Рекомендации для клиентов ООО «ИК «ФИНПРОИНВЕСТ» по обеспечению информационной безопасности, защите информации от воздействия вредоносного кода при работе в сети «Интернет» и использовании системы дистанционного обслуживания в целях противодействия незаконным финансовым операциям.

1. Общие положения

1.1. Настоящие Рекомендации по обеспечению информационной безопасности, защите информации от воздействия вредоносного кода при работе в сети «Интернет» и при использовании системы дистанционного обслуживания в целях противодействия незаконным финансовым операциям (далее – Рекомендации) разработаны ООО «ИК «ФИНПРОИНВЕСТ» (далее – Организация) в целях защиты финансовой и иной информации от воздействия вредоносных кодов (программ), от несанкционированного доступа путём использования ложных (фальсифицированных) ресурсов сети «Интернет», по защите от различных видов мошенничества, в целях противодействия незаконным финансовым операциям. Рекомендации разработаны с учетом требований «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», утвержденных Банком России 20.04.2021 № 757-П.

1.2. Целью Рекомендаций является доведение до Клиентов Организации информации:

1) о возможных рисках получения несанкционированного доступа к защищаемой информации, в том числе с целью осуществления финансовых операций, лицами, не обладающими правом их осуществления;

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 (программы).

1.3. Рекомендации доводятся до сведения Клиентов Организации посредством уведомления Клиентов в порядке, предусмотренном для уведомлений соответствующим договором об оказании услуг на рынке ценных бумаг и (или) путем размещения Рекомендаций на сайте Организации.

2. Определение терминов и сокращений

2.1. В целях настоящих Рекомендаций указанные ниже термины и сокращения используются в следующих значениях:

Вредоносная программа (вредоносный код) - любое программное обеспечение (программный код), приводящее к нарушению штатного функционирования средства вычислительной техники; предназначен для получения несанкционированного доступа к вычислительным ресурсам устройства Клиента или к информации, хранимой на устройстве Клиента с целью несанкционированного использования ресурсов устройства Клиента или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу устройства Клиента путем внедрения в автоматизированные системы, ПО, средства вычислительной техники, телекоммуникационное оборудование Клиентов - пользователей Систем дистанционного обслуживания, и приводит к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче защищаемой и иной информации, а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи.

Защищаемая информация:

информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками Организации и (или) Клиентами Организации;

информация, необходимая Организации для авторизации своих Клиентов в целях осуществления финансовых операций и удостоверения права Клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом;

информации об осуществленных Организацией и ее Клиентами финансовых операциях;

ключевая информация средств криптографической защиты информации, используемая Организацией и ее Клиентами при осуществлении финансовых операций (в предусмотренных договорами на оказание услуг на рынке ценных бумаг случаях).

Неуполномоченные лица – лица, не обладающие правом осуществления финансовых операций.

Несанкционированный доступ - незаконное либо не разрешенное обладателем информации использование возможности получения информации и ее использования.

Пользователь (Клиент) - обладатель защищаемой информации, используемой для проведения финансовых операций в рамках исполнения заключенных между Организацией и Клиентом договоров на обслуживание на рынке ценных бумаг.

Сайт Организации – официальный сайт Организации в сети «Интернет», размещенный по адресу http://www.finproinvest.ru.

Система дистанционного обслуживания – системы дистанционного обслуживания Клиентов Организации (личный кабинет, QUIK и т.д.);

Съемный носитель информации – носитель информации, предназначенный для ее автономного хранения и независимого от места записи использования (токен, CD, флэш-накопитель и т.д.).

Иные термины, специально не определенные настоящими Рекомендациями, используются в значениях, установленных законами и иными нормативными правовыми актами Российской Федерации.

3. Риски получения несанкционированного доступа к устройствам Клиента, а также цели и задачи защиты устройств Клиента от несанкционированного доступа

3.1. Задачи защиты защищаемой информации сводятся к минимизации ущерба и предотвращению каких-либо воздействий со стороны неуполномоченных лиц.

3.2. Защита устройства Клиента - участника системы дистанционного обслуживания от несанкционированного доступа осуществляется с целью исключения (минимизации) возможности:

- появления в устройствах, на которых установлено программное обеспечение дистанционного обслуживания вредоносных программ и программ, направленных на разрушение, блокирование, нарушение работоспособности или модификацию программного обеспечения Системы дистанционного обслуживания, либо на перехват информации, в том числе паролей секретных ключей;

- внесения несанкционированных изменений в технические и программные средства Системы дистанционного обслуживания, а также в их состав;

- внесения несанкционированных изменений в электронные документы или электронные сообщения.

