ПАМЯТКА
по снижению рисков при работе с ЭДО

Ключевые риски использования программного обеспечения для взаимодействия с клиентом/контрагентом связаны с:

- потенциальными техническими сбоями в программно-технических комплексах (ПТК), используемых при осуществлении электронного документооборота как на стороне клиента, так и на стороне ООО «ДКТ»;
- доступностью телекоммуникационных каналов, используемых при осуществлении такого взаимодействия;
- недостатками в организации изготовления/хранения/использования средств криптографической защиты и электронной подписи.

Риски, связанные с техническими сбоями используемых ПТК, нивелируются за счет использования надежных программных технических средств (ПТС), их своевременного обновления, а также применения современных средств защиты (в частности – антивирусной, резервирования, резервного копирования данных и т.п.).

Риски, связанные с доступностью телекоммуникационных каналов, нивелируются за счет использования надежных каналов и протоколов связи, а также применения современных средств защиты телекоммуникационных сетей (своевременного обновления оборудования и сигнатурных баз средств защиты телекоммуникационного оборудования, резервирования и дублирования оборудования и каналов связи и т.п.).

Уменьшение перечисленных рисков в рамках соответствующих систем ЭДО являются одной из главных задач владельцев соответствующих систем.

Тем не менее, часть ответственности за их поддержание на низком уровне ложится и на Участников ЭДО – в части касающейся.

Особый случай представляют риски, связанные с недостатками в организации изготовления/хранения/использования средств криптографической защиты (СКЗИ) и электронной подписи, ответственность за которые полностью возлагаются на Участников ЭДО.

Наибольшие риски в этом случае связаны с организацией хранения и использования средств электронной подписи.

В качестве рекомендаций по снижению данных рисков можно назвать следующие:

- использование (по возможности[1]) при осуществлении ЭДО квалифицированных электронных подписей (КЭП);
- использование при осуществлении ЭДО сертифицированные в РФ СКЗИ[2], поддерживающие выполнение требований соответствующих ГОСТ;
- обеспечить правильный учет, хранение и эксплуатацию ключей шифрования и КЭП в рамках вашей организации, а также контроль за реализацией этих мер;
- обеспечить подготовку и обучение правилам эксплуатации ПО, СКЗИ и средств электронной подписи, используемых при осуществлении ЭДО работников Общества – владельцев электронных подписей.

Как показывает практика, наименьший уровень риска возможно обеспечить при использовании электронной подписи самим её владельцем, размещением ключей шифрования и сертификатов электронных подписей на надежных носителях (например – USB-токенах), защищенных соответствующими PIN-кодами и хранимых вне моментов использования в закрываемых сейфах/металлических шкафах, доступ к которым имеет только сам владелец электронной подписи.

---

[1] Вид используемого при осуществлении ЭДО сертификата, как правило, определяет владелец соответствующей СЭД

[2] Вид СКЗИ также определяется владельцем ЭДО.