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

г. Москва, 2021 г.

I. Общие положения

1.1. Настоящие Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям Общества с ограниченной ответсвеностью «Управляющая компания «ОРЕОЛ» (далее – ***Рекомендации, Общество***) разработаны в соответствии с требованиями 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» и включают в себя информацию:

- о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом средства вычислительной техники, с использованием которого им совершались действия в целях осуществления финансовой операции (далее – ***устройство***), контролю конфигурации устройства, и своевременному обнаружению воздействия программных кодов, приводящих к нарушению штатного функционирования с устройства (далее – ***вредоносный код***).

1.2. Настоящие Рекомендации разработаны в целях предупреждения последствий недобросовестных действий третьих лиц, противодействия проведению незаконных финансовых операций в отношении активов, находящихся в доверительном управлении. Задачи защиты информации сводятся к минимизации ущерба и предотвращению воздействий со стороны злоумышленников. Для обеспечения надлежащей степени защищенности должен быть обеспечен комплексный подход, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне Общества, так и на стороне клиента.

1.3. В результате неправомерных действий третьих лиц информация, связанная с проведением финансовых операций, получаемая, подготавливаемая, обрабатываемая, передаваемая и хранимая в автоматизированных системах Общества, содержащаяся в электронных документах, которыми Общество обменивается с клиентами (электронные сообщения), информация, необходимая для авторизации клиента и удостоверения его прав на распоряжение активами (далее – ***идентификационные данные***), информация об осуществленных финансовых операциях, а также ключевая информация применяемых средств криптографической защиты (далее – ***криптографические ключи***) (далее в совокупности – ***защищаемая информация***), может быть подвергнута воздействию вредоносных кодов.

1.4. Антивирусная защита осуществляется с целью исключения возможностей появления на устройствах компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию специализированного и системного программного обеспечения, либо на перехват информации, в том числе паролей.

1.5. Средства и методы защиты информации, применяемые Обществом, позволяют обеспечить необходимый уровень безопасности при осуществлении доверительного управления и предотвратить несанкционированный доступ к защищаемой информации при условии выполнения клиентами рекомендаций, изложенных в данном документе.

II. Риски получения несанкционированного доступа к защищаемой информации

2.1. К рискам получения несанкционированного доступа к защищаемой информации относятся:

- хищение идентификационных данных клиента (далее – ***фишинг***) и их незаконное использование для выполнения несанкционированных операций от имени клиента;
- факт доступа постороннего лица к информации, содержащей закрытый ключ электронной цифровой подписи (далее – ***компрометация криптографических ключей***), а также подозрение на компрометацию криптографических ключей;
- утечка идентификационных данных клиента в сеть Интернет и её размещение на

общедоступных доступных ресурсах;

- нарушение целостности данных (изменение структуры баз данных, связей между таблицами и т.д.), искажение данных или их потеря (удаление информации) в результате действий злоумышленников, получивших доступ.

2.2. Наиболее распространенными способами фишинга являются:

- использование ложных (фальсифицированных) ресурсов (страниц, веб-сайтов) в сети Интернет;
- воздействие вредоносного кода.

III. Меры по предотвращению несанкционированного доступа к защищаемой информации путем использования ложных (фальсифицированных) ресурсов в сети Интернет

3.1. Ложный (фальсифицированный) ресурс (страница, веб-сайт и т.п.) в сети Интернет, как правило, является почти точной копией соответствующего ресурса в сети Интернет и предназначен для сбора защищаемой информации обманным путем. Ввод логина и пароля на таком ресурсе в сети Интернет приводит к получению вышеуказанной информации злоумышленниками, то есть разглашению идентификационных данных.

3.2. Меры по предотвращению несанкционированного доступа к защищаемой информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов в сети Интернет:

- удостовериться, что при подключении к системе электронного документооборота (далее – ***ЭДО***) защищённое SSL-соединение было установлено исключительно с официальным сайтом ЭДО, во избежание использования ложных (фальсифицированных) ресурсов в сети Интернет и программного обеспечения, имитирующих программный интерфейс системы ЭДО;
- проверить адрес отправителя перед просмотром письма, полученного по электронной почте, поскольку строка «Отправитель» может содержать адрес электронной почты, который является почти точной копией соответствующего подлинного адреса;
- прочитать текст письма, полученного по электронной почте, в случае наличия в нем слов на иностранном языке, специальных символов и т.п., существует большая вероятность того, что это письмо отправлено злоумышленниками;
- не открывать вложения, прикрепленные к письму, полученному по электронной почте, начинающемуся с обезличенного обращения (например, «Уважаемый пользователь»), или обращения по адресу электронной почты, т.к. типовое фишинговое письмо начинается с обезличенного приветствия;
- проанализировать ссылку в сети Интернет и не переходить по ней, если она выглядит подозрительно и/или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), поскольку данная ссылка может быть почти точной копией подлинной, однако перенаправить на ложный (фальсифицированный) ресурс в сети Интернет.

