

**Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям Общества с ограниченной ответственностью Управляющая компания «АКТИВЫ ЮГА»**

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» (далее - Рекомендации). Общество с ограниченной ответственностью Управляющая компания «АКТИВЫ ЮГА» (далее – Управляющая компания, Общество) осуществляет свою деятельность на основании лицензии по управлению инвестиционными фондами, паевыми инвестиционными фондами, и негосударственными пенсионными фондами. Осуществление указанной деятельности связано с накоплением, систематизацией и управлением информации, в том числе и информацией ограниченного доступа, являющейся важнейшим активом Управляющей компании, и зависит от обеспечения информационной безопасности.

Настоящие Рекомендации направлены на повышение уровня информационной безопасности при использовании объектов информатизации Общества.

Общество принимает необходимые и достаточные меры по защите информации, в том числе в соответствии с требованиями законодательства Российской Федерации, чтобы обезопасить информацию и активы клиентов, учитываемые в информационных системах Общества. Вместе с тем Общество полагает необходимым проинформировать клиентов о наличии рисков несанкционированного доступа к защищаемой информации, обрабатываемой на средствах вычислительной техники (в том числе в связи с потерей, хищением таких средств), реализация которых может привести к следующим негативным потенциальным последствиям:

- совершение юридически значимых действий от имени клиента против его воли: например, операции с активами, внесение изменений в регистрационные данные клиента, иные противоправные действия;
- разглашение информации конфиденциального характера, например, персональных данных, сведений о состоянии активов или операциях клиента;
- нарушение функционирования средств вычислительной техники и привычного режима взаимодействия с Обществом.

Общество рекомендует применять нижеперечисленные меры по обеспечению информационной безопасности, в том числе при использовании средств вычислительной техники (далее - устройство) для хранения и/или обработки защищаемой информации.

1. Организуйте использование устройства таким образом, чтобы исключить возможность его несанкционированного использования, в том числе исключить несанкционированный физический и логический (программный) доступы.

2. Организуйте использование устройства с минимальными, пользовательскими правами доступа, в том числе ограничив применение административных привилегий.

3. По возможности ограничьте использование устройства только для целей, связанных с осуществлением финансовой деятельности, в том числе избегайте установки программного обеспечения (далее - ПО), которое не связано с такой деятельностью.

4. Используйте на устройстве только лицензионное ПО, полученное из достоверных источников (например, официальный сайт производителя ПО).

5. Применяйте средства защиты информации, в том числе антивирусное ПО, персональные межсетевые экраны и средства защиты от несанкционированного доступа, средства контроля конфигурации устройств.

6. Своевременно устанавливайте обновления ПО, особенно те, которые связаны с устранением уязвимостей в ПО устройства.

7. Храните в тайне криптографические ключи и другую информацию для Вашей информационной обмена с Обществом, в том числе используйте съемные носители информации со встроенными средствами защиты от несанкционированного доступа.

8. Осуществляйте регулярный контроль состояния Ваших активов на предмет подозрительных и/или несанкционированных операций с ними.

9. При подозрении в компрометации ключей электронной подписи/шифрования или несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов незамедлительно обращайтесь в Общество.

10. Используйте сложные парольные фразы, состоящие из более чем девяти символов разных типов (цифры, строчные и прописные буквы, специальные символы).

11. Обновляйте пароль каждые пять месяцев, а также при каждом подозрении на компрометацию.

12. По возможности установите пароль на доступ в базовую систему ввода-вывода (BIOS) устройства и к жестким дискам, на которых сохранена операционная система и защищаемая информация.

13. Отключите возможность удаленного пользовательского и административного доступа к устройству.

14. При работе с электронной почтой ограничьте просмотр только ожидаемыми сообщениями из доверенных источников, в том числе использование вложенных ссылок и файлов. При необходимости до открытия вложенной ссылки или файла предварительно проверяйте их с помощью специализированных средств (например, интернет-сайт для проверки ссылки и файла).

15. При работе с интернет-сайтами также придерживайтесь ограничения по открытию размещенных ссылок, файлов и рекламных баннеров, а также помните про рекомендацию №3.

16. Ограничьте введение персональной и/или защищаемой информации только с использованием проверенного и известного Вам оборудования (устройств) и только на доверенных сетевых ресурсах.

17. Проявляйте осторожность и помните о существовании методов социальной инженерии, которые могут быть использованы недобросовестными третьими лицами для получения защищаемой информации и доступа к Вашим активам.

18. Поддерживайте и повышайте собственную осведомленность об информационной безопасности, в том числе ознакомьтесь с рекомендациями Банка России на их официальном сайте.

Обращаем Ваше внимание, что сотрудники Общества могут связываться с Вами только с номеров телефонов, указанных в Вашем договоре, либо на сайте Общества.

При любом подозрении в компрометации данных, клиенту необходимо незамедлительно обратиться в Общество.

Будьте бдительны и соблюдайте правила должной осмотрительности.