УТВЕРЖДЕНЫ
Приказом № 2 от 03.03.2025 г.
Президента ООО «УК «МАРТА»

РЕКОМЕНДАЦИИ ПО СОБЛЮДЕНИЮ КЛИЕНТАМИ ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «УПРАВЛЯЮЩАЯ КОМПАНИЯ «МАРТА» ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В соответствии с требованиями Положение 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» Общество с ограниченной ответственностью «Управляющая компания «МАРТА» (далее – Управляющая компания) доводит до сведения своих Клиентов основные рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям.

Клиенты Управляющей компании несут риски возможных финансовых потерь вследствие следующих обстоятельств:

- ✓ получение лицами, не обладающими правом осуществления финансовых операций от лица клиента, несанкционированного доступа к защищаемой информации;
- ✓ утрата (например, вследствие хищения) носителей информации, ключей электронной подписи, с использованием которых осуществляется взаимодействие с Управляющей компанией;
- ✓ воздействие вредоносного кода на устройства клиента, с которых совершаются финансовые операции или осуществляется взаимодействие с Управляющей компанией (персональный компьютер, планшет, мобильный телефон и т.д., далее – устройство);
- ✓ совершение в отношении клиента иных противоправных действий.

При взаимодействии с Управляющей компанией и осуществлении операций клиентам следует принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления ими несанкционированных операций с имуществом клиентов. Такие риски могут возникать, помимо прочего, вследствие следующих событий:

- ✓ кража пароля и идентификатора доступа или иных конфиденциальных данных, с помощью технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;
- ✓ установка на устройство вредоносного кода, который позволит злоумышленникам осуществить операции от имени клиента Управляющей компании;
- ✓ кража или несанкционированный доступ к устройству, с которого клиент может пользоваться услугами Управляющей компании для получения данных и/или несанкционированного доступа к услугам с этого устройства;

- ✓ несанкционированное получение злоумышленниками персональных данных клиента. Риск может реализоваться, помимо прочего, когда злоумышленник представляется сотрудником Управляющей компании или техническим специалистом, или использует иную легенду и просит клиента сообщить ему конфиденциальные данные или направляет поддельные почтовые сообщения с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;
- ✓ перехват почтовых сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если электронная почта клиента используется для информационного обмена с Управляющей компанией. В случае получения доступа к почте клиента - отправка сообщений Управляющей компании от его имени.

Риски, связанные с утратой и компрометацией данных, в связи с пренебрежением правилами информационной безопасности, несет владелец данных.

Клиентам Управляющей компании рекомендуется предпринимать все доступные меры для предотвращения несанкционированного доступа к защищаемой информации.

Обеспечение надлежащей защиты устройства, с помощью которого клиенты пользуются услугами Управляющей компании и обмениваются информацией с Управляющей компании:

- ✓ использование только лицензированного программного обеспечения, полученного из доверенных источников;
- ✓ запрет на установку программ из непроверенных источников;
- ✓ использование средств электронной безопасности и защиты, таких как антивирус с регулярно и своевременно обновляемыми базами, персональный межсетевой экран, защита накопителя и прочих;
- ✓ настройка прав доступа к устройству таким образом, чтобы несанкционированный доступ к информации на таком устройстве был невозможен даже при утрате устройства владельцем;
- ✓ хранение и использование устройства способом, исключающим риски его кражи и/или утери;
- ✓ своевременное обновление операционной системы устройства;
- ✓ активация парольной или иной защиты для доступа к устройству;
- ✓ передача защищаемой информации клиентов только через безопасные беспроводные сети.

Обеспечение конфиденциальности защищаемой информации:

- ✓ хранение в тайне идентификационных данных и ключевой информации, полученных от Управляющей компании. В случае компрометации указанных данных клиенту следует принять меры для смены таких данных и/или уведомления Управляющей компании о их компрометации;
- ✓ соблюдение принципа разумного раскрытия информации о номерах счетов, паспортных данных, номерах кредитных и дебетовых карт, CVC/CVV кодах. В случае запроса у клиента указанной информации в связи с оказанием услуг Управляющей компании, клиенту следует по возможности оценить ситуацию и уточнить полномочия отправителя запроса и процедуру раскрытия информации непосредственно у Управляющей компании.

