Платформа цифровых активов

Общество с ограниченной ответственностью
«Токены – Цифровые Инвестиции» (ООО «Токены»)

УТВЕРЖДЕНЫ

приказом от 02.10.2026 № 25202-П

РЕКОМЕНДАЦИИ

по информационной безопасности при осуществлении финансовых операций для клиентов Общества с ограниченной ответственностью «Токены – Цифровые Инвестиции»

(версия 1.0)

Москва, 2026

ИСТОРИЯ ИЗМЕНЕНИЙ ДОКУМЕНТА

Дата утверждения	Номер приказа	Номер версии	Изменения
02.10.2026	25202-П	1.0	Утверждение документа

СОДЕРЖАНИЕ

1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ 4
2. ОБЩИЕ ПОЛОЖЕНИЯ....4
3. МЕРЫ ПО ЗАЩИТЕ УСТРОЙСТВ КЛИЕНТА 7
4. МЕРЫ ПО ЗАЩИТЕ МОБИЛЬНОГО (ПЕРЕНОСНОГО) УСТРОЙСТВА КЛИЕНТА....9
5. МЕРЫ ПО ОБЕСПЕЧЕНИЮ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ ..10
6. ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» 11
7. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОДПИСЬЮ....12

1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Для целей настоящих Рекомендаций по информационной безопасности при осуществлении финансовых операций для клиентов Общества с ограниченной ответственностью «Токены – Цифровые Инвестиции» (далее – настоящий документ) используются следующие понятия, определения и сокращения:

Вредоносный код – компьютерная программа, предназначенная для внедрения в автоматизированные (информационные) системы, программное обеспечение, средства вычислительной техники, мобильные (переносные) устройства (сотовые телефоны, смартфоны, коммуникаторы, планшетные компьютеры) и телекоммуникационное оборудование, используемые Клиентами, приводящая к несанкционированному уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации, а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи информации.

Клиент – юридическое или физическое лицо, в т.ч. индивидуальный предприниматель (резидент или нерезидент Российской Федерации), пользующееся финансовыми услугами и (или) сервисами, предоставляемыми Обществом.

Общество – Общество с ограниченной ответственностью «Токены – Цифровые Инвестиции».

Иные термины, не определенные в настоящем разделе, применяются в значениях, установленных законодательством Российской Федерации, а при отсутствии таковых – в их общеупотребительном значении.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Целью настоящего документа является информирование Клиентов:

– о необходимости соблюдения рекомендаций по информационной безопасности, приведенных в настоящем документе, при осуществлении финансовых операций используя услуги и (или) сервисы Общества (далее – финансовые операции), с целью противодействия незаконным финансовым операциям;

– о необходимости своевременного обнаружения воздействия Вредоносного кода и обеспечения защиты устройств Клиента от воздействия Вредоносного кода, приводящего к нарушению штатного функционирования средств вычислительной техники и устройств Клиента;

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

– о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) и (или) контроле конфигурации устройства, с использованием которого Клиентом совершаются действия в целях осуществления финансовых операций.

2.2. Реализация и выполнение Клиентом совокупности мер и рекомендаций, отраженных в настоящем документе, направленных на непосредственное обеспечение защиты информации, позволяет снизить в

значительной степени риски, связанные с нарушением информационной безопасности, включая снижение возможности получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

2.3. Соблюдение рекомендаций, отраженных в настоящем документе, позволит Клиентам в целом снизить риски информационной безопасности и минимизировать негативные последствия, связанные с возможным нарушением целостности и конфиденциальности информации, но не гарантирует абсолютной невозможности нарушения информационной безопасности (обеспечения подтверждения подлинности, конфиденциальности, целостности и доступности информации).

