РЕКОМЕНДАЦИИ

для клиентов АО «ДРАГА»

по обеспечению информационной безопасности,

защите информации от воздействия вредоносного кода при работе в сети «Интернет» и использовании электронных сервисов АО «ДРАГА»

в целях противодействия незаконным финансовым операциям

2020 г.

1. Общие положения

1.1. Настоящие Рекомендации по обеспечению информационной безопасности, защите информации от воздействия вредоносного кода при работе в сети «Интернет» и использовании электронных сервисов АО «ДРАГА» в целях противодействия незаконным финансовым операциям (далее – Рекомендации) разработаны АО «ДРАГА» (далее – Общество) в целях защиты финансовой и иной информации от воздействия вредоносных кодов (программ), от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети «Интернет», защиты от различных видов мошенничества, а также 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 17.04.2019 № 684-П.

1.2. Задачами Рекомендаций являются доведение до Клиентов Общества следующей информации:

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

1.2.2. 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 Общества посредством уведомления Клиентов в порядке, предусмотренном для уведомлений соответствующим договором об оказании услуг на рынке ценных бумаг и (или) путем размещения Рекомендаций на сайте Общества.

2. Основные определения и используемые сокращения

Антивирусная программа (антивирус, средство антивирусной защиты, средство обнаружения вредоносных программ) – специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ, восстановления зараженных (модифицированных) такими программами файлов и профилактики (предотвращения) заражения (модификации) файлов или операционной системы устройства Клиента вредоносным кодом.

Вредоносный код (вредоносная программа, вредоносное ПО, компьютерный вирус) - любой программный код (программное обеспечение), приводящий 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, программное обеспечение, средства вычислительной техники,

телекоммуникационное оборудование Клиентов - пользователей электронных сервисов Общества, 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 сотрудниками Общества и (или) Клиентами Общества; информация, необходимая Обществу для авторизации своих Клиентов в целях осуществления финансовых операций и удостоверения права Клиентов распоряжаться ценными бумагами, инвестиционными средствами, или иным имуществом; информации об осуществленных Обществом и его Клиентами финансовых операциях; ключевая информация средств криптографической защиты информации, используемая Обществом и его 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 к информации – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств[1], предоставляемых средствами вычислительной техники или автоматизированными системами.

Пользователь (Клиент) – обладатель защищаемой информации, используемой для проведения финансовых операций в рамках исполнения

[1] Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем

заключенных между Обществом и Клиентом договоров на обслуживание на рынке ценных бумаг.

Сайт Общества – официальный сайт Общества в сети «Интернет», размещенный по адресу https://draga.ru

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

Электронные сервисы Общества – сервисы, размещенные информационно-телекоммуникационной сети «Интернет» на официальном сайте Общества, предоставляющие Клиентам Общества услуги для проведения финансовых операций в рамках исполнения заключенных между Обществом и Клиентом договоров на обслуживание на рынке ценных бумаг (личный кабинет акционера, личный кабинет эмитента, личный кабинет инвестора и т.д.).

Устройство Клиента – устройство, с использованием которого Клиентом совершаются действия в целях осуществления финансовой операции. К таким устройствам относятся стационарные (настольные) персональные компьютеры, различного рода портативные (мобильные) компьютеры (ноутбуки), а также мобильные телефоны, смартфоны и т.д. (далее – мобильное устройство).

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 Клиентов 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 устройств Клиентов – пользователей электронных сервисов Общества от несанкционированного доступа осуществляется с целью исключения (минимизации) возможности:

3.2.1. появления в устройствах, с помощью которых осуществляется доступ к электронным сервисам Общества, вредоносных программ и программ, направленных на разрушение, блокирование, нарушение работоспособности или модификацию программного обеспечения электронных сервисов Общества, либо на перехват информации, в том числе паролей секретных ключей;

3.2.2. внесения несанкционированных изменений в технические и программные средства электронных сервисов Общества, а также в их состав;

3.2.3. внесения несанкционированных изменений в электронные документы или электронные сообщения, циркулирующие при взаимодействии Клиента с электронными сервисами Общества.

