Источник: https://belforma.net/бланки/Банк/Соглашение_по_обеспечению_информационной_безопасностис возможностью скачать типовой бланк в формате PDF (Adobe Reader).

Соглашение по обеспечению информационной безопасности

Утверждено письмом Нацбанка от 09.12.1997 N 26026/621

Приложение 3
к Договору N _____

г._____

"___" _____ 20__ г.

Государственное предприятие "Белорусский межбанковский расчетный центр", именуемое в дальнейшем "БМРЦ", в лице директора Своятыцкого Д.А., действующего на основании Устава, с одной стороны, и _____, именуемый в дальнейшем "Участник", в лице _____, действующего на основании _____, с другой стороны, именуемые вместе "Стороны", в дополнение к основному Договору N _____ от "___" _____ 200_ г., заключили между собой настоящее Соглашение о нижеследующем:

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Осуществление межбанковских расчетов по крупным и срочным платежам в АС МБР осуществляется только на основе электронного платежного сообщения.

1.2. Электронные платежные сообщения передаются в АС МБР в виде файлов электронных платежных сообщений.

1.3. Неотъемлемой частью каждого электронного платежного сообщения и файла электронных платежных сообщений является электронная цифровая подпись (далее - "ЭЦП").

1.4. Наличие корректной ЭЦП файла электронных платежных сообщений является необходимым условием допуска такого файла в АС МБР.

1.5. Упомянутые в настоящем Соглашении документы представляются БМРЦ Участнику в прошитом и заверенном печатями и подписями обеих Сторон виде.

2. ОБЯЗАТЕЛЬСТВА СТОРОН

2.1. Обе Стороны обязуются использовать в расчетах через АС МБР средства криптографической защиты электронных платежных сообщений, поставляемые БМРЦ, строго в соответствии с требованиями документации, поставляемой в составе этих средств.

2.2. Участник обязуется:

2.2.1. Соблюдать правила обеспечения безопасности АС МБР и защиты информационного обмена, изложенные в документации, поставляемой БМРЦ по отдельному с ним договору поставки в составе абонентского комплекта подсистемы криптографической защиты информации.

2.2.2. Самостоятельно обеспечить непрерывную и устойчивую работу программно-технического комплекса, на котором установлено программное обеспечение (далее - "ПО") абонентского комплекта подсистемы криптографической защиты информации, и защиту его ресурсов от несанкционированного доступа, в том числе защиту от воздействия деструктивных программ (вирусов) т.е.:

2.2.2.1. Оснастить источником бесперебойного электропитания необходимой мощности;

2.2.2.2. Включить и настроить имеющиеся в стандартном системном и сетевом ПО средства ограничения доступа к ресурсам и протоколирования событий;

2.2.2.3. Обеспечить защиту от деструктивных программ (вирусов);

2.2.2.4. Обеспечить объектовые меры защиты;

2.2.2.5. Соблюдать порядок использования и хранения КЛЮЧЕЙ в соответствии с действующими инструкциями, а именно:

- использовать КЛЮЧ только по назначению;

- в случае смены ключевой информации на носителе, использовать КЛЮЧ только после разрешения, полученного от администратора безопасности БМРЦ;

- хранить КЛЮЧ в месте не доступном другим лицам;

- не передавать носитель ключа лицам не являющимся их владельцами (в случае изменений функциональных обязанностей, увольнения и т.п. соответствующий ключ подлежит ликвидации, об этом необходимо незамедлительно сообщить администратору безопасности БМРЦ);

- в случае утраты носителя срочно сообщить об этом администратору безопасности БМРЦ;

- в случае подозрения на компрометацию КЛЮЧА (носитель временно находился без контроля владельца) незамедлительно сообщить администратору безопасности БМРЦ;

- если носитель оказался сбойным (программа шифрования выдает сообщение о сбое при работе с носителей ключа), сообщить об этом администратору безопасности БМРЦ.

2.3. БМРЦ обязуется:

2.3.1. Предоставить программно-технический комплект подсистемы криптографической защиты информации по заявке Участника в составе, определенном документом "Система BIS. Пусковой комплекс. Система информационной безопасности. Подсистема криптографической защиты информации. Абонентский комплект. Спецификация. БМРЦ.5110.01".

2.3.2. Осуществлять управление ключами в подсистеме криптографической защиты информации в АС МБР.

2.3.3. Обеспечивать проверку подлинности и целостности файлов электронных платежных сообщений, при этом:

2.3.3.1. В случае корректности ЭЦП файла обработать электронные платежные сообщения, содержащиеся в файле, в соответствии с п. 2.1 основного Договора;

2.3.3.2. В случае некорректности ЭЦП файла не допустить его обработки.

2.3.4. Обеспечивать конфиденциальность информации, связанной с проведением расчетов в АС МБР.

3. ОТВЕТСТВЕННОСТЬ СТОРОН

3.1. В случаях ошибок программного обеспечения, сбоев и отказов технических средств ответственность несет Сторона, не принявшая достаточных мер по обеспечению их надлежащей надежности.

4. РАЗРЕШЕНИЕ КОНФЛИКТОВ

4.1. Разрешение конфликтов между участниками АС МБР осуществляется на претензионной основе.

4.2. Все споры, возникающие в процессе работы в АС МБР, Участники стремятся разрешать путем двухсторонних договоренностей на основе компромиссов, а в случае возникновения разногласий при исполнении данного Соглашения Стороны договариваются о его обязательном досудебном рассмотрении Согласительной Комиссией в соответствии с разделом 6 основного Договора.

5. ПОРЯДОК И СРОКИ ВЫСТАВЛЕНИЯ ПРЕТЕНЗИЙ

5.1. Факт наличия спорного вопроса регистрируется с момента получения обвиняемой Стороной (БМРЦ) документированной претензии обвиняющей стороны (Участник).

5.2. Претензия оформляется в виде свободного изложения существа обвинения в письменном виде на бланке организации за подписью первого руководителя и направляется обвиняемой стороне (в адрес первого руководителя) с уведомлением о вручении.

5.3. Претензия выставляется (доставляется) обвиняемой стороне не позднее двух рабочих дней с момента обнаружения факта невыполнения обязательств.

6. ПОРЯДОК И СРОКИ РАЗРЕШЕНИЯ СПОРОВ

6.1. Обе Стороны, по инициативе обвиняемой стороны, уточняют наличие предмета спора, выясняют причины его возникновения и последствия и договариваются о мерах по его урегулированию.

6.2. В случае обвинений Участника в невыполнении БМРЦ обязательств по п. 2.3.3 настоящего Соглашения (при невыполнении п. 2.2 обвинения считаются несостоятельными), руководитель обвиняемой Стороны организует служебное расследование по существу претензии. Расследование производится с использованием процедур, изложенных в Приложении к настоящему Соглашению "Процедуры определения подлинности ЭЦП". Все полученные при этом обвиняемой Стороной данные оформляются актом, утверждаемым руководителем. Акт направляется обвиняющей Стороне с уведомлением о вручении.

6.3. Если Стороны пришли к взаимоприемлемому решению спорного опроса, то это означает, что договоренность между Сторонами достигнута, и это решение является обязательным для обеих Сторон.

6.4. Если Стороны не пришли к взаимоприемлемому решению спорного вопроса, то в этом случае Стороны составляют и подписывают протокол разногласий, который включается в комплект документов для последующего его досудебного рассмотрения Согласительной Комиссией Сторон в соответствии с разделом 6 основного Договора.