиента. Лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у Клиента, с этой целью необходимо контролировать 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.

- При работе с ключами электронной подписи необходимо использовать специальные защищенные носители ключевой информации (ключевые носители), например: e-token, смарт-карта и т.п., не оставлять без присмотра и не передавать третьим лицам ключевые носители, 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.

При работе на компьютере необходимо:

- использовать лицензионное программное обеспечение (операционные системы 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 работе с мобильным приложением не оставлять Мобильное устройство без присмотра с целью исключения несанкционированного использования Мобильного приложения.
- использование только официального мобильного 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 АО «ПБС».

Установить на Мобильном устройстве пароль для доступа к устройству и приложению.

c) 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 Компанию .