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 без согласия Клиента;

риск повреждения программного обеспечения Клиента, а также риск искажения, изменения, уничтожения или шифрования информации об активах (ценных бумагах, инвестициях и ином имуществе) и финансовых операциях Клиентов и Общества;

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 может быть реализован неуполномоченным лицом (злоумышленником) посредством как непосредственного, так и удаленного доступа к устройству Клиента.

3.5. Удаленный доступ к устройству Клиента реализуется в результате взлома защиты устройства или получения данных для проведения операции и/или доступа к защищаемой информации (коды доступа, коды SMS-подтверждения и т.д.) с помощью методов социальной инженерии, т.е. методов доступа к защищаемой информации, основанных на особенностях психологии людей («Фишинг», «Троянский конь», «Дорожное яблоко», и т.д.), а также вследствие заражения устройства Клиента вредоносной программой.

3.6. Для защиты от непосредственного несанционированного доступа к устройству рекомендуется: исключить возможность физического доступа к

нему неуполномоченных лиц, включить блокировку экрана на устройстве и отключить показ любых паролей при вводе.

3.7. Оптимальным способом защиты от методов социальной инженерии является своевременное выявление (распознавание) и противодействие способам этих злоумышленных действий. Основными способами получения несанкционированного доступа к защищаемой информации (методы, техники социальной инженерии) являются:

3.7.1. «Фишинг» – метод получения несанкционированного доступа путем использования ложных ресурсов сети «Интернет». Один из самых распространенных способов «Фишинга» заключается в отправке электронных писем лицами, которые выдают себя за представителей Общества либо эмитента, акционером которого является Клиент. Как правило, в электронных письмах от таких лиц содержится ссылка на небезопасную страницу сайта в сети «Интернет», на которой предлагается ввести свои личные данные. Клиент при этом предполагает, что ввод данных безопасен, но на самом деле информация похищается злоумышленниками.

3.7.2. «Троянский конь» – метод, предполагающий расчет злоумышленника на любопытство, алчность, страх и другие эмоции Клиента. В этих целях Клиенту отправляется по электронной почте письмо, во вложении которого находится «обновление» антивируса, ключ к денежному выигрышу, компромат на сотрудника и т.п.; на самом деле в письме находится вредоносная программа.

3.7.3. «Дорожное яблоко» – метод, представляющий собой адаптацию «троянского коня» и состоит в подбрасывании пользователю съемного носителя информации, зараженного вредоносной

программой. Чтобы у пользователя возник интерес к данному съемному носителю информации, на него наносятся логотип компании или какая-нибудь надпись, например, «данные о продажах», «зарплата сотрудников» и т.п.; при запуске съемного носителя информации, зараженного вредоносной программой, вредоносная программа устанавливается на устройство Клиента.

3.7.4. Кви про кво (услуга за услугу) – метод, предполагающий обращение злоумышленника к Клиенту по электронной почте или корпоративному телефону. Злоумышленник может представиться, например, сотрудником технической поддержки и информировать о возникновении технических проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В процессе «решения» такой проблемы, злоумышленник подталкивает жертву на совершение действий, позволяющих атакующему выполнить определенные команды или установить необходимое программное обеспечение на устройстве Клиента, являющимся жертвой.

3.7.5. «Обратная социальная инженерия» – метод, направленный на создание такой ситуации, при которой Клиент (жертва) вынужден будет сам обратится к злоумышленнику за «помощью». Например, злоумышленник может выслать письмо с телефонами и контактами «службы поддержки» и через некоторое время создать обратимые неполадки на Устройстве клиента (жертвы). Клиент в таком случае позвонит или свяжется по электронной почте с злоумышленником сам, и в процессе «исправления» проблемы злоумышленник сможет получить необходимые ему данные.

3.8. Заражение устройства Клиента может быть осуществлено также через спам-рассылку SMS или MMS-сообщения, сообщения электронной

почты, мессенджеров, содержащих ссылки на внешние ресурсы, или при переходе по ссылкам на ресурсы сети «Интернет». При переходе по ссылкам вредоносная программа устанавливается на устройство Клиента.

