Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям.

В соответствии с требованиями Положения 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 (утв. Банком России 17.04.2019 № 684-П) ООО «Интерпромлизинг» (далее – Компания) доводит до сведения своих клиентов следующую информацию:

1. О возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

1.1. Клиенты Компании несут риски возможных финансовых потерь вследствие следующих обстоятельств:

− получение лицами, не обладающими правом осуществления финансовых операций от лица клиента, несанкционированного доступа к защищаемой информации; − утрата (потеря, хищение) носителей ключей электронной подписи, с использованием которых осуществляются финансовые операции;
− воздействие вредоносного кода на устройства клиента, с которых совершаются финансовые операции (персональный компьютер, планшет, мобильный телефон и пр., далее – устройство);
− совершение в отношении клиента Компании иных противоправных действий.

1.2. При осуществлении финансовых операций клиентам Компании следует принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами.

Такие риски также могут возникать вследствие:

− кражи пароля и идентификатора доступа или иных конфиденциальных данных, например, закрытого ключа, посредством технических средств и/или вредоносного кода и использовании злоумышленниками указанных данных с других устройств для несанкционированного доступа;
− установки на устройство вредоносного кода, который позволит злоумышленникам осуществить операции от имени клиента Компании;
− использования злоумышленником утерянного или украденного телефона для получения СМС кодов, которые могут применяться Компанией в качестве элемента простой электронной подписи либо дополнительного способа идентификации клиента, для подтверждения несанкционированных финансовых операций;
− кражи или несанкционированного доступа к устройству, с которого клиент Компании пользуется услугами Компании для получения данных и/или несанкционированного доступа к услугам с этого устройства;
− получения злоумышленниками персональных данных клиента Компании, пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих конфиденциальных данных путем обмана и/или злоупотребления доверием. Описанный риск может реализоваться, помимо прочего, когда злоумышленник представляется

сотрудником Компании или техническим специалистом или использует иную легенду и просит клиента сообщить ему указанные конфиденциальные данные или направляет поддельные почтовые сообщения с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;
− перехвата почтовых сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если электронная почта клиента используется для информационного обмена с Компанией. В случае получения доступа к почте клиента, отправка сообщений Компании от его имени.

1.3. Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) для доступа к информационным системам Компании несет Владелец учётных данных. Компания не несет ответственности в случаях финансовых потерь, понесенных клиентами в связи с пренебрежением правилами информационной безопасности.

2. 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.

2.1. Клиентам Компании следует предпринять все доступные меры для предотвращения несанкционированного доступа к защищаемой информации таких клиентов. Для указанных целей клиентам Компании следует принять, помимо прочего, следующие меры:

2.1.1. Обеспечение надлежащей защиты устройств, с помощью которых клиенты пользуются услугами Компании и обмениваются информацией с Компанией:

− использование только лицензированного программного обеспечения, полученного из доверенных источников;
− запрет на установку программ из непроверенных источников;
− использование средств электронной безопасности и защиты, таких как антивирус с регулярно и своевременно обновляемыми базами, персональный межсетевой экран, защита накопителя и пр.;
− настройка прав доступа к устройству таким образом, чтобы несанкционированный доступ к информации на таком устройстве был невозможен даже при утрате устройства владельцем;
− хранение и использование устройства способом, исключающим риски его кражи и/или утери;
− своевременное обновление операционной системы устройства;
− активация парольной или иной защиты для доступа к устройству;
− незамедлительное изменение учетных данных, используемых для доступа к услугам Компании, после удаления с устройства обнаруженного вредоносного программного обеспечения;
− передача защищаемой информации клиентов только через безопасные беспроводные сети. Работая в общедоступных беспроводных сетях, клиентам не следует вводить учетные данные, используемые для доступа к услугам Компании.

