Описание рисков, связанных с использованием программного обеспечения и рекомендации по обеспечению информационной безопасности, защите от воздействия вредоносного кода при использовании сервисов ООО УК «Система Капитал» в сети Интернет в целях противодействия незаконным финансовым операциям

1. Общие положения.

1.1. Настоящий документ (далее – Рекомендации) содержит описание рисков, связанных с использованием программного обеспечения и рекомендации для клиентов ООО УК «Система Капитал» (далее – Общество) по обеспечению защиты информации при использовании программного обеспечения и сервисов Общества в сети Интернет.

1.2. Рисками, связанными с использованием программного обеспечения и сервисов Общества, для клиентов Общества являются:
- риск воздействия вредоносного кода и не своевременного обнаружения такого воздействия;
- риск несанкционированного доступа к информации путём использования ложных (фальсифицированных) ресурсов сети Интернет;
- риск различных видов мошенничества, в т.ч. о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, и 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.

1.3. Рекомендации по обеспечению защиты информации доводятся до сведения клиентов Общества посредством размещения на сайте Общества в сети Интернет по адресу http://www.sistema-capital.com/ (далее – Сайт Общества).

1.4. В целях настоящего документа:
- термины и определения, применяемые в тексте Рекомендаций, имеют то же значение, что и в Соглашении об электронном документообороте Общества, размещенном на Сайте Общества, если в тексте Рекомендаций не указано иное;
- под клиентами Общества понимаются физические лица, заключившие и (или) намеренные заключить с Обществом договор с использованием простой электронной подписи посредством Сайта Общества и (или) Личного кабинета;
- под сервисами Общества понимаются Сайт Общества, а также Личный кабинет, доступ к которому осуществляется посредством Сайта Общества или через Мобильное приложение «МТС Инвестиции»;
- под средствами вычислительной техники (далее – СВТ) понимаются устройства, с использованием которого клиентом совершаются, совершались или будут совершаться действия в целях осуществления финансовой операции;
- под действиями, совершаемыми клиентом в целях осуществления финансовой операции, понимается совокупность действий клиента, совершаемых им с использованием СВТ в целях заключения договора с Обществом и последующей передачей денежных средств и (или) ценных бумаг Обществу по такому договору.

2. Обеспечение защиты от воздействий вредоносного кода

2.1. Вредоносный код (далее - ВК) – любой программный код (компьютерный вирус, троян, сетевой червь и пр.), приводящий к нарушению штатного функционирования СВТ и/или предназначенный для искажения, модификации, уничтожения, блокирования или несанкционированного копирования информации. ВК способен создавать свои копии, сохраняющие все его свойства и требующие для своего размножения другие программы, каналы связи или машинные носители.

2.2. Возможен следующий характер проявлений действий ВК:
- искажение изображения на экране монитора;
- искажение символов, вводимых с клавиатуры;
- блокирование клавиатуры, звуковые эффекты;
- стирание или порча отдельных частей жесткого диска СВТ или файлов;
- повреждение загрузочных секторов жесткого диска СВТ;

– остановка загрузки или зависание СВТ, значительное замедление его работы.

2.3. ВК может попасть на СВТ со сменного носителя (CD-ROM, USB флеш-накопителей и других носителей, даже если эти носители не содержат файлов), при загрузке файлов из сети, с сообщением, полученным по электронной почте, а также через уязвимости операционных систем при наличии сетевого подключения СВТ к локальной вычислительной сети.

2.4. В целях обеспечения защиты СВТ от воздействий ВК и недопущения таких событий, как появление в СВТ вредоносных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификации СВР, на перехват информации, в том числе паролей секретных ключей, информация о которых содержится в СВР и иные формы несанкционированного доступа, внесение несанкционированных изменений в технические и программные средства СВР, приводящие к некорректной работе сервисов Общества, в т.ч. внесения несанкционированных изменений в электронные документы, формируемые сервисами Общества, клиенту рекомендуется:

