УТВЕРЖДЕНО

Приказом Генерального директора
Общества с ограниченной ответственностью
«Эссет Менеджмент Солюшнс»
№ 20012001-од от 20.01.2020

_____/Д.В. Горин/

# Рекомендации по соблюдению информационной безопасности клиентами

# Общества с ограниченной ответственностью

# «Эссет Менеджмент Солюшнс»

# в целях противодействия незаконным финансовым операциям

Москва, 2020 г.

В соответствии с требованиями Положения Банка России 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» Общество с ограниченной ответственностью «Эссет Менеджмент Солюшнс» (далее – Управляющая компания) уведомляет своих клиентов о возможных рисках, связанных с получением третьими лицами несанкционированного доступа к защищаемой информации:

- Несанкционированный доступ к устройствам (т.е. любому техническому средству, включая, но, не ограничиваясь, компьютер, ноутбук, планшет, мобильный телефон, с помощью которого клиент может взаимодействовать с Управляющей компанией (далее – Устройства), влечет риск получения третьими лицами несанкционируемого доступа к защищаемой информации.
- Несакционированный доступ со стороны третьих лиц к защищаемой информации может повлечь за собой риски разглашения конфиденциальной информации: персональных данных клиента, сведений об операциях, о состоянии счета, другой значимой информации.
- Несакционированный доступ со стороны третьих лиц к защищаемой информации может повлечь совершение такими третьими лицами юридически значимых действий, включая, но, не ограничиваясь, совершение финансовых операций от имени клиента, изменений регистрационных данных клиента, и иных действий, совершенных без воли клиента, и направленных против его интересов.

Доводим до сведения своих клиентов рекомендации по соблюдению информационной безопасности:

**Обеспечение безопасности устройства:**

- Блокировать устройства после использования. Использовать настройки устройства, требующие ввода пароля для его разблокировки и использования.
- Не передавать третьим лицам и не оставлять устройства без присмотра.

**Использование программного обеспечения на Устройствах:**

- Использовать на устройствах антивирусное программное обеспечение (ПО), поддерживать версию антивирусного ПО и входящих в его состав баз вирусных определений в актуальном состоянии.
- Регулярно проводить полную проверку устройства на вирусы и вредоносный код.
- Прекратить использование устройства в случае обнаружения вирусов и вредоносного кода, до момента полного удаления вирусов и вредоносного кода.

**Использовать на Устройствах исключительно лицензионное ПО и операционные системы.**

- Регулярно устанавливать обновления безопасности ПО и операционной системы, используемых на Устройствах.
- Не использовать на Устройствах ПО неизвестных разработчиков, которые не гарантируют отсутствие скрытых возможностей по сбору информации с устройств.
- Исключить использование средств удаленного администрирования на Устройствах.

**Безопасность паролей:**

- Выбирать пароли самостоятельно. Проводить регулярную смену паролей.
- Использовать сложные пароли, требующие ввода заглавных и прописных букв, цифр и специальных символов, в общем количестве не менее 8 символов. Не рекомендуется в качестве паролей использовать имена близких лиц, домашних животных, даты рождения и т.п., которые могут быть легко подобраны злоумышленниками.
- Не сохранять пароли в текстовых файлах на Устройстве либо иных электронных носителях.
- Не хранить пароль совместно с Устройством.
- Не передавать третьим лицам пароли, коды доступа к Устройству.

**Соблюдение правил безопасности в сети Интернет:**

- При работе с Устройств в сети Интернет удостовериться в том, что сертификат безопасности сайта действителен, а соединение происходит в защищенном режиме (адресная строка браузера начинается с https, либо используется значок в виде замка).
- При наличии на Устройстве программ фильтрации сетевого трафика (брандмауэра) держать его включённым и блокировать все незнакомые или подозрительные подключения.
- Не отвечать на подозрительные сообщения, полученные с неизвестных адресов.
- Не устанавливать и не сохранять подозрительные файлы, программы, полученные из ненадежных источников, скаченные с неизвестных сайтов в сети Интернет, присланные с неизвестных адресов электронной почты.
- Не открывать и не использовать сомнительные Интернет - ресурсы на Устройстве.

**Осуществление контроля подключения:**

- Не работать с Устройств, использующих подключение к общедоступной wi-fi сети.

**Дополнительные рекомендации:**

- Для связи с Управляющей компанией по телефону и e-mail необходимо использовать контактные данные, указанные на официальном сайте Управляющей компании в сети Интернет.