Рекомендации Клиенту для обеспечения безопасности информации

Акционерное Общество «Профессиональная депозитарная компания» (далее – Общество) в целях соблюдения требований Положение Банка России от 20.04.2021 N 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" **уведомляет** клиентов Общества о возможных рисках получения несанкционированного доступа к защищаемой информации:

1. Доступ со стороны третьих лиц может повлечь за собой риски разглашения информации конфиденциального характера: сведений об операциях, активах, состоянию счетов, подключенных услугах, персональных данных и иной значимой информации.

2. Доступ со стороны третьих лиц может повлечь за собой совершение юридически значимых действий, включая: совершение операций с доступными активами, подключение и отключение услуг (в том числе платных), внесение изменений в регистрационные данные клиента, использование счетов и находящихся на них активов для прикрытия иных действий, носящих противоправный характер, совершения иных действий против воли клиента.

3. Доступ со стороны третьих лиц может повлечь за собой деструктивное воздействие на носители информации и их содержимое, что в свою очередь может привести к воспрепятствованию своевременного исполнения своих обязательств по договору или невозможности использования сервисов компании для реализации своих намерений.

В рамках защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям, а также для предотвращения 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, Общество **рекомендует** следующее:

1. Рекомендации по защитным мерам для компьютера

– На компьютере необходимо использовать только лицензионное системное и прикладное программное обеспечение.

– На компьютере должна быть установлена только одна операционная система.

– Доступ к изменению настроек должен быть защищен паролем.

– Рекомендуется своевременно проводить обновления системного и прикладного программного обеспечения.

– В обязательном порядке должны быть установлены и регулярно обновляться антивирусные программы (например, Kaspersky, Dr.Web, Symantec, Avira, ESET, NOD 32, McAfee). Отдавайте предпочтение российским разработчикам. Рекомендуется установить по умолчанию максимальный

уровень политик безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов и другого вредоносного программного обеспечения.

– Локальными (или доменными) политиками на компьютере рекомендуется ограничить список пользователей, имеющих возможность входа в операционную систему.

– Не устанавливать и не использовать на компьютере программы для удаленного управления (Например, RDP, TeamViewer, Radmin, Ammyy Admin др.).

– Для доступа к информационным системам не используйте общедоступные компьютеры (например, установленные в интернет-кафе, гостинице), публичные беспроводные сети (бесплатный Wi-Fi и прочее).

2. Рекомендации по защитным мерам для мобильного устройства

– Устанавливать Приложения на мобильное устройство можно только из официальных репозиториев производителей мобильных платформ: AppStore и Google Play.

– Установите на мобильное устройство антивирус и своевременно его обновляйте.

– Своевременно устанавливайте обновления безопасности операционной системы.

– Не взламывайте свой телефон (например, через Jailbreaking, реинжиниринг, принудительное получение root-прав), так как это отключает защитные механизмы, заложенные производителем мобильной платформы. В результате ваш телефон становится уязвимым к заражению вирусным программным обеспечением.

– Не отключайте и не взламывайте встроенные механизмы безопасности вашего устройства.

– При наличии технической возможности включите шифрование данных на своём устройстве.

– Сохраняйте в тайне Ваши имя пользователя (логин), пароль для доступа в информационные системы и СМС-коды. Не сообщайте эти данные никому.

3. Рекомендации по парольной защите

Учетные записи операционной системы должны быть защищены паролями с учётом следующих параметров:

– Использовать сложные пароли, включающие в себя комбинацию цифр, букв и специальных символов.

– Не рекомендуется пользоваться одинаковыми паролями на разных сайтах и сервисах.

– В качестве пароля не следует использовать имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе.

– В качестве пароля не следует использовать повторяющуюся комбинацию из нескольких символов, либо комбинацию символов, набираемых в закономерном порядке.

– Не сохранять своих логинов и паролей на чужих компьютерах (выходить их всех аккаунтов и личных кабинетов).

– Пароль должен меняться не реже 1 раза в 3 месяца, а также при компрометации (или подозрении в компрометации) пароля.

– При смене пароля новый пароль не должен совпадать с ранее используемыми паролями.

– Запрещено произносить вслух, записывать и хранить в любом доступном посторонним лицам месте пароли.

– Не храните логин и пароль в мобильном телефоне, смартфоне.

– Не пользоваться конфиденциальной информацией через общедоступные сети WiFi, не пересылать через них пароли и данные от аккаунтов.

4. Рекомендации по эксплуатации внешнего ключевого носителя

– Для повышения уровня безопасности хранения ключей электронной подписи (далее - ЭП) внешний ключевой носитель должен храниться только у тех лиц, которым он принадлежит.

– Во время работы с внешним ключевым носителем доступ к ним посторонних лиц должен быть исключен.

– Уничтожение ключей ЭП может производиться путем физического уничтожения внешнего ключевого носителя, на котором они расположены, или путем стирания без повреждения внешнего ключевого носителя (для обеспечения возможности его многократного использования).

– В случае компрометации или подозрения на компрометацию ключа ЭП Клиент, Владелец Квалифицированного сертификата, прекращает обмен электронными документами с использованием скомпрометированного ключа и незамедлительно информирует Удостоверяющий центр о компрометации посредством любого вида связи с целью блокировки ключа ЭП.

К компрометации ключей можно отнести следующие события: утрата ключевого носителя (в том числе с последующим обнаружением); хищение; несанкционированное копирование; передача ключевой информации по каналам связи в открытом виде; увольнение сотрудников, имевших доступ к ключевой информации; любые другие виды разглашения ключевой информации, в результате которых ключи могут стать доступны лицам, к ним не допущенным.

5. Работа с сообщениями

– Не отвечайте на сообщения, требующие предоставить, подтвердить или уточнить вашу конфиденциальную информацию: пароли, логины, фамилию, имя, отчество, паспортные данные, номер мобильного телефона, на который поступают одноразовые пароли и другие данные.

– Не открывайте подозрительные файлы, поступившие Вам по электронной почте.

– Не отвечайте на полученное подозрительное сообщение и не переходите по ссылкам, указанным в сообщении.

– Не пересылать конфиденциальную информацию в сообщениях мессенджеров, чатах и электронной почте.