2.4. Нарушения в области защиты информации и информационной безопасности, влияющие на бизнес-процессы Клиента, а также на целостность, доступность и конфиденциальность информации, могут быть обусловлены следующими основными факторами:

– воздействие Вредоносного кода на устройства, применяемые для информатизации бизнес-процессов, с использованием которых Клиентом совершаются финансовые операции;

– несанкционированный доступ к информации Клиента лицами, не обладающими на это правом, а также осуществление указанными лицами финансовых операций;

– хищение или утеря ключей электронной подписи Клиента (в том числе, носителей ключей электронной подписи Клиента), с использованием которых осуществляются финансовые операции;

– совершение в отношении Клиента иных противоправных действий, связанных с нарушением информационной безопасности.

2.5. При осуществлении финансовых операций Клиенту необходимо принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом на их осуществление. Такие риски могут быть обусловлены (включая, но не ограничиваясь) следующими причинами:

– кража идентификатора доступа и пароля или иных конфиденциальных данных Клиента (например, ключей электронной подписи и (или) шифрования, CVC/CVV номера карты и т.п.) посредством технических средств и (или) Вредоносного кода, и использование злоумышленниками указанных данных с других устройств для осуществления несанкционированного доступа;

– внедрение в устройство Клиента и (или) каналы связи, с использованием которых совершаются финансовые операции, Вредоносного кода, который позволит злоумышленникам осуществить финансовые операции от имени Клиента;

– кража или несанкционированный доступ к устройству, с использованием которого Клиент пользуется услугами и (или) сервисами Общества, для получения данных и (или) несанкционированного доступа к сервисам Общества с этого устройства;

– использование злоумышленником утерянного или украденного сотового телефона (смартфона) Клиента или SIM-карты от него, для получения

SMS-кодов, которые могут применяться Обществом в качестве дополнительной защиты от несанкционированных финансовых операций, в целях преодоления указанной защиты;

– получение идентификатора доступа и пароля, и (или) SMS-кода, и (или) кодового слова, и прочих конфиденциальных данных (например, номеров счетов, паспортных данных и т.д.) путем обмана и (или) злоупотребления доверием, когда злоумышленник используя методы социальной инженерии представляется по телефону, например, сотрудником Общества или техническим специалистом, или использует иную легенду и просит Клиента сообщить ему указанные данные, или направляет, например, фальсифицированные сообщения от имени Общества по электронной почте, либо письмом по обычной почте, либо в виде SMS-сообщения, с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства, используемого Клиентом для осуществления финансовых операций, либо для информационного обмена с Обществом;

– перехват электронных сообщений и получение несанкционированного доступа к отчетам, выпискам и прочей финансовой информации в случае, если электронная почта Клиента используется для информационного обмена с Обществом;

– получение несанкционированного доступа к электронной почте Клиента в целях отправки фальсифицированных сообщений от имени Клиента в Общество;

– совершение Клиентом финансовых операций не через официальные сервисы (например, официальный сайт, личный кабинет, мобильное приложение), принадлежащие Обществу, вне зависимости от их визуальной схожести, схожести названия и (или) адреса в информационно-телекоммуникационной сети «Интернет».

2.6. Настоящий документ разработан с учетом требований положения Банка России от 20 апреля 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».

2.7. Рекомендации, представленные в настоящем документе, действуют в части, применимой к текущей деятельности Общества, как оператора информационной системы для выпуска цифровых финансовых активов. В связи с тем, что требования информационной безопасности также могут быть отражены в договорах, политиках, положениях, регламентах, правилах и иных документах Общества, регламентирующих предоставление услуг и (или) сервисов, настоящий документ действует в части, не противоречащей положениям внутренних документов Общества.

2.8. Клиентам рекомендуется внимательно изучить договор, заключенный с Обществом, приложения к договору и иные документы (в частности, размещенные на официальном сайте Общества в информационно-телекоммуникационной сети «Интернет» по адресу https://tokeon.ru/documents), связанные с исполнением договора, ознакомиться с разделами, посвященными обеспечению информационной безопасности и конфиденциальности.

2.9. Клиентам рекомендуется поддерживать в актуальном состоянии свою контактную информацию, предоставленную Обществу, чтобы в случае необходимости работники Общества могли оперативно связаться с Клиентом.

