Общество с ограниченной ответственностью
«РСХБ Управление Активами»
(ООО «РСХБ Управление Активами»)

УТВЕРЖДЕНЫ
Приказом Генерального директора
ООО «РСХБ Управление Активами»
от 12.05.2026 № 108-ОД

Рекомендации
для клиентов ООО «РСХБ Управление Активами» по защите информации

Москва

1. Общие рекомендации

Данные 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 - Положение Банка России от 20.04.2021 № 757-П). Рекомендации 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 гарантируют обеспечение конфиденциальности, целостности и доступности информации, но позволяют в целом снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации. В связи с тем, что требования информационной безопасности также могут быть отражены в договорах, регламентах, правилах и иных документах ООО «РСХБ Управление Активами» (далее – Общество), регламентирующих предоставление услуг/сервисов, настоящие Рекомендации действуют в части, не противоречащей положениям внутренних документов.

Общество в рамках исполнения требований Положения Банка России от 20.04.2021 № 757-П информирует клиентов о возможных рисках несанкционированного доступа к защищаемой информации:

1. Риск воздействия программных кодов, приводящего к нарушению штатного функционирования средства вычислительной техники.

2. Риск несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

3. Риск разглашения конфиденциальной информации (состояние счетов, история финансовых операций, персональные данные и другая конфиденциальная информация).

4. Риск совершения третьими лицами от имени клиента, но против его желания, значимых действий, таких как: подача заявок на приобретение/обмен/погашение паёв, изменение регистрационных данных клиента, получение третьими лицами несанкционированного доступа к персональным данным и значимой защищенной информации конфиденциального характера, а также их разглашения, совершение злоумышленниками юридически значимых действий: операций с имуществом, подключения и отключения услуг (в том числе платных), внесение изменений в регистрационные данные, использование ваших счетов и находящегося на них имущества для прикрытия каких-либо действий, носящих противоправный характер, и совершение иных действий против вашей воли и других лиц. Совершение иных действий, которые могут повлечь нарушение информационной безопасности.

5. Риск повреждения либо изменения защищаемой информации.

6. Риск потери (хищения) средств вычислительной техники (ноутбуков, планшетов, телефонов), с использованием которых осуществляются критичные операции при взаимодействии с Обществом.

7. Риск получения 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 работником Общества или техническим специалистом и/или использует иную легенду и просит Вас сообщить ему эти конфиденциальные 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.

Вышеуказанные риски могут реализоваться как с использованием вредоносных кодов и программ (вирусов) на Вашем ноутбуке, планшете, телефоне, так и вследствие обмана со стороны мошенников, которые могут пытаться различными способами узнать от Вас пароли, коды доступа и другую конфиденциальную информацию.

Для минимизации вероятности реализации вышеуказанных рисков, а также в целях защиты от вредоносного кода, рекомендуем Вам:

1. Использовать антивирусное программное обеспечение (далее - ПО) и поддерживать его актуальность. Необходимо устанавливать ПО, регулярно обновлять его версии и базы вирусных определений. При обнаружении вирусов или вредоносного кода следует немедленно прекратить использование устройства до полного удаления угроз.

2. Регулярно обновлять ПО и операционную систему. Важно своевременно устанавливать все доступные обновления безопасности для операционной системы и программного обеспечения, используемого при взаимодействии с Обществом.

3. Избегать установку ПО от неизвестных разработчиков. Не следует использовать программы, которые не гарантируют отсутствие скрытых возможностей по сбору информации с устройства Используйте только лицензионное программное обеспечение.

4. Контролировать конфигурацию устройства. Необходимо следить за изменениями в настройках устройства, с которого совершаются финансовые операции. При обнаружении подозрительных изменений следует немедленно сообщить об этом Обществу.

5. Использовать надёжные пароли. Пароли должны быть сложными, включать заглавные и строчные буквы, цифры и специальные символы, иметь длину не менее 12 символов. Периодически следует проводить смену паролей. Не рекомендуется использовать в качестве паролей имена близких, даты рождения и другие легко угадываемые данные. Пароли не следует сохранять в текстовых файлах, на электронных носителях или совместно с устройством, а также передавать третьим лицам. Не рекомендуется использовать одинаковые пароли для доступа к различным системам. Также использование двухфакторной аутентификация существенно повышает уровень защиты вашего аккаунта, защищает при утечке пароля, препятствует несанкционированному доступу, при попытке взлома позволяет своевременно проинформировать владельца о несанкционированной попытке входа.

6. Проверять безопасность соединений. При работе в интернете нужно убедиться, что сертификат безопасности сайта действителен, а соединение происходит в защищённом режиме (адресная строка браузера начинается с HTTPS, используется значок замка).

7. Избегать подозрительные сообщения и файлы. Не стоит отвечать на сообщения, направленные с неизвестных адресов, устанавливать или сохранять

подозрительные файлы и программы, полученные из ненадёжных источников, а также открывать сомнительные интернет-ресурсы.

8. Не использовать общедоступные Wi-Fi сети. Для работы с финансовыми операциями не следует подключаться к публичным или незащищённым беспроводным сетям.

9. Использовать для взаимодействия с Обществом только официальные каналы связи. Используйте для связи с Обществом контактные данные, указанные на его официальном сайте и в Вашем личном кабинете, а не в подозрительных сообщениях или на сторонних ресурсах.

10. Немедленно сообщать о потере или хищении устройства. Если устройство, с которого совершались финансовые операции, утеряно или похищено, необходимо незамедлительно сообщить об этом Обществу.

11. Проверять реквизиты и не сообщать третьим лицам информацию, полученную для проведения финансовой операции в СМС-сообщениях;

12. Не разглашать, в том числе посредством средств связи (по телефону или электронной почте) информацию, если это может повлечь несанкционированный доступ к системам, конфиденциальной информации или финансовым операциям;

13. Соблюдать принцип разумного раскрытия идентификационных данных, в том числе персональных данных. В случае получения клиентом запроса указанной информации в связи с оказанием услуг Обществом, клиенту рекомендуется оценить ситуацию и уточнить полномочия запрашивающего лица и процедуру предоставления запрашиваемой информации через независимый канал связи).

Если у Вас появились подозрения на то, что Ваши пароли стали кому-либо известны, необходимо как можно скорее изменить их.

В случае попытки реализации вышеуказанных рисков необходимо сообщить о факте Обществу по адресу электронной почты: info@rshb-am.ru.

Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) для доступа к личному кабинету и электронной почте клиента, несет клиент. Клиент несет ответственность за финансовые потери, возникшие в связи с пренебрежением правилами информационной безопасности.