Информация о программном обеспечении, используемом профессиональным участником для взаимодействия с клиентом

При взаимодействии с клиентами ТКБ Инвестмент Партнерс (АО), далее – Общество, использует следующее программное обеспечение:

1. Личный кабинет клиента (https://online.tkbip.ru)
2. Система ТКБ-Агент
3. Программное обеспечение для обмена электронными документами с клиентами - участниками электронного взаимодействия в рамках выставления и получения счетов-фактур в электронной форме по телекоммуникационным каналам связи с применением усиленной квалифицированной электронной подписи в соответствии со статьей 169 НК РФ
4. Система электронного документооборота ООО «Технический центр ИНФИНИТУМ»
5. Система электронного документооборота НКО АО НРД
6. Мобильное приложение «TKBIP – Портфель инвестиций»
7. Сервисы электронной почты.

Использование указанного выше программного обеспечения, далее – ПО, клиентом связано с несением следующих основных рисков, характерных для электронного обмена информацией:

1. Риски, связанные с нарушением непрерывности функционирования ПО, в частности они включают в себя:

- риск прекращения использования Обществом ПО во время действия заключенного с пользователем договора;

- риск сбоя в ПО, который может привести к нарушениям или временной приостановке работы ПО, к потере информации, к задержкам при информационном обмене, а также к задержкам при обработке информации клиента;

- риск перебоев в работе каналов связи, в том числе риск перебоев в работе сети Интернет, что может привести к задержкам передачи информации;

- риск перебоев в энергоснабжении и иные причины технического характера, которые могут привести к перерывам в работе ПО.

2. Риски информационной безопасности, связанные с несанкционированным доступом к информации неуполномоченными лицами и воздействием вредоносных программ. Указанные риски могут быть обусловлены, в частности: (1) кражей идентификатора и пароля доступа (в т.ч. SMS-кодов) или иных конфиденциальных данных посредством технических средств и/или вредоносного кода и использование

злоумышленниками указанных данных с других устройств для несанкционированного доступа; (2) установкой на устройство клиента вредоносной программы, которая позволит злоумышленникам осуществить операции в ПО от имени клиента; (3) кражей или несанкционированным доступом к устройству, с которого клиент пользуется ПО для получения данных и/иди несанкционированного доступа к сервисам с этого устройства; (4) получением идентификатора доступа, пароля, SMS-кодов и прочих конфиденциальных данных путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником Общества или агента Общества, техническим специалистом и т.п. и просит клиента сообщить ему эти конфиденциальные данные; (5) перехватом сообщений электронной почты и получения несанкционированного доступа к отчетам и прочей финансовой информации, если электронная почта используется для информационного обмена такой информацией. (6) получением доступа к электронной почте клиента, в результате чего могут быть отправлены сообщения от имени клиента в Общество.

Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) и клиентских устройств, используемых для доступа к ПО, а также с передачей SMS-кодов в нарушение порядка их использования несет Клиент. Общество не несет ответственность в случаях финансовых потерь, понесенных Клиентами в связи с пренебрежением правилами информационной безопасности.

3. Риски, связанные с ошибками, совершаемыми клиентом при использовании ПО для взаимодействия с Обществом, в результате чего возможна некорректная работа ПО.