2.10. Клиентам рекомендуется проводить профилактические мероприятия, направленные на повышение уровня информационной безопасности и повышения уровня осведомленности в вопросах защиты информации.

2.11. Настоящий документ доводится до сведения Клиентов путем размещения на официальном сайте Общества в информационно-телекоммуникационной сети «Интернет» и (или) посредством уведомления Клиентов способом, определяемым Обществом самостоятельно.

2.12. Положения настоящего документа имеют рекомендательный характер. Соблюдение и (или) несоблюдение Клиентом изложенных в настоящем документе рекомендаций не порождает для Общества обязанности по возмещению убытков, расходов или иного ущерба, причиненного Клиенту в результате действий и (или) бездействия Клиента, третьих лиц, а также иных обстоятельств, не зависящих от Общества. Общество не гарантирует отсутствие рисков информационной безопасности при исполнении Клиентом рекомендаций, приведенных в настоящем документе.

3. МЕРЫ ПО ЗАЩИТЕ УСТРОЙСТВ КЛИЕНТА

3.1. Для снижения риска финансовых потерь Общество рекомендует Клиенту обеспечить защиту устройств, с которых Клиент пользуется услугами и (или) сервисами Общества для осуществления финансовых операций, в том числе путем:

– установки (инсталляции) и использования только лицензионного программного обеспечения (например, операционной системы, системного и прикладного программного обеспечения и т.д.), полученного из доверенных источников;

– своевременного обновления операционной системы[1], системного и прикладного программного обеспечения, установленных на устройствах Клиента, особенно в части обновлений безопасности, установка которых, в том числе, направлена на снижение рисков заражения устройства Вредоносным кодом;

– запрета на загрузку и установку (инсталляцию) программного обеспечения из недоверенных и непроверенных источников;

– наличия на устройствах Клиента своевременно обновляемых средств защиты информации, таких как: антивирусное программное обеспечение (с регулярно и своевременно обновляемыми антивирусными базами данных)[2], персональный межсетевой экран, средства защиты от несанкционированного доступа, средства контроля конфигурации устройства и пр.;

---

[1] На устройствах рекомендуется использовать современные операционные системы, которые являются более защищенными, в отличие от предыдущих устаревших версий

[2] Следует регулярно (не менее одного раза в неделю) осуществлять полную антивирусную проверку устройства, а также проверку на наличие Вредоносного кода любого программного обеспечения перед его установкой (инсталляцией) на устройство

– настройки прав доступа к устройствам Клиента с целью предотвращения к ним несанкционированного доступа, в том числе, путем исключения (ограничения) возможности дистанционного (удаленного) подключения к устройствам со стороны третьих лиц;

– организации хранения и использования устройств Клиента таким образом, чтобы максимально избегать рисков их кражи и (или) утери.

3.2. Для обеспечения защиты устройств, с которых Клиент пользуется услугами и (или) сервисами Общества для осуществления финансовых операций, рекомендуется использовать парольную защиту[3].

При этом необходимо соблюдать следующие требования:

– самостоятельно выбирать пароли;

– использовать сложные пароли, требующие ввода как минимум по одному символу из заглавных и прописных букв, цифр и специальных символов, в общем количестве не менее 8 символов;

– не использовать в качестве пароля один и тот же повторяющийся символ, либо комбинацию из нескольких рядом стоящих символов;

– проводить регулярную смену паролей (рекомендуется осуществлять смену пароля каждые 45 календарных дней);

– в обязательном порядке производить внеплановую смену пароля, если он стал известен постороннему лицу или если у Клиента есть подозрение, что пароль стал известен постороннему лицу.

Общество не рекомендует:

– в качестве паролей использовать свои имя и фамилию, имена близких лиц, клички домашних животных, даты рождения и другие памятные даты, номер телефона и автомобиля, девичью фамилию матери и другие данные, т.е. все то, что может быть легко подобрано злоумышленниками путем анализа информации о Клиенте и его окружении;

– устанавливать один и тот же пароль для доступа к устройству и другим информационным системам и мобильным приложениям;

– сохранять пароли в открытом (не защищенном) виде в текстовых файлах на устройстве либо иных электронных носителях информации, а также записывать пароли на бумажных носителях;

– хранить пароль совместно с устройством;

– оставлять пароли в легкодоступных местах, а также передавать любым третьим лицам пароли и (или) коды доступа к устройствам.

