Информация о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.

Общество с ограниченной ответственностью «Управляющая Компания «Овербест Эссет Менеджмент» (далее – общество*)* доводит до своих клиентов информацию о необходимости выполнения следующих мер защиты информации:

1. Меры по предотвращению несанкционированного доступа к защищаемой информации:

- исключение доступа посторонних лиц к устройствам, посредством которых осуществляются финансовые операции;

- использование на устройствах исключительно лицензионного программного обеспечения;

- использование специализированного программного обеспечения, обеспечивающего защиту устройств от вредоносных программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (антивирусных программных комплексов);

- регулярное обновление безопасности операционных систем устройств и антивирусных баз данных антивирусных программных комплексов;

- антивирусный контроль любой информации, получаемой и передаваемой с использованием устройства по телекоммуникационным каналам, а также информации на подключаемых к устройствам съемных носителях (магнитных, CD-дисках, DVD-дисках, USB-накопителях и т.п.);

- обеспечение сохранности и секретности аутентификационных данных для входа в информационные системы, а также ключей электронной подписи;

- ограничение возможности инсталляции в память устройств, с использованием которых совершаются действия в целях осуществления финансовых операций, программ и компонентов, полученных из ненадежных источников;

- предотвращение применения устройств, используемых для финансовых операций, для работы с сомнительными и развлекательными сайтами в сети Интернет (игровые сайты, сайты знакомств, сайты распространения программного обеспечения, мультимедийного контента, социальные и файлообменные сети и т.п.);

- предотвращение подключения устройств, используемых для финансовых операций, к открытым публичным и непроверенным проводным и беспроводным сетям (кафе, отели, парки, вокзалы и аэропорты);

- запрет запуска/открытия файлов, загруженных с ненадежных сайтов в сети Интернет и/или полученных от неизвестных адресатов, или в случае сомнений в их подлинности;

- использование на всех устройствах (включая сетевое оборудование) и компьютерных программах уникальных паролей длиной не менее 8 символов, состоящих из сочетания строчных и прописных букв, цифр и символов, регулярная замена паролей;

- запрет функции сохранения логина и пароля в памяти программного обеспечения браузера, используемого для доступа к информационным системам общества;

- в случае подозрений на возможную компрометацию (раскрытие) паролей – незамедлительная замена паролей.

2. Меры по предотвращению несанкционированного доступа злоумышленников к защищаемой информации методами психологического манипулирования и социальной инженерии:

- в случае получения обращения от имени общества (по телефону, по электронной почте и т.д.) с требованием срочного совершения какого-либо действия (например, заблокировать операцию, подтвердить свою регистрацию / обновить свои данные либо номер телефона / изменить пароль, получить выигрыш / выплату и т.п.) - рекомендуется отказаться от предлагаемых срочных действий, прекратить телефонный разговор либо не отвечать на сообщение электронной почты;

- необходимо сохранять спокойствие и уравновешенность и критический подход; необходимо самостоятельно перезвонить или написать электронное письмо по контактным данным, указанным на официальном сайте общества для уточнения запрашиваемого действия, а также сообщить о факте обращения от имени финансовой организации;

- никогда не сообщать любым другим лицам идентифицирующие сведения о номерах банковских счетов (счетов депо, лицевых счетов в реестрах владельцев ценных бумаг и т.п.), свои логины, пароли и сведения об устройствах, использующихся для осуществления финансовых операций, о моделях, версиях операционных систем и программ, о параметрах сетевых адаптеров (MAC- и IP-адресах) и другую информацию.

3. Меры по предотвращению несанкционированного доступа к защищаемой информации, которые необходимо выполнить при утрате клиентом устройства (потере, хищении), с использованием которого им совершались действия в целях осуществления финансовой операции, либо ключа электронной подписи клиента:

- как можно быстрее предпринять все возможные меры по временной блокировке доступа к информационным системам и ресурсам, через которые с утраченного устройства осуществлялись финансовые операции, для чего необходимо обратиться в общество по телефонам или по электронной почте, указанным на официальном сайте общества или в соответствующих инструкциях по работе с информационными ресурсами;

- выполнить процедуры, указанные в эксплуатационной документации на все программное обеспечение, используемое при информационном обмене в целях совершения финансовых операций, включая средства криптографической защиты (электронной подписи) в случае их использования (как можно быстрее совершить действия по блокировке / замене электронной подписи);

- провести процедуру замены паролей и другой аутентификационной информации, электронных подписей в информационных ресурсах финансовых организаций, в электронных почтовых ящиках, использованных ранее для обмена информацией в целях осуществления финансовых операций или подтверждения своих действий (в том числе - при восстановлении паролей).

4. Меры по контролю конфигурации устройств, с использованием которых клиентом совершаются действия в целях осуществления финансовой операции:

- своевременное обновление операционных систем устройств, а также всего программного обеспечения, повышающего безопасность;

- использование на устройствах, используемых для финансовых операций, исключительно лицензионного программного обеспечения;

- отказ от предоставления прав администратора устройства, позволяющих самостоятельно вносить изменения в конфигурацию устройства;

- использование функции предварительной авторизации на устройствах и блокировки экрана устройства при отсутствии активности.

5. Меры по своевременному обнаружению воздействия вредоносного кода:

- использование на устройствах не менее одного специализированного программного обеспечения, обеспечивающего защиту устройств, с использованием которых совершаются действия в целях осуществления финансовых операций, от вредоносного кода (антивирусного программного комплекса);

- регулярное обновление безопасности операционных систем устройств и антивирусных баз данных антивирусных программных комплексов;

- антивирусный контроль любой информации, получаемой и передаваемой с использованием устройства по телекоммуникационным каналам, а также информации на подключаемых к устройствам съемных носителях (магнитных, CD-дисках, DVD-дисках, USB-накопителях и т.п.);

- настройка антивирусного программного обеспечения по умолчанию с максимальным уровнем политик безопасности, не требующих действий пользователя при обнаружении вирусов, при этом лечение (удаление) зараженных файлов должно производиться антивирусным средством в автоматическом режиме;

- настройка антивирусного программного обеспечения для автоматической периодической (не реже одного раза в неделю) полной проверки устройств на предмет наличия вирусов и вредоносного программного кода;

- при возникновении подозрения на наличие компьютерного вируса (признаки – нетипичная работа устройства, пропадание / появление файлов, частое появление сообщений о системных ошибках и сбоях, значимое замедление работы, увеличение исходящего/входящего трафика и т.п.) рекомендуется провести дополнительные проверки и приостановить работу с финансовой информацией до устранения проблем;

- рекомендуется перезагружать устройство непосредственно перед работой с сервисами финансовой организации, а также после завершения сеанса работы с такими сервисами;

- в случае обнаружения антивирусным программным обеспечением вредоносного кода рекомендуется определить предположительную дату его появления (дату появления зараженного файла и т.п.), проконтролировать отсутствие несанкционированных распоряжений и запросов в финансовую организацию от своего имени за указанный период, и, по возможности, произвести замену используемой в целях совершения финансовых операций аутентификационной информации (пароли и т.п.);

- рекомендуется периодически проверять в системах (ресурсах), посредством которых осуществляются финансовые операции, статистику своей работы, сеансов, запрошенной информации, собственных запросов на совершение операций; появление неочевидной активности в журналах работы может свидетельствовать о компрометации реквизитов доступа или наличия вредоносного кода на устройстве.