3.3. К основным рискам получения несанкционированного доступа к защищаемой информации неуполномоченными лицами, в том числе с использованием вредоносных программ, относятся:

- риск совершения финансовых операций с активами Клиентов, в том числе путем формирования и отправки от имени Клиента распоряжения на осуществление финансовой операции, включая отправку сообщений на «короткие номера», а также путем перехвата сообщений с кодами подтверждения, приходящими на мобильное устройство в целях подтверждения операции или доступа к защищаемой информации;

- риск совершения иных юридически значимых действий, включая: подключение и отключение услуг (в том числе платных), внесение изменений в регистрационные данные Клиента, использование счетов и находящихся на них активов для прикрытия иных действий, носящих противоправный характер, совершения иных действий против воли Клиента;

- риск повреждения программного обеспечения Клиента, а также риск искажения, изменения, уничтожения или шифрования информации об активах (ценных бумагах, денежных средствах) и финансовых операциях Клиентов и Организации;

- риск разглашения информации конфиденциального характера: сведений об операциях, активах, состояния счетов, подключенных услугах, иной значимой информации и персональных данных Клиента.

3.4. Несанкционированный доступ к защищаемой информации происходит посредством удалённого доступа к устройствам Клиента в результате взлома защиты устройства или получения данных для проведения операции и/или доступа к защищаемой информации (коды доступа, коды SMSподтверждения и т.д.) с помощью методов социальной инженерии, т.е. методов доступа к защищаемой информации, основанных на особенностях психологии людей («Фишинг», «Дорожное яблоко», «Троянский конь» и т.д.), а также вследствие заражения устройства Клиента вредоносной программой.

3.5. Заражение устройства Клиента осуществляется также через спам-рассылку SMS или MMScообщения, сообщения электронной почты, сообщения, в том числе в мессенджерах, содержащих ссылки на внешние ресурсы, или при переходе по ссылкам на ресурсы сети «Интернет». При переходе по ссылкам вредоносная программа устанавливается на устройство Клиента.

3.6. Наибольший риск таких операций связан с тем, что в ряде случаев вредоносная программа скрывает от Клиента приходящие от Организации уведомления. Клиент, не зная о несанкционированной операции и/или доступе к защищаемой информации, не может направить в Организацию соответствующие возражения и пресечь несанкционированный доступ.

4. Меры по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства Клиента, контролю конфигурации устройства, и своевременному обнаружению воздействия вредоносной программы.

4.1. Меры по обеспечению защиты от несанкционированного доступа неуполномоченных лиц к устройству Клиента с которого осуществляется доступ к Системам дистанционного обслуживания.

4.1.1. При осуществлении доступа к Системе дистанционного обслуживания необходимо удостовериться в правильности указанного адреса в адресной строке браузера (исключить выход на сайты, внешне маскирующиеся под Систему дистанционного обслуживания, а также удостовериться в наличии значка защищенного соединения (замок).

4.1.2. Персональные стационарные компьютеры Клиента – юридического лица должно располагаться в помещении, в которое исключен несанкционированный доступ. При входе в помещение, в котором вход в Систему дистанционного обслуживания осуществляется в процессе выполнения сотрудниками Клиента трудовых функций в офисе, должно быть установлено средство регистрации и контроля доступа в виде электронного замка и видео-фиксации; посетителей всегда должен сопровождать кто-то из сотрудников Клиента.

4.1.3. Включенное устройство не должно оставаться без контроля при наличии иных лиц в помещении, пока происходит сеанс связи с Организацией.

4.1.4. Категорически не рекомендуется пользоваться Системой дистанционного обслуживания в местах с публичным доступом в сеть «Интернет» из-за отсутствия должной системы безопасности в вышеперечисленных заведениях.

4.1.5. Мобильное устройство Клиента не должно оставляться без присмотра, чтобы исключить несанкционированное использование мобильного приложения.

4.2. Меры по обеспечению защиты устройств Клиента от воздействия вредоносных программ.

4.2.1. Не рекомендуется переходить по ссылкам и/или устанавливать приложения/обновления безопасности, пришедшие по SMS/электронной почте, в том числе от имени Организации.

4.2.2. На устройство, в том числе мобильное, должно устанавливаться только лицензионное программное обеспечение; на устройство не должно устанавливаться

программное обеспечение, полученное из сомнительных источников (например, скачанное с файлообменников или торрентов).

4.2.3. На устройство, в том числе устройство мобильное, должно быть установлено лицензионное средство антивирусной защиты со своевременно обновляемыми антивирусными базами данных и проверкой по расписанию всех объектов системы; работать антивирусное программное обеспечение должно в автоматическом режиме; не реже одного раза в неделю должно проводиться полное антивирусное сканирование устройства; в случае обнаружения подозрительные файлы должны быть удалены, а при невозможности удаления – заблокированы; антивирусное программное обеспечение не должно отключаться ни при каких обстоятельствах; рекомендуется установить по умолчанию максимальный уровень политик безопасности, т. е. не требующий ответов пользователя при обнаружении вирусов.