3.9. Наибольший риск таких операций связан с тем, что в ряде случаев вредоносная программа скрывает от Клиента приходящие от Общества уведомления. Клиент, не зная о несанкционированной операции и/или доступе к защищаемой информации, не может направить в Общество соответствующие возражения и предотвратить 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 электронным сервисам Общества:

4.1.1. При осуществлении доступа к электронным сервисам Общества необходимо удостовериться в правильности указанного адреса в адресной строке web-браузера (исключить выход на сайты, внешне маскирующиеся под электронные сервисы Общества), а также удостовериться в наличии значка защищенного соединения (изображение замка рядом с адресной строкой web-браузера).

4.1.2. Устройство Клиента - юридического лица, представляющее собой персональный компьютер, должно располагаться в помещении, исключающем несанкционированный доступ к устройству. При входе в помещение, в котором вход в электронные

сервисы Общества 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; нахождение посетителей в помещении должно осуществляться только в присутствии Клиента.

4.1.3. На устройстве, с которого осуществляется работа с электронными сервисами Общества, должен быть настроен безопасный вход в систему и блокировка сеанса при бездействии не более 15 минут.

4.1.4. Категорически не рекомендуется пользоваться электронными сервисами Общества в местах с публичным доступом в сеть «Интернет» из-за отсутствия должной системы безопасности в указанных заведениях.

4.1.5. Мобильное устройство Клиента не должно оставляться без присмотра, чтобы исключить несанкционированный вход в электронные сервисы Общества и применение приложения myDSS, используемого для подписания усиленной квалифицированной электронной подписью Клиента.

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 Общества.

4.2.2. На устройство, в том числе мобильное, должно устанавливаться только лицензионное программное обеспечение (далее – ПО). Установка ПО, полученного из сомнительных и недоверенных источников запрещена.

4.2.3. На устройство, в том числе мобильное, должно быть установлено лицензионное средство антивирусной защиты со своевременно обновляемыми антивирусными базами данных и проверкой по расписанию всех объектов системы. Работа антивирусного ПО должна осуществляться автоматическом режиме. Полное антивирусное сканирование устройства должно проводиться не реже одного раза в неделю. В случае обнаружения подозрительные файлы должны быть удалены, а при невозможности удаления – заблокированы. Антивирусное ПО должно функционировать постоянно. Для наиболее эффективной защиты устройства рекомендуется установить по умолчанию максимальный уровень политик безопасности, не требующий ответов пользователя при обнаружении вирусов.

4.2.4. Устройство должно быть защищено средством сетевой защиты (межсетевой экран, брандмауэр, файрвол), предназначенным для предотвращения несанкционированного или нежелательного сообщения устройства с компьютерными сетями (в том числе с сетями общего доступа и «Интернет»), а также с другими устройствами.

4.2.5. На установленное на устройстве ПО должны своевременно устанавливаться обновления безопасности операционной системы, а также обновления безопасности прикладного ПО.

4.2.6. На устройства Клиента рекомендуется устанавливать только одну операционную систему, и только то ПО, которое необходимо для работы с электронными сервисами Общества. На устройство не рекомендуется устанавливать ПО, содержащее средства разработки и отладки приложений, а также средства, позволяющие

осуществлять несанкционированный доступ к системным ресурсам устройства. Клиентам (пользователям устройств) при работе с устройством не рекомендуется обладать на устройстве правами привилегированного пользователя (локального/доменного администратора, root). 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.

4.2.7. Во время работы с электронными сервисами Общества рекомендуется отключить все неиспользуемые службы и процессы операционной системы Windows, в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, отключить гостевую локальную учетную запись («Гость», Guest), а на локальные учетные записи пользователей операционной системы – установить пароли, удовлетворяющие требованиям, установленным в п. 4.3.2. настоящих Рекомендаций. Рекомендуется активировать подсистему регистрации событий информационной безопасности. Подключение съемных носителей информации, не участвующих в работе с электронными сервисами Общества, рекомендуется отключить.