3.3. Не рекомендуется сразу после подключения к устройству открывать съемный носитель информации, без его предварительной полной проверки на наличие Вредоносного кода.

3.4. Не рекомендуется использовать устройство для посещения Интернет-сайтов сомнительного содержания, а также непроверенных и небезопасных Интернет-ресурсов. Это может привести к неправомерной загрузке на устройство Вредоносного кода.

3.5. В случае обнаружения Клиентом на устройстве Вредоносного кода, Общество рекомендует прекратить его использование до момента полного удаления обнаруженного Вредоносного кода с устройства.

---

[3] Или иной способ дополнительной защиты для доступа к устройству, например, двухфакторную аутентификацию

3.6. При подозрении на несанкционированный доступ под идентификационными данными Клиента к услугам и (или) сервисам Общества, и (или) компрометацию устройства, с которого Клиент пользуется услугами и (или) сервисами Общества для осуществления финансовых операций, необходимо сменить пароль от идентификатора доступа воспользовавшись другим доверенным устройством и (или) заблокировать доступ, обратившись в Общество.

3.7. Клиенту рекомендуется организовать выполнение требований[4] технической и эксплуатационной документации производителей и поставщиков оборудования, программного обеспечения и услуг связи.

3.8. Для осуществления финансовых операций Клиенту рекомендуется использовать отдельное, максимально защищенное устройство, доступ к которому есть только у Клиента.

4. МЕРЫ ПО ЗАЩИТЕ МОБИЛЬНОГО (ПЕРЕНОСНОГО) УСТРОЙСТВА КЛИЕНТА

4.1. Для снижения риска финансовых потерь Общество рекомендует (дополнительно к мерам, указанным в п. 3 настоящего документа) Клиентам обеспечить защиту мобильных (переносных) устройств (сотовых телефонов, смартфонов, коммуникаторов, планшетных компьютеров), с которых Клиент пользуется услугами и (или) сервисами Общества для осуществления финансовых операций:

– не оставлять мобильное (переносное) устройство без присмотра, чтобы исключить возможность его несанкционированного использования;

– устанавливать (инсталлировать) мобильные приложения только из официальных магазинов приложений и использовать только официальные мобильные приложения, в том числе официальное мобильное приложение Общества;

– не переходить по ссылкам и не устанавливать мобильные приложения и (или) обновления к ним (в том числе, обновления безопасности), пришедшие в SMS-сообщениях и PUSH-уведомлениях или по электронной почте, в том числе от имени Общества;

– установить пароль[5] для доступа к мобильному (переносному) устройству и мобильному приложению, которое Клиентом используется для получения услуг и (или) сервисов Общества в рамках осуществления финансовых операций.

4.2. При утрате или краже мобильного (переносного) устройства Клиента (SIM-карты от него), используемого для получения SMS-кодов и (или) доступа к услугам и (или) сервисам Общества для осуществления финансовых операций через соответствующее мобильное приложение Общества, Клиенту следует:

– незамедлительно проинформировать Общество по контактному телефону Общества, указанному в договоре и (или) на официальном сайте Общества в информационно-телекоммуникационной сети «Интернет»;

---

[4] В части обеспечения информационной безопасности

[5] Пароль должен удовлетворять требованиям к сложности и правилам хранения, приведенным в п. 3.2 настоящего документа

– по возможности оперативно (с учетом прочих рисков и особенностей использования мобильного (переносного) устройства) заблокировать и перевыпустить SIM-карту, произвести смену пароля в мобильном приложении Общества.