4.2.4. На установленное на устройстве программное обеспечение должны своевременно устанавливаться обновления безопасности операционной системы устройства, а также обновления безопасности прикладного программное обеспечение (желательно в автоматическом режиме)

4.2.5. На устройства Клиента рекомендуется устанавливать только одну операционную систему, и только то программное обеспечение, которое необходимо для работы в Системе дистанционного обслуживания; на устройство не рекомендуется устанавливать программное обеспечение, содержащее средства разработки и отладки приложений, а также средства, позволяющие осуществлять несанкционированный доступ к системным ресурсам; пользователи не должны обладать правами локального администратора; настройку устройства Клиента (управление привилегиями, квотами, установка прав доступа пользователей и т.п.) должен выполнять специалист, обладающий необходимыми навыками по администрированию компьютерной техники и сети;

4.2.6. Рекомендуется соблюдать осторожность при получении сообщений с файламивложениями. Следует уделять внимание расширениям файлов. Файлы, зараженные вредоносной программой, часто маскируются под обычные графические, аудио, видео файлы или файлы приложений MS Office и pdf, а также архивы, содержащие вышеперечисленные файлы. Режим отображения расширении файлов должен быть включен постоянно. Не рекомендуется открывать вложения электронных писем, полученные от неизвестных вам адресатов. Такие письма лучше немедленно удалить, как и любые подозрительные сообщения.

4.2.7. При получении извещений о недоставке почтовых сообщений обращайте внимание на причину и, в случае автоматического оповещения о возможной отправке вируса, немедленно проверяйте устройство антивирусной программой на наличие вредоносных программ.

4.2.8. При использовании браузера не переходите по ссылке и не нажимайте кнопки во всплывающих окнах. При получении ссылок по электронной почте или в мессенджерах, рекомендуется скопировать ссылку, вставить в адресную строку используемого браузера и убедиться, что адрес соответствует интересующему запросу.

4.2.9. Рекомендуется избегать сайтов, которые могут иметь незаконное и/или вредоносное содержание. Не следует устанавливать и /или сохранять без предварительной антивирусной проверки файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте или полученные из иных ранее неизвестных пользователю источников.

4.2.10. Рекомендуется регулярно выполнять резервное копирование важной информации, а также иметь системный загрузочный диск на случай подозрения на заражение компьютера.

4.3. Требования, предъявляемые к паролям Клиента, в целях обеспечения защиты информации.

4.3.1. На устройство должна быть установлена парольная защита на вход в операционную систему.

4.3.2. При выборе пароля целесообразно соблюдать следующие требования:

1) пароль должен содержать не менее 8 символов;

2) пароль должен содержать как минимум по одному символу из букв нижнего и верхнего регистра, цифры и знаки препинания;

3) в качестве пароля не должен использоваться один и тот же повторяющийся символ, либо комбинация из нескольких рядом стоящих символов;

4) в качестве пароля не следует использовать имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, девичью фамилию матери и другие данные, которые могут быть подобраны неуполномоченными лицами путем анализа информации о пользователе;

5) пароль от операционной системы, а также пароль для входа в Систему дистанционного обслуживания рекомендуется менять каждые 45 календарных дней; не рекомендуется ставить один и тот же пароль на операционную систему и Систему дистанционного обслуживания;

6) не рекомендуется записывать пароли на бумажных носителях или в текстовых файлах на рабочем месте, оставлять их в легкодоступных местах, передавать неуполномоченным лицам;

7) не рекомендуется сохранять пароль от доступа к Системе дистанционного обслуживания в браузере;

8) пароль в обязательном порядке подлежит изменению в том случае, если он стал известен постороннему лицу или у пользователя есть подозрения, что пароль стал известен постороннему лицу.

4.4. Требования по обеспечению информационной безопасности, предъявляемые к ключевой информации Клиента.

4.4.1. В случае использования Клиентом ключа электронной подписи при взаимодействии с Организацией в рамках заключения и (или) исполнения договоров об оказании услуг на рынке ценных бумаг, ключевая информация (ключ электронной подписи) должна размещаться на сменном носителе информации (eToken PRO USB, Рутокен ЭЦП 2.0 и смарт-карта eToken ГОСТ). Размещение ключевой информации на жестком диске компьютера, на котором установлена Система дистанционного обслуживания, запрещено.

4.4.2. Съемный носитель информации с ключевой информацией должен быть установлен в считывающее устройство только во время работы в Системе дистанционного обслуживания. Размещение сменного носителя в считывающем устройстве вне сеансов работы в Системе дистанционного обслуживания должно быть исключено.

4.4.3. Съемный носитель информации с ключевой информацией должен использоваться только владельцем сертификата ключа проверки электронной подписи либо лицом, уполномоченным на использование такого сменного носителя.