4.2.8. Рекомендуется соблюдать осторожность при получении сообщений с файлами-вложениями. 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. Рекомендуется в проводнике Windows включить режим отображения расширений

файлов. Не рекомендуется открывать вложения электронных писем, полученных от неизвестных адресатов. Такие письма и любые подозрительные сообщения рекомендуется немедленно удалять, не открывая.

4.2.9. При получении извещений о недоставке почтовых сообщений рекомендуется обращать внимание на причину и, в случае автоматического оповещения о возможной отправке вируса, немедленно проверять устройство антивирусной программой на наличие вредоносных программ.

4.2.10. При использовании web-браузера рекомендуется не переходить по ссылкам и не нажимать кнопки во всплывающих окнах. При получении ссылок по электронной почте или в мессенджерах, рекомендуется скопировать ссылку, вставить в адресную строку используемого web-браузера и убедиться, что адрес соответствует интересующему запросу. Также ссылку на вредоносное содержимое можно проверить на соответствующих бесплатных сервисах:

https://www.virustotal.com/gui/home/url

https://opentip.kaspersky.com/

4.2.11. 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 Клиенту источников.

4.2.12. Рекомендуется регулярно выполнять резервное копирование важной информации, хранимой на устройстве Клиента.

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

4.3.1. На устройстве для авторизации пользователя должна быть установлена парольная защита (на мобильном устройстве может применяться иная защита – пин-код, графическая или биометрическая).

4.3.2. При выборе пароля целесообразно соблюдать следующие требования:

- пароль должен содержать не менее 8 символов;
- пароль должен содержать как минимум по одному символу из букв нижнего и верхнего регистра, цифры и знаки препинания;
- в качестве пароля не должен использоваться один и тот же повторяющийся символ, либо комбинация из нескольких рядом стоящих символов;
- 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;
- пароль от операционной системы, а также пароль для входа в электронные сервисы Общества рекомендуется менять каждые 45 календарных дней; не рекомендуется ставить

один и тот же пароль на операционную систему и электронные сервисы Общества;

- не рекомендуется записывать пароли на бумажных носителях или в текстовых файлах на рабочем месте, оставлять их в легкодоступных местах, передавать неуполномоченным лицам;
- не рекомендуется сохранять пароли для доступа к электронным сервисам Общества в web-браузере;
- пароль в обязательном порядке подлежит изменению в том случае, если он стал известен постороннему лицу или у Клиента есть подозрения, что пароль стал известен постороннему лицу.

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

4.4.1. Работа Клиентов с электронными сервисами Общества осуществляется с применением облачной усиленной квалифицированной электронной подписи (далее – УКЭП), закрытый ключ которой хранится в специализированном удаленном сервисе («облаке») удостоверяющего центра. Применение Клиентом выданной ему УКЭП производится с использованием мобильного устройства Клиента с установленным на нем приложением MyDSS. Требования по обеспечению информационной безопасности, предъявляемые к ключевой информации Клиента, изложены в контексте использования Клиентом при работе с электронными сервисами Общества облачной УКЭП.

4.4.2. При использовании web-браузера в качестве интерфейса для осуществления доступа к сервису облачной УКЭП рекомендуется отключить функцию автоматического сохранения пароля и логина.

4.4.3. При осуществлении доступа к сервису облачной УКЭП необходимо удостовериться в правильности указанного адреса в адресной строке web-браузера, а также удостовериться в наличии значка защищенного соединения (изображение замка рядом с адресной строкой web-браузера).

4.4.4. Категорически не рекомендуется использовать для доступа к сервису облачной УКЭП мобильные устройства с «рутованной» версией прошивки Android или произведенной операцией Jailbreak для мобильных устройств от Apple. Модифицированные и не поддерживаемые официальном производителем прошивки для мобильных устройств могут содержать в себе закладки или недокументированные возможности, которые злоумышленник при определенных условиях с успехом сможет использовать. Не рекомендуется устанавливать приложения из посторонних источников, а по возможности рекомендуется минимизировать список установленного программного обеспечения на мобильном устройстве.

4.4.5. Категорически запрещается сообщать посторонним лицам, в том числе сотрудникам Общества или службе поддержки, коды, смс-сообщения, парольные и контрольные фразы, необходимые для доступа к сервису облачной УКЭП.

