УТВЕРЖДЕНО

Генеральным директором

ООО УК «Джи Пи Ай»

Приказ № 1В/1

от «10» января 2020 г.

Рекомендации по соблюдению клиентами Общества с ограниченной ответственностью «Управляющая компания «Джи Пи Ай» правил информационной безопасности

Настоящие Рекомендации по соблюдению клиентами Общества с ограниченной ответственностью «Управляющая компания «Джи Пи Ай» (далее – Управляющая компания) требований к информационной безопасности при использовании услуг Управляющей компании разработано 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 17.04.2019 года № 684-П и подлежат доведению до сведения клиентов Управляющей компании.

1. Уведомление о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями третьих лиц.

1.1. Клиенты Управляющей 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 (например, вследствие хищения) носителей информации, ключей электронной подписи, с использованием которых осуществляется взаимодействие с Управляющей компанией;

– воздействие вредоносного кода (вредоносных программ, приложений) на устройства клиента, с которых совершаются финансовые операции или осуществляется взаимодействие с Управляющей компанией (планшет, мобильный телефон и т.д., далее – устройство);

– совершение в отношении клиента иных противоправных действий.

1.2. При взаимодействии с Управляющей компанией и осуществлении операций клиентам следует принимать во внимание риск получения третьими лицами несанкционированного доступа к информации с целью осуществления ими несанкционированных операций с имуществом клиентов. Такие риски могут возникать, в том числе, вследствие следующих событий:

– кража пароля или иного идентификатора доступа, иных конфиденциальных данных, с помощью специальных устройств и/или вредоносного кода и использование злоумышленниками указанных данных для несанкционированного доступа;

– установка на устройство вредоносного кода, который позволит злоумышленникам осуществить операции от имени клиента Управляющей компании;

– кража или несанкционированный доступ к устройству, посредством которого клиент может пользоваться услугами Управляющей компании для получения данных и/или несанкционированного доступа к услугам с этого устройства.

– несанкционированное получение злоумышленниками персональных данных клиента. Описанный риск может реализоваться, помимо прочего, когда злоумышленник представляется сотрудником Управляющей компании или техническим специалистом, или использует иную легенду и просит клиента сообщить ему конфиденциальные данные или направляет поддельные почтовые сообщения с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;

– перехват почтовых сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если электронная почта клиента используется для информационного обмена с Управляющей компанией. В случае получения доступа к почте клиента - отправка сообщений Управляющей компании от его имени.

1.3. Описанные выше риски, связанные с утратой и компрометацией учётных данных несет владелец таких данных.

2. Меры по предотвращению несанкционированного доступа к защищаемой информации.

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

2.1.1. Обеспечение надлежащей защиты устройства, с помощью которого клиенты пользуются услугами Общества и обмениваются информацией с Обществом:

– 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 прочих;

– 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 Общества, после удаления с устройства обнаруженного вредоносного программного обеспечения;

– передача защищаемой информации клиентов только через безопасные беспроводные беспроводные сети. Работая в общедоступных беспроводных сетях клиентам не следует вводить учетные данные, используемые для доступа к услугам Общества.

2.1.2. Обеспечение конфиденциальности защищаемой информации:

– хранение в тайне идентификационных данных и ключевой информации, полученных от Общества. В случае компрометации указанных данных клиенту следует принять меры для смены таких данных и/или уведомления Общества о их компрометации;

– соблюдение принципа разумного раскрытия информации о номерах счетов, паспортных данных, иной информации. В случае запроса у клиента указанной информации в связи с оказанием услуг Управляющей компанией, клиенту следует по возможности оценить ситуацию и уточнить полномочия отправителя запроса и процедуру предоставления информации непосредственно у Управляющей компании.

2.1.3. Проявление осторожности и предусмотрительности:

– клиенту Управляющей 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 Управляющую компанию или иных доверенных лиц;

– клиентам Управляющей компании не рекомендуется заходить на сайты, в системы удаленного доступа с непроверенных устройств, которые клиент не имеет возможности контролировать.;

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

– при обращении в Управляющую компанию клиенту рекомендуется осуществлять звонок только по номеру телефона, указанному на сайте Управляющей компаниив сети Интернет;

– при предоставлении клиентом доступа к устройству третьим лицам клиент несет риск загрузки такими лицами на устройство вредоносного кода. В случае утраты устройства злоумышленники могут воспользоваться им для доступа к системам Общества от лица клиента;

– клиенту рекомендуется использовать для связи с Управляющей компанией отдельное, максимально защищенное устройство, доступ к которому есть только у клиента;

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

2.1.4. В случае использования клиентом при взаимодействии с Управляющей компанией электронной подписи, клиенту рекомендуется:

– использовать для хранения ключей электронной подписи внешние носители;

– 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 рекомендуется:

– 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 и средства защиты от несанкционированного доступа;

– 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 официальных магазинов приложений;

– не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в смс-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Общества;

– установить на устройстве пароль для доступа к устройству.

2.1.7. При обмене информацией через сеть Интернет рекомендуется:

– 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 не вызывающих доверие 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;

– не нажимать на баннеры и всплывающие окна, возникающие во время работы в сети Интернет;

– открывать файлы только известных клиенту расширений.

2.2. При подозрении в компрометации электронной подписи или несанкционированном движении активов клиенту следует незамедлительно обращаться в Управляющую компанию по телефону и/или адресу электронной почты, указанным на официальном сайте Управляющей компании в сети Интернет.