Рекомендации по обеспечению безопасности при работе с Системой ДБО «iBank» и мобильным приложением «Банк Ермак – для бизнеса»

Применяемые термины:

АРМ – Автоматизированное рабочее место на стороне Клиента обеспечивающее доступ к системе ДБО «iBank»;
Ключ ЭП – уникальная последовательность символов (байт), самостоятельно генерируемая Клиентом с использованием средств системы ДБО «iBank», и предназначенная для формирования Клиентом электронной подписи электронных документов;
Электронный идентификатор (далее ЭИ) – специализированное устройство предназначен для безопасной двухфакторной аутентификации пользователей, генерации и защищенного хранения ключей шифрования и ключей электронной подписи, выполнения шифрования и самой электронной подписи «на борту». Может быть реализовано в виде USB-токена (Рутокен ЭЦП 2.0);
ПЭВМ – персональная электронно-вычислительная машина (Персональный компьютер);
Системе ДБО – Система дистанционное банковское обслуживание.

Требования информационной безопасности обязательные для выполнения Клиентом:

- назначить Администратора информационной безопасности Клиента – работника, ответственного за настройку и эксплуатацию средств защиты информации, установленных на АРМ;
- Клиент обеспечивает хранение Ключей ЭП, только на специализированных устройствах - ЭИ;
- ЭИ должен быть подключен к АРМ только на время работы в системе ДБО;
- на АРМ Клиента должно быть установлено лицензионное антивирусное программное обеспечение и выполнена настройка автоматического обновления антивирусных баз с официального web-сайта разработчика антивирусного ПО. На АРМ Клиента, при наличии, должен быть настроен персональный межсетевой экран (Firewall) имеющийся в составе операционной системы;
- на АРМ Клиента должны быть отключены сервисы, позволяющие удаленно управлять компьютером;
- на АРМ Клиента должно использоваться лицензионное программное обеспечение (операционные системы, офисные пакеты, прикладные программы) и обеспечено автоматическое обновление системного и прикладного ПО;
- Клиент обеспечивает хранение и использование ЭИ таким образом, чтобы исключить доступ к нему неуполномоченных лиц;
- по окончании работы с Системой ДБО ЭИ должен быть извлечен и хранится в месте, обеспечивающем его защиту от доступа посторонних лиц, неуполномоченных для работы в Системе ДБО. Запрещается оставлять ЭИ подключенным в USB-порт или вставленным в картридер при отсутствии лица, уполномоченного на работу в Системе ДБО;

В целях повышения безопасности информации, обрабатываемой в системе ДБО, помимо обязательных мер, Банк рекомендует:

- выделить отдельную ПЭВМ, предназначенную только для работы в системе ДБО. При отсутствии возможности использования отдельной ПЭВМ, выполнить настройку множественной загрузки ПЭВМ с созданием отдельного профиля для работы только с Системой ДБО;
- установить на АРМ лицензионное специализированное программное обеспечение, повышающее уровень защищенности: межсетевой экран (Firewall), антишпионское ПО (antispyware). В настройках межсетевого экрана запретить любые соединения, кроме IP-адреса Банка;
- отключить неиспользуемые на АРМ сетевые протоколы и службы;
- отключить все общие ресурсы операционной системы, в том числе и создаваемые по умолчанию при ее установке;
- установить для учетной записи оператора АРМ минимальный уровень прав доступа, необходимого для нормальной работы в системе ДБО. Работу оператора АРМ под учетной записью с правами «Администратор» исключить.
- ограничить доступ работников и посторонних лиц к АРМ, используемому для работы с Системой ДБО. Доступ к АРМ предоставить только лицам, непосредственно работающим с системой ДБО;
- при использовании услуг сторонней организации или частных лиц по настройке и обслуживанию ПЭВМ, обеспечить контроль действий лица, осуществляющего непосредственную настройку и не допускать его к

Системе ДБО и Ключам ЭП. При необходимости проверки работоспособности Системы ДБО она должна выполняться исключительно лицами, уполномоченными для работы с Системой;

- по возможности, использовать одновременно два средства технической защиты;
- не отключать услугу фильтрации IP-адресов;
- использовать услугу дополнительного подтверждения платежных поручений;
- организовать хранение ЭИ в персональных надежных опечатываемых хранилищах (сейфах);
- обеспечить использование паролей ключей ЭП, удовлетворяющих следующим минимальным требованиям - пароль:
  - не должен состоять из одних цифр;
  - должен быть длиннее 6 знаков;
  - должен содержать в себе строчные и прописные буквы, цифры и знаки препинания;
  - не должен состоять из символов, находящихся на одной линии на клавиатуре;
  - не должен быть значимым словом (имя, фамилия, дата рождения, девичья фамилия супруги, кличка собаки, кошки и т.д.).

Правила эксплуатации и хранения ЭИ:

- необходимо оберегать ЭИ от воздействия влаги и агрессивных сред сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т. п.), воздействия высоких и низких температур. При резкой смене температур (вносе охлажденного ЭИ с мороза в теплое помещение) не рекомендуется использовать ЭИ в течение 3 (Трёх) часов во избежание повреждения ЭИ из-за сконденсированной на его электронной схеме влаги. Необходимо оберегать ЭИ от попадания на него прямых солнечных лучей;
- недопустимо воздействие на ЭИ сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества;
- при подключении ЭИ к компьютеру недопустимо прилагать излишние усилия;
- ЭИ в нерабочее время необходимо всегда держать закрытым во избежание попадания на разъем ЭИ пыли, грязи, влаги и т. п. При засорении разъема токена нужно принять меры для его очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо. Не следует разбирать ЭИ, это ведет к потере гарантии. В случае неисправности или неправильного функционирования ЭИ необходимо обратиться в Банк.

При работе с мобильным приложением «Банк «Ермак» - для бизнеса» Клиент обязан соблюдать следующие требования безопасности:

- Хранить в секрете и не передавать третьим лицам пароли доступа к мобильному устройству, мобильному приложению **«Банк «Ермак» - для бизнеса»** и ключам ЭП.
- Не оставлять мобильное устройство (SIM-карту), с установленным мобильным приложением **«Банк «Ермак» - для бизнеса»** или используемое для получения SMS-кода, без присмотра в местах, доступных для третьих лиц, и никому их не передавать.
- Устанавливать мобильное приложение **«Банк «Ермак» - для бизнеса»** АО Банк «Ермак» только из авторизованных магазинов App Store и Google Play и только на принадлежащие Клиенту мобильные устройства. Перед установкой приложения убедитесь, что его разработчиком является компания БИФИТ.
- Использовать антивирусное программное обеспечение, в случае, если оно доступно для используемого Клиентом мобильного устройства.
- Не использовать мобильное приложение **«Банк «Ермак» - для бизнеса»** на устройствах, на которых повышены привилегии пользователя до административных (получены root-права на Android устройствах и проведен jailbreak на iPhone).
- В случае утраты мобильного устройства (SIM-карты), с установленным мобильным приложением «Банк «Ермак» - для бизнеса» или используемого для получения SMS-кода и (или) их использование без согласия Клиента, сообщить об этом в Банк незамедлительно после обнаружения факта утраты и (или) использования без согласия Клиента, но не позднее дня, следующего за днем обнаружения факта утраты и (или) получения от Банка уведомления о совершенной операции с использованием Системы ДБО.