Утверждено
Приказом АО «РДЦ ПАРИТЕТ»
№ 25.03.24/01 от «25» марта 2024 г.

Рекомендации по информационной безопасности клиентам АО «РДЦ ПАРИТЕТ»

Общие положения

1.1. В соответствии с требованиями Положения Банка России от 20 апреля 2021 г. № 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" уведомляем своих клиентов о возможных рисках, связанных с получением третьими лицами несанкционированного доступа к защищаемой информации:

1.2. 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.

1.3. 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.

1.4. 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.

1.5. Доводим до сведения своих клиентов рекомендации по соблюдению информационной безопасности:

Использование программного обеспечения на Устройствах:

2.1. Использовать на Устройствах антивирусное программное обеспечение (ПО), поддерживать версию антивирусного ПО и входящих в его состав баз вирусных определений в актуальном состоянии.

2.2. Регулярно проводить полную проверку Устройств на вирусы и вредоносный код.

2.3. 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:

3.1. Регулярно устанавливать обновления безопасности ПО и операционной системы, используемых на Устройствах.

3.2. Не использовать на Устройствах ПО неизвестных разработчиков, которые не гарантируют отсутствие скрытых возможностей по сбору информации с устройств.

3.3. Исключить использование средств удаленного администрирования на Устройствах.

Безопасность паролей:

4.1. Выбирать пароли самостоятельно. Проводить регулярную смену паролей.

4.2. 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.

4.3. Не сохранять пароли в текстовых файлах на Устройстве либо иных электронных носителях.

4.4. Не хранить пароль совместно с Устройством.

4.5. Не передавать третьим лицам пароли, коды доступа к Устройству.

Соблюдение правил безопасности в сети Интернет:

5.1. 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).

5.2. При наличии на Устройстве программ фильтрации сетевого трафика (брандмауэра) держать его включённым и блокировать все незнакомые или подозрительные подключения.

5.3. Не отвечать на подозрительные сообщения, полученные с неизвестных адресов.

5.4. 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.

5.5. Не открывать и не использовать сомнительные Интернет - ресурсы на Устройстве.

5.6. При работе с интернет-сервисами АО «РДЦ ПАРИТЕТ» использовать функции двухфакторной авторизации с помощью личного телефона.

Осуществление контроля подключения:

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

Дополнительные рекомендации:

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