ПРИЛОЖЕНИЕ 1

Приложение 2 к Договору

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ КЛЮЧЕЙ АСП СИСТЕМЫ

1. Настоящие рекомендации действуют по отношению к Клиентам Банка, осуществляющим эксплуатацию ключей АСП на основании договора с Банком.

1.1. Рекомендации по организационному обеспечению безопасности ключей АСП:

- в организации Клиента назначаются лица, ответственные за эксплуатацию и хранение ключей АСП;
- в организации Клиента разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации ключей АСП;
- к работе с ключами АСП допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации ключей АСП.

1.2. Рекомендации по аппаратно-программному обеспечению рабочего места:

- на автоматизированных рабочих местах Клиента использовать только лицензионное программное обеспечение;
- на системное программное обеспечение и Интернет-браузер должны быть установлены все обновления;
- необходимо использовать антивирусное программное обеспечение, с обновлением вирусных баз не реже раза в сутки и проведением периодических антивирусных проверок компьютеров;
- необходимо осуществлять вход в «Интернет-Банк» путем ввода его цифрового адреса через адресную строку браузера и\или контролировать данный адрес;
- необходимо отключить на автоматизированных рабочих местах Клиента автозагрузку со сменных носителей (дискет, флэш-накопителей, оптических дисков) как потенциальный источник угроз;
- необходимо отключить на автоматизированных рабочих местах Клиента у пользователей права администрирования персонального компьютера и сетевой удалённый доступ.

1.3. Рекомендации по работе с системой:

- необходимо регулярно, не реже одного раза в день проверять состояние счета;
- необходимо подключиться к оповещению о проведении платежа с помощью SMS;
- на телефоне, использующемся для SMS-авторизации, необходимо отсутствие подключения к сети Интернет.
- необходимо использовать для набора пароля виртуальную клавиатуру;
- необходимо использовать персональное изображение (картинку) в своей системе Интернет-Банк;

- пользуясь пунктом Безопасность, необходимо установить ограничение IP-адресов, с которых можно осуществлять доступ в систему.
- при обнаружении любых признаков несанкционированного доступа к автоматизированному рабочему месту Клиента или к ключам АСП необходимо незамедлительно заявить в Банк о необходимости заблокировать доступ к системе, заменить ключи АСП и провести расследование причин случившегося.

1.4. Рекомендации по размещению автоматизированные рабочих мест Клиента:

- помещения, в которых размещаются автоматизированные рабочие места Клиента и/или сервера, взаимодействующие с Банком, должны обеспечивать конфиденциальность проводимых работ;
- размещение помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств;
- размещение автоматизированные рабочих мест Клиента и/или серверов, взаимодействующих с Банком и предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности;
- входные двери помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время;
- системные блоки компьютеров автоматизированных рабочих мест Клиента оборудуются средствами контроля вскрытия.

1.5. Рекомендации по подключению автоматизированных рабочих мест Клиента и/или серверов, взаимодействующих с Банком, к локальным сетям и сетям общего пользования (Internet):

- необходимо исключить прямое подключение автоматизированных рабочих мест Клиента и/или серверов, взаимодействующих с Банком, к сетям общего пользования (Internet);
- автоматизированные рабочие места Клиента и/или сервера, взаимодействующие с Банком, должны располагаться за средствами межсетевого экранирования (фаервола) во внутренней сети Клиента или в демилитаризованной зоне;
- входящий и исходящий сетевой трафик должен фильтроваться средствами межсетевого экранирования (фаервола);
- должны быть настроены механизмы оповещения о попытках несанкционированного доступа;
- не реже одного раза в неделю должны проводиться мероприятия по аудиту информационной безопасности автоматизированных рабочих мест Клиента и/или серверов, взаимодействующих с Банком, согласно методикам аудита информационной безопасности принятым у Клиента.

1.6. Рекомендации по обеспечению безопасности ключевой информации:

- ключевые носители АСП и автоматизированные рабочие места Клиента и/или сервера, взаимодействующие с Банком и содержащие ключи АСП, в организации Клиента берутся на поэкземплярный учет в выделенных для этих целей журналах;

- доступ к ключам АСП должен быть ограничен на уровне операционной системы и прикладной программы только учетными записями пользователей, имеющих прямое отношение к обработке ключевой информации, и запрещен по сети;
- должны быть настроены механизмы аудита доступа и оповещения о попытках несанкционированного доступа к ключам АСП, хранящимся на автоматизированных рабочих местах Клиента и/или серверах, взаимодействующих с Банком;
- подключение ключевых носителей к автоматизированным рабочим местам Клиента и/или серверам, взаимодействующим с Банком, допускается только на время работы с системой Интернет-банк.
- для хранения ключевых носителей с ключами АСП выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации;
- хранение ключевых носителей допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования, применение;
- при транспортировке ключевых носителей АСП, автоматизированных рабочих мест Клиента и/или серверов, взаимодействующих с Банком, с ключевой информацией создаются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию;
- уничтожение ключей АСП осуществляется в соответствие с процедурами принятыми у Клиента для уничтожения конфиденциальной информации.