УТВЕРЖДЕНЫ
Приказом Генерального директора
ООО «УК «Овербест Эссет Менеджмент»
№ 23/03/10-01 от 10.03.2023 г.

_____А.В. Садков

Рекомендации клиентам ООО «УК «Овербест Эссет Менеджмент» для обеспечения безопасности информации

ООО «УК «Овербест Эссет Менеджмент» (далее – Общество) в рамках соблюдения требований Положения Банка России от 20.04.2021 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» 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.

Настоящие Рекомендации клиентам ООО «УК «Овербест Эссет Менеджмент» для обеспечения безопасности информации (далее - Рекомендации) 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. Настоящие Рекомендации действуют в части не противоречащей положениям внутренних документов Общества, а также требованиям действующего законодательства РФ, носят открытый характер и размещаются в свободном доступе на официальном сайте Общества в сети Интернет по адресу http://www.overbestam.ru.

Общество предупреждает клиентов, что деятельность на рынке ценных бумаг, связанная с использованием электронно-вычислительной техники, несет в себе риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций от имени клиента финансовой организации (его уполномоченного лица). Реализоваться такие инциденты (нежелательные или неожиданные события защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов (клиента), технологических процессов организации и (или) нарушить безопасность информации) могут вследствие:

• несанкционированного доступа к информации лицами, не обладающими правом осуществления значимых (критичных) операций (в т.ч. финансовых), в том числе, кражи пароля и идентификатора доступа, использования SIM-карты для получения смс- кодов и пр.;

• потери (хищения) носителей ключей электронной подписи, с использованием которых, осуществляются критичные (финансовые) операции;

• воздействия вредоносного кода на устройства, с которых совершаются критичные (финансовые) операции;

• совершения в отношении клиента иных противоправных действий, связанных с информационной безопасностью (получение несанкционированного доступа к электронной почте с информацией об операциях и пр.)

В целях минимизации риска получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций Общество рекомендует клиентам применять, в том числе, но не ограничиваясь, следующие меры:

• организация контроля за устройствами, с использованием которых совершаются действия в целях осуществления финансовых операций;

• регламентация доступа к устройствам, с использованием которых совершаются действия в целях осуществления финансовых операций, и запрет доступа к таким устройствам посторонних лиц;

• использование паролей, регламентация требований к ним, в том числе порядка их использования, обновления, смены и уничтожения;

• использование исключительно лицензионного программного обеспечения, полученного из доверенных источников;

• использование специализированного программного обеспечения, обеспечивающего защиту устройств, с использованием которых совершаются действия в целях осуществления финансовых операций, от вредоносного кода (антивирусных программных комплексов) для АРМ пользователей и серверного оборудования, обеспечение функционирования средств защиты от вредоносного кода в автоматическом режиме, в том числе, в части установки обновлений, выполнение регулярных операций по проведению проверок на отсутствие вредоносного кода;

• организация регулярного обновления безопасности операционных систем и антивирусных баз данных;

• ограничение возможности загрузки и установки в память компьютеров или мобильных устройств, с использованием которых совершаются действия в целях осуществления финансовых операций, программ и компонентов, полученных из ненадежных источников;

• запрет запуска файлов, загруженных с ненадежных интернет сайтов и полученных от неизвестных адресатов (в том числе, посредством электронной почты);

• запрет на использование открытых общедоступных сетей Wi-Fi;

• обеспечение сохранности и секретности аутентификационных данных для входа в информационные системы, личные кабинеты, системы ЭДО (в случае использования), а также ключей электронной подписи;

• оперативное уведомление сотрудников Общества и удостоверяющего центра об утрате (хищении) ключевых носителей и иных случаях компрометации ключей

электронной подписи.

Для обеспечения конфиденциальности:

1. Храните в тайне аутентификационные / идентификационные данные: пароли, коды, кодовые слова, ключи электронной подписи/шифрования, а в случае компрометации немедленно примите меры для смены и / или блокировки.

2. Соблюдайте принцип разумного раскрытия информации о номерах счетов, о ваших паспортных данных, о других секретных номерах / кодах.

3. Не открывайте электронные письма от незнакомых лиц, содержащие ссылки и вложения, они могут привести к заражению вашего устройства вредоносным кодом. Будьте осторожны при просмотре/работе с интернет-сайтами, так как вредоносный код может быть загружен с сайта. При занесении вредоносного кода на устройство и отсутствии эффективных антивирусных средств защиты, злоумышленник может получить доступ к любым данным и информационным системам на устройстве, а также продолжить заражение иных устройств через зараженное.

4. Не пользуйтесь системами удаленного доступа с устройств, которые вы не контролируете (например, общедоступные компьютеры). На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию.

5. Не оставляйте без присмотра носители, содержащие ключи электронной подписи, не передавайте их третьим лицам, извлекайте носители из компьютера, если они не используются для работы. Храните внешние носители в сейфах.

6. Не сохраняйте пароли в памяти интернет-браузера, если к компьютеру есть доступ третьих лиц.

7. Не нажимайте на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет.

8. Не открывайте файлы полученные (скачанные) из неизвестных источников. При подозрении компрометации идентификационных или аутентификационных данных, подозрении нарушений штатного функционирования средств вычислительной техники, которые способны повлечь совершения незаконных финансовых операций необходимо незамедлительно обращаться в Общество.