УТВЕРЖДЕНО:
Решением единственного участника
ООО «АКЦЕНТ УПРАВЛЕНИЕ АКТИВАМИ»
от «23» января 2020 года

РЕКОМЕНДАЦИИ
по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям

В соответствии с требованиями Положения Банка России от 17.04.2019 № 684-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» Обществом с ограниченной ответственностью «АКЦЕНТ УПРАВЛЕНИЕ АКТИВАМИ» (далее по тексту – «Общество») уведомляет клиентов Общества о возможных рисках получения третьими лицами, не обладающими правом осуществления финансовых операций, несанкционированного доступа к защищаемой информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах, используемых Обществом.

Под защищаемой информацией понимается:

- учетные данные (логины и пароли для доступа к электронной почте, личным кабинетам сайтов и мобильных приложений, используемых для проведения финансовых операций, и т.п.);
- информация, необходимая для удостоверения права клиентов Общества распоряжаться своим имуществом;
- информация по осуществлению Вами финансовых операций, состоянию счетов и имеющихся активах;
- документы, получаемые при осуществлении финансовых операций;
- ключевая информация средств криптографической защиты информации (СКЗИ), используемых при проведении финансовых операций;
- персональные данные.

Несанкционированный доступ со стороны третьих лиц может повлечь за собой риски разглашения вышеуказанной информации, а также совершение юридически значимых действий, включая: совершение операций с доступными активами, подключение и отключение услуг (в том числе платных), внесение изменений в регистрационные данные клиента, использование счетов и находящихся на них активов для прикрытия действий, носящих противоправный характер, совершение иных действий против воли клиента.

Несанкционированный доступ со стороны третьих лиц также может повлечь за собой деструктивное воздействие на носители информации и их содержимое, что в свою очередь может привести к воспрепятствованию своевременного исполнения Вами своих обязательств или реализации намерений.

В рамках защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в том числе для своевременного обнаружения воздействия вредоносного кода, в целях противодействия незаконным финансовым операциям, в обеспечение контроля конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, а также для предотвращения несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом электронного устройства (персонального переносного компьютера, мобильных устройств т.п.), с использованием которого совершались финансовые операции, Общество рекомендует соблюдать следующие меры:

- надежно храните свои электронные устройства во избежание их утраты (потери или хищения);
- используйте только лицензионное системное и прикладное программное обеспечение, проводите его своевременное обновление;

- используйте официально приобретенные антивирусные программы, периодически проводите полную проверку своих электронных устройств и подключаемых к ним съемных носителей информации;
- по возможности избегайте установки и использования программ для удаленного управления электронными устройствами;
- контролируйте конфигурацию устройств, с использованием которых совершаются действия в целях осуществления финансовой операции, не отключайте и не взламывайте встроенные механизмы обеспечения безопасности;
- при наличии технической возможности всегда используйте шифрование носителей данных на своём электронном устройстве;
- не храните в открытом виде на своих электронных устройствах скан-копии документов, удостоверяющих Вашу личность, а также электронные файлы, содержащие учетные данные для доступа к информационным ресурсам финансовых учреждений, с которыми Вы сотрудничаете;
- для доступа к информационным системам финансовых учреждений в целях совершения финансовых операций не используйте общедоступные электронные устройства (например, установленные в интернет-кафе, гостинице), публичные бесплатные беспроводные сети;
- используйте на электронных устройствах или в приложениях надежные пароли доступа (с длиной пароля не менее 8 (восьми) символов, включающего в себя заглавные и прописные буквы, а также цифры и специальные символы) и имеющиеся блокировки;
- не используйте одинаковые пароли для доступа к разным информационным системам, web-сервисам;
- осуществляйте систематическое изменение паролей (например, не реже одного раза в 3 (Три) месяца, либо при наличии подозрения в их возможной компрометации);
- сохраняйте в тайне Ваши учетные данные для доступа к информационным системам, не записывайте и не храните их в доступном посторонним лицам месте;
- не посещайте сайты сомнительного содержания, не переходите по ссылкам во вложении к электронным письмам, sms, mms, в сообщениях мессенджеров от незнакомых адресатов, т.к. данные действия могут привести к краже Ваших данных и проникновению на электронные устройства вредоносного кода;
- не отвечайте на сообщения от неизвестных адресатов, требующих предоставить, подтвердить или уточнить вашу конфиденциальную информацию: пароли, логины, фамилию, имя, отчество, паспортные данные, номер мобильного телефона, на который поступают одноразовые пароли от финансовых учреждений, а также данные о Ваших финансовых операциях.

Настоятельно советуем Вам соблюдать предложенные рекомендации в целях защиты информации от воздействия вредоносных кодов, предотвращения несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) электронного устройства, с использованием которого Вами совершались финансовые операции.

Для связи с Обществом по вопросам выполнения настоящих рекомендаций необходимо использовать контактные данные, указанные на официальном сайте Общества в сети «Интернет» https://accent-am.ru/.

Генеральный директор
ООО «АКЦЕНТ УПРАВЛЕНИЕ АКТИВАМИ» **А.А. Богданов**