2.1.2. Обеспечение конфиденциальности защищаемой информации:

− хранение в тайне аутентификационных/идентификационных данных и ключевой информации, полученных от Компании: паролей, СМС-кодов, кодовых слов. В случае компрометации указанных данных клиенту следует принять меры для смены таких данных и/или уведомления Компании об их компрометации;

− соблюдение принципа разумного раскрытия информации о номерах счетов, паспортных данных, номерах кредитных и дебетовых карт, CVC/CVV кодах. В случае запроса у клиента указанной информации в связи с оказанием услуг Компанией, клиенту следует по возможности оценить ситуацию и уточнить полномочия отправителя запроса и процедуру раскрытия информации через независимый канал связи, например, обратившись в Компанию.

2.1.3. Проявление осторожности и предусмотрительности:

− клиенту Компании следует проявлять повышенную осторожность в следующих обстоятельствах:

а) при получении электронных сообщений со ссылками и вложениями, так как они могут привести к заражению устройства клиента вредоносным кодом;

б) при просмотре/работе с сайтами в сети Интернет, так как вредоносный код может быть загружен с сайта;

в) при получении файлов в архиве с паролем, так как в таком файле может быть вредоносный код. Вредоносный код, попав к клиенту через почту или ссылку на сайт в сети Интернет, может получить доступ к любым данным и информационным системам на зараженном устройстве.

− следует внимательно проверять отправителя электронных сообщений. Входящее сообщение может быть от злоумышленника, который маскируется под Компанию или иных доверенных лиц;

− клиентам Компании не следует заходить в системы удаленного доступа с недоверенных устройств, которые клиент не контролирует. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;

− при наличии в средствах массовой информации и на сайте Компании сведений о последних критичных уязвимостях и о вредоносном коде, клиентам рекомендуется принимать такую информацию к сведению;

− при обращении в Компанию клиенту следует осуществлять звонок только по номеру телефона, указанному на официальном сайте Компании в сети Интернет;

− клиенту рекомендуется использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у клиента;

− в случае выхода из строя сим-карты, используемой для получения СМС-кодов, клиенту следует незамедлительно обратиться к своему сотовому оператору для уточнения причин неработоспособности сим-карты и восстановления связи;

− контактная информация, предоставленная клиентом Компании, должна поддерживаться в актуальном состоянии для того, чтобы в случае необходимости представитель Компании мог оперативно связаться с клиентом.

2.1.4. При работе с ключами электронной подписи необходимо:

− использовать для хранения секретных ключей электронной подписи внешние носители;

− крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра

и не передавать третьим лицам, извлекать носители из компьютера, если они не используются для работы;
− использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи, не хранить пароли в текстовых документах на устройстве.

2.1.5. При работе с защищаемой информацией на персональном компьютере необходимо:

− использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и т.д.);
− своевременно устанавливать актуальные обновления безопасности (операционные системы, офисные пакеты и т.д.);
− использовать антивирусное программное обеспечение, регулярно обновлять антивирусные базы;
− использовать специализированные программы для защиты информации (персональные межсетевые экраны и средства защиты от несанкционированного доступа), средства контроля конфигурации устройств;
− использовать сложные пароли;
− ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

2.1.6. При работе с мобильным устройством необходимо:

− не оставлять устройство без присмотра, чтобы исключить его несанкционированное использование;
− использовать только официальные мобильные приложения, загруженные при помощи официального магазина приложений;
− не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие не от имени Компании в смс-сообщении, Push-уведомлении или по электронной почте;
− установить на устройстве пароль для доступа к устройству.

2.1.7. При обмене информацией через сеть Интернет необходимо:

− не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам;
− не вводить персональную информацию на подозрительных сайтах и других неизвестных клиенту ресурсах;
− исключить посещение сайтов сомнительного содержания;
− не сохранять пароли в памяти Интернет-браузера, если третьи лица имеют доступ к компьютеру;
− открывать файлы только известных расширений.

2.2. При подозрении в компрометации ключей или несанкционированном движении денежных средств необходимо обращаться в Компанию по телефону и/или адресу электронной почты, указанным на официальном сайте Компании в сети Интернет.