Рекомендации клиенту – пользователю информационной системы, в которой осуществляется выпуск цифровых финансовых активов, по защите информации

В соответствии с требованиями п.1.13 Положения Банка России от 20.04.2021г. 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» Общество с ограниченной ответственность «Лайтхаус» информирует своих Клиентов – пользователей информационной системы, в которой осуществляется выпуск цифровых финансовых активов, о возможных рисках получения несанкционированного доступа к защищаемой информации.

В результате несанкционированного доступа к защищаемой информации с целью осуществления финансовых и иных операций, лицами, не обладающими правом их осуществления, могут возникать следующие риски и негативные последствия:

1) риски разглашения информации конфиденциального характера: сведений об операциях, активах, состоянию расчетов, персональных данных и иной значимой информации.

2) совершение операций с доступными активами, внесение изменений в регистрационные данные клиента, использование информационной системы и учитываемых в ней активов для прикрытия действий, носящих противоправный характер, совершения действий против воли клиента – пользователя информационной системы.

3) деструктивное воздействие на носители информации и их содержимое, что в свою очередь может привести к невозможности использования клиентом сервисов информационной системы.

В целях предотвращения рисков, связанных с получением несанкционированного доступа к защищаемой информации, в том числе при утрате клиентом – пользователем информационной системы устройства, с использованием которого совершались действия по осуществлению финансовых операций, и своевременному обнаружению воздействия вредоносного кода, рекомендуем принять к сведению следующие способы защиты устройства (персонального компьютера), используемого для работы с информационной системой, в которой осуществляется выпуск цифровых финансовых активов:

- Используйте для работы с информационной системой отдельное устройство (персональный компьютер или ноутбук), не используемое Вами для иных целей, кроме работы с информационной системой;

- Не допускайте к работе с устройством иных пользователей, чем Вы сами; локальными (или доменными) политиками на устройстве ограничьте список пользователей, имеющих возможность входа в операционную систему;

- Обязательно используйте современные и актуальные методы блокировки устройства;

- Храните устройство таким образом, чтобы исключить возможность его хищения и несанкционированного использования;

- Устанавливайте надежные пароли. 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. Также в качестве пароля не следует использовать комбинацию символов, набираемых в закономерном порядке;

• При утере устройства не используйте на новом устройстве прежние пароли (смените пароль доступа);

• Устанавливайте на устройстве только одну операционную систему;

• Устанавливайте обновления безопасности программного обеспечения Вашего устройства; Применяйте и регулярно обновляйте антивирусные программы (например, Kaspersky) с предпочтением установки по умолчанию максимального уровня политики безопасности (когда не требуется ответов пользователя при обнаружении вирусов и другого вредоносного программного обеспечения), а также используйте встроенные средства межсетевого экранирования (брандмауэр);

• Используйте только лицензионное системное и прикладное программное обеспечение;

• Не устанавливайте и не используйте на устройстве программы для удаленного управления (например, RDP, TeamViewer, Radmin, Ammyy Admin и др.).

• Не осуществляйте доступ к информационной системе, находясь с устройством в местах общего пользования (например, в интернет-кафе, гостинице, вокзале, аэропорту, метрополитене) и используя публичные беспроводные сети (бесплатный Wi-Fi);

• При эксплуатации устройства не посещайте и не вводите конфиденциальную информацию на неофициальных, подозрительных Интернет-ресурсах;

• Не разглашайте конфиденциальную информацию по телефону или электронной почте, которая может повлечь несанкционированный доступ к устройству, конфиденциальной информации или финансовым операциям;

• Для повышения уровня безопасности при работе с информационной системой используйте усиленный ключ электронной подписи (далее - УКЭП); УКЭП должен храниться только у Вас, и доступ к нему посторонних лиц должен быть исключен;

• Уничтожение УКЭП может производиться Вами путем физического уничтожения внешнего ключевого носителя, на котором он расположен, или путем стирания без повреждения внешнего ключевого носителя (для обеспечения возможности его многократного использования);

• В случае компрометации или подозрения на компрометацию УКЭП необходимо прекратить обмен электронными документами с использованием скомпрометированного ключа и незамедлительно информировать Удостоверяющий центр о компрометации посредством любого вида связи с целью блокировки ключа. 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; любые другие виды разглашения ключевой информации, в результате которых ключи могут стать доступны лицам, к ним не допущенным;

• Не отвечайте на звонки, требующие предоставить, подтвердить или уточнить вашу конфиденциальную информацию: пароли, логины, фамилию, имя, отчество, паспортные данные, номер мобильного телефона и т. п.;

• Не открывайте подозрительные файлы, поступившие Вам по электронной почте, не отвечайте на получаемые подозрительные сообщения и не переходите по ссылкам, указанным в сообщениях (к подозрительным относятся сообщения неизвестных Вам лиц и представителей организаций);

Всегда помните, что от Вашей внимательности, осторожности и осведомленности зависит Ваша безопасность в цифровом мире!