IV. Меры по предотвращению несанкционированного доступа к защищаемой информации путем воздействия вредоносного кода

4.1. Меры по предотвращению несанкционированного доступа к защищаемой информации от несанкционированного доступа путем воздействия вредоносного кода:

- использовать устройства с установленным лицензионным программным обеспечением;
- установить на устройстве лицензионное антивирусное программное обеспечение, которое должно в автоматическом режиме
  - запускаться одновременно с загрузкой операционной системы,
  - обновлять вирусные базы,
  - удалять зараженные вирусом файлы с устройства;
- подвергать антивирусному контролю любую информацию, получаемую по телекоммуникационным каналам связи, а также информацию на съемных носителях (CD/DVD дисках, USB-накопителях и т.п.);

- проводить полную проверку жесткого диска устройства на предмет наличия вирусов и вредоносного программного кода не реже одного раза в неделю в автоматическом режиме;
- воздержаться от использования системы ЭДО в случае подозрений на наличие вредоносных кодов (неожиданных «зависаниях», перезагрузках и т.п.) на устройстве, с которого осуществляется информационный обмен по системе ЭДО, до устранения проблемы;
- обновлять своевременно программное обеспечение и операционную систему (в части критичных обновлений);
- входить в операционную систему устройства с учетной записью пользователя, не использовать права администратора в повседневной практике;
- исключить возможность бесконтрольного доступа посторонних лиц (гостей, посетителей) к устройству;
- ограничить информационный обмен в сети Интернет только надежными информационными порталами;
- не использовать устройство, с которого осуществляется информационный обмен по системе ЭДО, для общения в социальных сетях, переписке в интернет-мессенджерах, а также для посещения развлекательных сайтов и сайтов сомнительного содержания (игровые сайты, сайты знакомств, сайты, распространяющие программное обеспечение, музыку, фильмы и т.п.).
- применять иные меры, указанные в разделе III Рекомендаций.

V. Меры по предотвращению несанкционированного доступа к защищаемой информации третьими лицами

5.1. Меры по предотвращению несанкционированного доступа к защищаемой информации третьими лицами:

- выделить отдельное устройство, предназначенное для доступа к системе ЭДО, с установленным на нем минимальным необходимым для работы набором программного обеспечения;
- не использовать на устройстве, предназначенном для доступа к системе ЭДО, средства удаленного администрирования;
- исключить возможность физического доступа к устройству, предназначенному для доступа к системе ЭДО, для посторонних лиц и персонала, не имеющего отношения к работе с ЭДО;
- хранить (записывать) логины и пароли в местах не доступных посторонним лицам, исключив возможность несанкционированного доступа;
- хранить информацию криптографических ключей на отчуждаемом носителе (USB-накопителе) в сейфе или запираемом шкафу, исключив возможность несанкционированного доступа;
- не передавать носитель криптографического ключа третьим лицам;
- отключать и извлекать носитель криптографического ключа из устройства, если он не используются для доступа к системе ЭДО, поскольку размещение носителя криптографического ключа в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к нему третьих лиц;
- использовать разные уникальные пароли для различных ресурсов в сети Интернет, а также систем, на которых вводится защищаемая информация;
- не пересылать защищаемую информацию с использованием электронной почты, интернет-мессенджеров и/или SMS-сообщений;
- незамедлительно обратиться к оператору ЭДО для блокировки скомпрометированного криптографического ключа в случае его компрометации или подозрении на компрометацию (утрате, потере, хищении носителя криптографического ключа);
- удалить с устройства все следы работы с системой ЭДО в случае передачи (списания) устройства, на котором ранее была установлена система ЭДО;
- принять меры по контролю за конфигурацией устройства, предназначенного для доступа к системе ЭДО, и не допускать несанкционированных программно-аппаратных изменений конфигурации;
- применять иные меры, указанные в разделах III и IV Рекомендаций.

Указанный выше перечень мер и рисков не является исчерпывающим в виду многообразия ситуаций, которые могут возникать при совершении финансовых операций.

Общество не несет ответственности в случае возникновения у клиента финансовых потерь, понесенных в связи с нарушением и/или ненадлежащим исполнением мер по предотвращению несанкционированного доступа к защищаемой информации.