- применять программные средства защиты от воздействия ВК, а также регулярно производить их обновление;
- не использовать при работе «зараженный» вредоносным кодом либо с подозрением на «заражение» носитель и/или файл, и/или СВТ;
- проводить контроль на отсутствие ВК любых сменных и подключаемых носителей (CD-дисков, DVD-дисков, USB флеш-накопителей и т.п.) и файлов;
- при появлении сообщений, формируемых средствами защиты информации, об обнаружении вредоносного кода немедленно прекратить работу с СВТ;
- использовать носители, которые не принадлежат клиенту или в надежности которого он не может быть уверен;
- не производить установку программного обеспечения на СВТ из непроверенных источников;
- отключать, удалять и изменять настройки установленных средств защиты в сторону снижения степени защиты.

3. Рекомендации по защите от различных видов мошенничества

3.1. SMS- сообщения используются мошенниками для сбора информации и убеждения клиента осуществить финансовые операции в пользу третьих лиц под различными предлогами.
Признаками таких сообщений могут быть:

- запрашиваемые в сообщении действия требуют срочного ответа клиента;
- сообщение содержит требование предоставить, обновить или подтвердить персональные данные (кодовое слово, пароль и т. д.);
- сообщение содержат форму для ввода персональных данных клиента;
- сообщение содержат информацию, что на счёт клиента поступили деньги, поступление которых не ожидается клиентом;
- сообщение содержит просьбу пройти по ссылке в сообщении;
- сообщение содержит просьбу подтвердить что-либо, ответив на SMS.

В случае, если клиентом получено SMS, содержащее признаки сообщения, направленного в целях совершения мошеннических действий, рекомендуется не осуществлять ответ на такие сообщения, переход по ссылкам, которое оно содержит, а также не производить иных действий, указание на которые содержится в таком сообщении. Если полученное сообщение имеет признаки сообщения, направленного клиенту от имени Общества, рекомендуется обратиться в Общество для получения подтверждения о том, что такое сообщение было направлено Обществом в адрес клиента.

3.2. Мошенничество по электронной почте. Сообщения электронной почты, которые используются в целях мошеннических действий, могут содержать ссылки на фальшивые веб-сайты, замаскированные под сервис Общества, сайты организаций, например, банков, чтобы получить персональные данные клиента (номер банковской карты, пароль, ПИН код) и использовать данную информацию для хищения средств клиента. Такие сообщения могут содержать явные опечатки или орфографические ошибки, что позволяет им обходить «spam» фильтры, установленные у Интернет провайдеров.

В случае, если клиент осуществил переход по ссылке на фальшивый сайт или сайт, имеющий признаки такового, клиенту категорически не рекомендуется передать персональные данные и давать свое согласие на их обработку. В этом случае СВТ клиента может быть заражено вирусом, который будет сканировать нажатие клавиш клавиатуры и передавать лицам, намеренным совершить мошеннические действия, данные, вводимые в подлинном сервисе Общества или на подлинном сайте иной организации. Если же клиентом осуществлен ввод, к примеру, номера телефона, то на телефон может быть отправлено (в зависимости от модели телефона)

сообщение с вирусом, позволяющее лицам, намеренным совершить мошеннические действия, перехватывать все сообщения.

В случае, если клиентом получено сообщение электронной почты, содержащее признаки сообщения, направленного в целях совершения мошеннических действий, рекомендуется не осуществлять ответ на такие сообщения, переход по ссылкам, которое оно содержит, а также не производить иных действий, указание на которые содержится в таком сообщении. Если полученное сообщение имеет признаки сообщения, направленного клиенту от имени Общества, рекомендуется обратиться в Общество для получения подтверждения о том, что такое сообщение было направлено Обществом в адрес клиента.

3.3. Телефонное мошенничество. Звонки по телефону, наряду с сообщениями электронной почты и СМС, используются мошенниками для сбора конфиденциальной информации, часто похожи на «настоящие» звонки. В случае получения такого звонка, имеющего признаки мошеннического, от имени Общества, рекомендуется не осуществлять взаимодействие в рамках такого звонка, и незамедлительно его прервать. В дальнейшем рекомендуется обратиться в Общество для получения подтверждения о том, что звонок был осуществлен клиенту представителем Общества.