4.3. Рекомендуется контролировать мобильное (переносное) устройство, используемое Клиентом для получения SMS-кодов и (или) PUSH-уведомлений. В случае выхода из строя SIM-карты рекомендуется незамедлительно обратиться к оператору связи для уточнения причин и восстановления связи.

5. МЕРЫ ПО ОБЕСПЕЧЕНИЮ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

5.1. Полученные Клиентом от Общества данные, предназначенные для аутентификации Клиента (например, идентификатор доступа и установленный Клиентом для него пароль, ключ электронной подписи, коды из SMS-сообщений, кодовые слова (фразы), иные конфиденциальные данные, используемые Обществом для идентификации Клиента при оказании услуг и (или) предоставлении сервиса для осуществления финансовых операций), следует хранить в тайне с принятием необходимых мер, направленных на предотвращение их разглашения. В случае компрометации указанных данных Клиенту следует незамедлительно принять меры для их смены или блокировки, а также уведомить Общество о такой компрометации.

5.2. Следует не допускать использование в качестве паролей, ключевых слов (фраз), ответов на контрольные вопросы ранее использовавшиеся пароли и кодовые фразы, а также данные, которые могут быть прямо или косвенно сопоставлены с информацией о Клиенте и быть известны третьим лицам, а также сочетания, которые могут быть подобраны перебором.

5.3. При осуществлении финансовых операций, Клиенту необходимо не допускать публичного доступа к конфиденциальной информации, включая возможность дистанционного наблюдения, нахождение в прямой видимости систем видеонаблюдения.

5.4. Необходимо соблюдать принцип разумного раскрытия идентификационных данных (в том числе, персональных данных), а в случае запроса у Клиента указанной в п. 5.1 настоящего документа информации (следует иметь в виду, что от лица сотрудников Общества не могут поступать звонки или сообщения, в которых от Клиента требуют передать или предоставить SMS-код, пароль, кодовое слово[6] и другие идентификаторы доступа), в связи с оказанием Обществом услуг и (или) предоставления сервиса для осуществления финансовых операций, Клиенту рекомендуется по возможности оценить ситуацию и уточнить полномочия запрашивающего лица и процедуру предоставления запрашиваемой информации через независимый канал связи, например, по контактному номеру телефона Общества, указанному в договоре и (или) на официальном сайте Общества в информационно-телекоммуникационной сети «Интернет».

[6] Кодовое слово может быть запрошено только, если Клиент сам позвонил на контактный номер Общества, для проведения дополнительной идентификации Клиента

5.5. В следующих случаях, рекомендуется проявлять бдительность и должную осторожность:

– при получении электронных писем, SMS-сообщений и PUSH-уведомлений со ссылками и (или) вложениями, которые могут привести к заражению устройства Клиента Вредоносным кодом, который может обеспечить доступ к любым данным и программному обеспечению на устройстве Клиента, а также позволит злоумышленнику выполнять на «зараженном» устройстве Клиента любые действия;

– при проверке адресата (и темы сообщений), от которого пришло электронное письмо, т.к. входящее письмо может быть направлено злоумышленником, который маскируется под Общество или иных доверенных лиц;

– при посещении и работе на Интернет-сайтах, т.к. с них на устройство Клиента может быть загружен Вредоносный код;

– при использовании сетей (каналов) связи общего доступа, при подключении к общедоступным недоверенным Wi-Fi сетям (например, в гостиницах, офисных центрах, Интернет-кафе и т.д.), существует риск компрометации устройства Клиента и перехвата доступа к финансовым сервисам Общества;

– при работе (скачивании, запуске, открытии и т.п.) с файлами из новых и непроверенных источников (в том числе с архивами защищенными паролем, зашифрованными файлами и архивами, в связи с тем, что подобного рода файлы не могут быть проверены антивирусным программным обеспечением, установленным на устройство Клиента, в автоматическом режиме);

– не осуществлять финансовые операции через недоверенные устройства, т.к. они могут содержать Вредоносный код, осуществляющий сбор паролей и идентификаторов доступа или способны осуществлять подмену проводимых операций;

– осуществлять мониторинг средств массовой информации и официального сайта Общества об информации о последних выявленных критических уязвимостях и Вредоносном коде для ее принятия к сведению;

– не открывать полученное электронное письмо, если нет уверенности в том, что оно пришло из надежного и доверенного источника;

– не стоит доверять дружественному тону электронных сообщений или уведомлениям о срочности содержащейся в них просьбы;

– не следует выполнять какие-либо действия, если в полученном электронном письме сообщается, что проблема требует безотлагательного решения, для чего требуется срочно открыть приложенный файл, имеющий расширение *.exe или любой другой исполняемый файл.

6. ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

6.1. Не рекомендуется вводить любую персональную информацию на подозрительных и недоверенных Интернет-сайтах, а также других неизвестных Клиенту ресурсах информационно-телекоммуникационной сети «Интернет».

6.2. Не рекомендуется сохранять пароли в памяти Интернет-браузеров.

6.3. Не рекомендуется нажимать на баннеры и всплывающие окна, в том числе содержащие рекламу, возникающие во время работы с ресурсами информационно-телекоммуникационной сети «Интернет». Предпочтительнее настроить Интернет-браузер на автоматическую блокировку таких окон.

6.4. Следует внимательно относиться к не характерным, странным и непонятным сообщениям об ошибках Интернет-браузера. В случае возникновения подозрений Клиенту следует осуществить полную антивирусную проверку устройства.

6.5. При наличии на устройстве Клиента программ фильтрации сетевого трафика (брандмауэра) рекомендуется держать его включенным и блокировать все незнакомые или подозрительные подключения.

6.6. При посещении официального сайта Общества (как и других Интернет-ресурсов) следует удостовериться в том, что сертификат безопасности сайта действителен, а соединение происходит в защищенном режиме (адресная строка Интернет-браузера начинается с https, либо используется пиктограмма в виде замка).

6.7. Рекомендуется использовать надежно защищенные и доверенные сети (каналы) связи.

7. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОДПИСЬЮ

7.1. Для защиты ключей электронной подписи Клиента от хищения, например, с использованием Вредоносного кода, рекомендуется для их записи и хранения использовать сертифицированные ключевые носители информации – USB-токены (например, Рутокен ЭЦП, Рутокен S, Рутокен Lite и т.д.).

7.2. В случае отсутствия USB-токена, хранилище с ключом электронной подписи рекомендуется сохранить на съемном носителе информации (USB-накопителе), для которого необходимо выполнять меры, направленные на отсутствие несанкционированного доступа к USB-накопителю. Не допускается сохранять хранилище с ключом электронной подписи в местах, где к нему может получить доступ третьи лица.

7.3. Пароль на доступ к ключу электронной подписи должен быть известен только владельцу ключа электронной подписи. Пароль должен удовлетворять требования к сложности и правилам хранения, приведенным в п. 3.2 настоящего документа.

7.4. Рекомендуется осуществлять подключение носителя с ключом электронной подписи к устройству Клиента только в момент осуществления финансовых операций (после совершение которых носитель с ключом электронной подписи необходимо извлечь из устройства). В остальных случаях не следует допускать постоянного и бесконтрольного подключения носителя с ключом электронной подписи к устройству Клиента.

7.5. Не следует кому-либо осуществлять передачу носителя с ключом электронной подписи, а также не оставлять его без присмотра.

7.6. Не рекомендуется использовать носитель с ключом электронной подписи в Интернет-кафе и прочих общественно-доступных местах, а также на

устройстве, которое не принадлежит Клиенту, если нет уверенности в его безопасной настройки и эксплуатации в соответствии с рекомендациями, приведенными в п. 3 настоящего документа.

7.7. При возникновении любых подозрений на компрометацию ключа электронной подписи и (или) устройства, на котором он использовался, необходимо сообщить в Общество для принятия решения о необходимости блокировки (или отзыва[7]) ключа электронной подписи.

[7] В соответствии с правилами, отраженными в договоре, приложениях к договору и иных документах Общества, связанных с исполнением договора