Проявление осторожности и предусмотрительности:

- ✓ клиенту Управляющей компании следует проявлять повышенную осторожность в следующих обстоятельствах:

а) при получении электронных сообщений со ссылками и вложениями, так как они могут привести к заражению устройства клиента вредоносным кодом;

б) при просмотре/работе с сайтами в сети Интернет, так как вредоносный код может быть загружен с сайта;

в) при получении файлов в архиве с паролем, так как в таком файле может быть вредоносный код.

Вредоносный код, попав к клиенту через почту или ссылку на сайт в сети Интернет, может получить доступ к любым данным и информационным системам на зараженном устройстве.

- ✓ следует внимательно проверять отправителя электронных сообщений. Входящее сообщение может быть от злоумышленника, который маскируется под Управляющую компанию или иных доверенных лиц;
- ✓ клиентам Управляющей компании не рекомендуется заходить на сайты, в системы удаленного доступа с непроверенных устройств, которые клиент не имеет возможности контролировать;
- ✓ при наличии в средствах массовой информации и на сайте Управляющей компании сведений о последних критичных уязвимостях и о вредоносном коде, клиентам рекомендуется принимать такую информацию к сведению;
- ✓ при обращении в Управляющую компанию клиенту рекомендуется осуществлять звонок только по номеру телефона, указанному на сайте Управляющей компании в сети Интернет;
- ✓ при предоставлении клиентом доступа к устройству третьим лицам клиент несет риск загрузки такими лицами на устройство вредоносного кода. В случае утраты устройства злоумышленники могут воспользоваться им для доступа к системам Общества от лица клиента;
- ✓ клиенту рекомендуется использовать для связи с Управляющей компанией отдельное, максимально защищенное устройство, доступ к которому есть только у клиента;
- ✓ контактная информация, предоставленная клиентом Управляющей компании, должна поддерживаться в актуальном состоянии для того, чтобы в случае необходимости представитель Управляющей компании мог оперативно связаться с клиентом.

В случае использования клиентом при взаимодействии с Управляющей компанией электронной подписи, клиенту рекомендуется:

- ✓ использовать для хранения ключей электронной подписи внешние носители;
- ✓ внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они не используются для работы;
- ✓ использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи, не хранить пароли в текстовых документах на устройстве.

При работе с защищаемой информацией на персональном компьютере рекомендуется:

- ✓ использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и т.д.);
- ✓ своевременно устанавливать актуальные обновления безопасности (операционные системы, офисные пакеты и т.д.);
- ✓ использовать антивирусное программное обеспечение, регулярно обновлять антивирусные базы;
- ✓ использовать специализированные программы для защиты информации и средства защиты от несанкционированного доступа;
- ✓ использовать сложные пароли;
- ✓ ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

При работе с мобильным устройством необходимо:

- ✓ не оставлять устройство без присмотра, чтобы исключить его несанкционированное использование;
- ✓ использовать только официальные мобильные приложения, загруженные при помощи официальных магазинов приложений;
- ✓ не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в смс-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Общества;
- ✓ установить на устройстве пароль для доступа к устройству.

При обмене информацией через сеть Интернет рекомендуется:

- ✓ не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам;
- ✓ не вводить персональную информацию на не вызывающих доверие сайтах и других неизвестных клиенту ресурсах;
- ✓ исключить посещение сайтов сомнительного содержания;
- ✓ не сохранять пароли в памяти интернет-браузера, если третьи лица имеют доступ к компьютеру;
- ✓ не нажимать на баннеры и всплывающие окна, возникающие во время работы в сети Интернет;
- ✓ открывать файлы только известных клиенту расширений.

При подозрении в компрометации электронной подписи или несанкционированном движении активов клиенту следует незамедлительно обращаться в Управляющую компанию по телефону и/или адресу электронной почты, указанным на официальном сайте Управляющей компании в сети Интернет.