4.4.6. Мобильное устройство с установленным приложением MyDSS, используемое для доступа и работы с электронными сервисами

Общества, должно использоваться только владельцем сертификата ключа проверки электронной подписи.

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 Клиента, которая ни при каких обстоятельствах не подлежит раскрытию кому-либо, включая сотрудников Общества.

4.5.2. Категорически не рекомендуется сохранять мобильный код и постоянный пароль на мобильных устройствах, применяемых Клиентами для доступа в электронные сервисы Общества, а также в текстовых файлах и иных электронных носителях в связи с риском их кражи, компрометации и утечки защищаемой информации.

4.5.3. При любых подозрениях на компрометацию мобильного кода или постоянного пароля посторонними лицами (в т. ч. представившимися сотрудниками Общества), Клиенту следует незамедлительно обратиться в Общество.

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

4.5.5. Категорически не рекомендуется взламывать мобильное устройство (например, через Jailbreaking или Rooting – процесс, который предоставляет получение прав суперпользователя операционной системы мобильного устройства), т.к. это отключает защитные механизмы, заложенные производителем мобильной

платформы. В результате таких действий мобильное устройство становится уязвимым к заражению вредоносным ПО.

4.5.6. Рекомендуется установить парольную защиту на мобильное устройство в соответствии с п. 4.3.1. настоящих Рекомендаций.

4.5.7. Рекомендуется завершать работу с электронными сервисами Общества через завершение сессии.

4.5.8. 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 Общество для выявления возможных несанкционированных операций.

4.5.9. При утрате мобильного устройства, используемого для работы с электронными сервисами Общества, следует незамедлительно обратиться к своему оператору сотовой связи для блокировки SIM-карты, а также в Общество для блокировки доступа в электронные сервисы Общества и выявления возможных несанкционированных операций.

4.5.10. При смене номера телефона рекомендуется незамедлительно обратиться в Общество для перерегистрации номера телефона в соответствии с регламентами и правилами, утвержденными Обществом для пользования электронными сервисами Общества.

4.5.11. Рекомендуется регулярно контролировать состояние своих счетов и незамедлительно сообщать в Общество по Единому телефону технической поддержки, указанному в п. 4.6.1. настоящих Рекомендаций, обо всех подозрительных или несанкционированных операциях.

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

4.6.1. По всем случаям обнаружения подозрительных или несанкционированных операций, иных фактов, указанных в разделе 4 Рекомендаций, следует незамедлительно обратиться в Общество по телефону: (495) 123-30-90, либо лично явиться в Общество с целью блокирования паролей и (или) скомпрометированных ключей электронно-цифровой подписи с последующей их заменой.

4.6.2. Ни при каких обстоятельствах не рекомендуется отвечать на письма, якобы от имени электронных сервисов Общества, Общества, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену https://www.draga.ru, переслать ключевую фразу, используемую для многофакторной аутентификации, пароли, используемые для доступа к электронным сервисам Общества, СМС сообщения, присылаемые Сервисом электронной подписи, установить какое-либо ПО на устройство и т.д. О факте подобного обращения следует немедленно сообщить в Общество.

4.6.3. В случае поступления на мобильный номер телефона SMS-оповещения или электронного сообщения об операции, совершенной без согласия Клиента (не инициированной Клиентом), немедленно сообщить об этом в Общество по телефону, указанному в п. 4.6.1., по иным каналам связи либо лично явиться в любой офис Общества.

4.6.4. При подозрении на компрометацию ключевой информации, в случаях кадровых перестановок у Клиента – юридического лица в отношении лиц, имевших доступ к электронным сервисам Общества, устройствам Клиента, в том числе мобильным, и ключам электронной подписи, при подозрениях в несанкционированном доступе, при обнаружении вредоносного ПО (компьютерного вируса) необходимо немедленно обратиться в Общество либо лично явиться в любой из офисов Общества с целью блокирования паролей и (или) скомпрометированных ключей электронно-цифровой подписи с последующей их заменой.