4.4.4. Вся ответственность за конфиденциальность секретных ключей электронной подписи Клиента лежит на Клиенте, как на единственном владельце секретных ключей электронной подписи.

4.4.5. Не допускается: 1) снимать несанкционированные копии с носителей ключевой информации; 2) передавать носители ключевой информации лицам, к ним не допущенным; 3) записывать на носители ключевой информации постороннюю информацию.

4.5. Специальные рекомендации по обеспечению информационной безопасности при пользовании приложениями на мобильных устройствах Клиента.

4.5.1. Пароли (постоянные и одноразовые), мобильные коды для входа в мобильное приложение – это личная конфиденциальная информация пользователя, которая ни при каких обстоятельствах не подлежит раскрытию кому-либо, включая сотрудников Организации.

4.5.2. Категорически не рекомендуется сохранять мобильный код и постоянный пароль на мобильное устройство, на которых запускается мобильное приложение, применяемое для совершения финансовых операций.

4.5.3. Не рекомендуется сохранять мобильный код и постоянный пароль в текстовых файлах на компьютерах либо на других электронных носителях информации, т.к. при этом существует риск их кражи и компрометации.

4.5.4. При любых подозрениях на компрометацию мобильного кода или постоянного пароля посторонними лицами (в т. ч. представившимися сотрудниками Организации), следует незамедлительно обратиться в Организацию.

4.5.5. Рекомендуется своевременно устанавливать доступные обновления операционной системы и приложений на мобильное устройство.

4.5.6. Категорически не рекомендуется взламывать мобильное устройство, так как это отключает защитные механизмы, заложенные производителем мобильной платформы; в результате таких действий мобильное устройство становится уязвимым к заражению вредоносной программой.

4.5.7. Рекомендуется установить парольную защиту на мобильное устройство; данная возможность доступна для любых современных моделей мобильных устройств.

4.5.8. Рекомендуется завершать работу с мобильным приложением через завершение сессии.

4.5.9. В случае неожиданного прекращения работы SIM-карты телефона, следует незамедлительно обратиться к своему оператору сотовой связи для блокировки абонентского номера и замены SIM-карты, а также в Организацию для выявления возможных несанкционированных операций.

4.5.10. При утрате мобильного устройства, на которое установлено мобильное приложение, следует незамедлительно обратиться к своему оператору сотовой связи для блокировки SIM-карты, заблокировать доступ в мобильное приложение при помощи специалистов Организации, а также в Организацию для выявления возможных несанкционированных операций.

4.5.11. При смене номера телефона рекомендуется незамедлительно сообщить об этом в Организацию.

4.5.12. Рекомендуется регулярно контролировать состояние своих счетов и незамедлительно сообщать сотрудникам Организации обо всех подозрительных или несанкционированных операциях.

4.6. Действия Клиента при получении сообщений из Организации о несанкционированных операциях, утрате мобильного устройства и (или) компрометации ключевой информации.

4.6.1. Организация информирует Вас, что: - не осуществляет рассылку электронных писем с просьбой прислать ключи электронно-цифровой подписи или пароль; - не рассылает по электронной почте программы для установки на компьютеры Клиентов, а также ссылки или указания на установку приложений через SMS/MMS/E-mail - сообщения.

4.6.2. По всем случаям обнаружения подозрительных или несанкционированных операций, иных фактов, указанных в разделе 4 Рекомендаций, следует незамедлительно обратиться в Организацию по телефонам: 8 (4725) 46-15-42, 8-800-200-31-53, либо лично явиться в Организацию с целью блокирования паролей и (или) скомпрометированных ключей электронно-цифровой подписи с последующей их заменой.

4.6.3. Ни при каких обстоятельствах не рекомендуется отвечать на письма, якобы от имени Системы дистанционного обслуживания, Организации, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену http://www.finproinvest.ru , пересылать секретный ключ, пароль доступа к системе или сеансовый ключ, установить какое-либо ПО на устройство и т.д.; о факте подобного обращения следует немедленно сообщить Организации в рабочие часы Организации.

4.6.4. В случае поступления на мобильный номер телефона SMS-оповещения или электронного сообщения о совершенной операции, немедленно связаться с Организацией по указанным выше телефонам, иным каналам связи либо лично явиться в Организацию, если операция не была Вами осуществлена.

4.6.5. При подозрении на компрометацию ключевой информации, в случаях кадровых перестановок у клиента – юридического лица в отношении лиц, имевших доступ к Системе дистанционного обслуживания, компьютеру и ключам, при подозрениях в несанкционированном доступе, при обнаружении вируса необходимо немедленно обратиться в Организацию либо лично явиться в Организацию с целью блокирования паролей и (или) скомпрометированных ключей электронно-цифровой подписи с последующей их заменой.