Приложение №3
к Приказу ООО «Экспобанк»
от 07.12.2018г. № Пр-01/18-420
Введено в действие с 12.12.2018 г.

Рекомендации по обеспечению информационной безопасности при работе в Системе «Банк-Клиент»*

Внимание! Ответственность за безопасное хранение и использование ключа электронной подписи (далее - ЭП), а также мобильных устройств при использовании мобильной версии системы «Банк-Клиент»/ мобильного приложения, лежит на Клиенте. Выполнение указанных ниже рекомендаций поможет обеспечить сохранность ваших финансовых средств.

В целях минимизации рисков мошенничества и предотвращения атак вредоносного кода[1] при работе с системой «Банк-Клиент», в том числе при работе в мобильной версии системы «Банк-Клиент» / мобильном приложении, ООО «Экспобанк» рекомендует Вам выполнять следующие действия и правила:

Для обеспечения информационной безопасности ключа ЭП Вы должны:

- по завершении работы с Системой «Банк-Клиент» не оставлять ключевой носитель, подключенным к компьютеру;
- обеспечить хранение ключевого носителя в месте, исключающем доступ к носителю третьих лиц (в сейфе, личной запираемой ячейке и т. п.), не оставлять без присмотра и в легкодоступных местах;
- исключить передачу ключа ЭП или его копий третьим лицам, а также передачу по публичным сетям (например, Интернет).
- исключить хранение ключа ЭП на жестком диске, в сетевых каталогах и прочих общедоступных ресурсах;
- при смене сотрудника организации, отвечающего за формирование и проведение платежей с помощью Системы «Банк-Клиент», сменить логины, пароли доступа и криптографические ключи;
- для доступа к мобильной версии / мобильному приложению требуется только логин и пароль. В случае, если от Вас требуется ввод иной дополнительной информации (номеров банковских карт, мобильного телефона, и других данных, в т.ч. персональных), следует прекратить пользование услугой и незамедлительно связаться с Банком;
- ни при каких обстоятельствах не сообщать иным лицам свой логин и пароль, включая сотрудников Банка, родственников;
- при утрате мобильного устройства, на который Банк отправляет SMS-уведомления, незамедлительно обратиться к оператору сотовой связи для блокировки SIM-карты и в Банк для блокировки доступа;
- при смене номера телефона, на который подключены SMS-уведомления, незамедлительно обратиться в Банк и отключить услугу от ранее использовавшегося номера телефона и подключить услугу на новый номер.

Для обеспечения безопасности устройства, с которого осуществляется работа с Системой «Банк-Клиент», рекомендуем:

- использовать только лицензионные общее и прикладное программное обеспечение и средства антивирусной защиты;
- на мобильные устройства устанавливать приложения только из известных источников;
-

[1] Атака вредоносного кода – воздействие вредоносного кода на автоматизированные системы программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование кредитной организации и её клиентов – пользователей ДБО, осуществляемое локально или через информационно-телекоммуникационные сети, в т.ч. через информационно-телекоммуникационную сеть «Интернет».

- обеспечить на устройстве непрерывное функционирование средств антивирусной защиты и межсетевого экранирования (брандмауэр, firewall);
- ограничить права пользователя на внесение изменений в настройку операционной системы и установку каких-либо программ на устройство. При использовании для работы в Системе «Банк-Клиент» нескольких компьютеров, желательно поместить их в отдельный сегмент сети;
- обеспечить своевременное обновление операционной системы, антивирусного программного обеспечения, а также антивирусных баз данных;
- осуществлять автоматическую периодическую (не реже одного раза в неделю) проверку устройства на наличие вирусов, при обнаружении вирусов, шпионских программ и т. п. немедленно их удалять;
- установить пароль доступа к ключу ЭП, а также пароль на компьютер таким образом, чтобы они соответствовали требованиям сложности (пароль должен быть не менее 8 символов, состоять из комбинации прописных и строчных букв с цифрами и символами);
- соблюдать правила информационной безопасности при работе в Интернете (не посещать подозрительные сайты, не устанавливать программы из «недоверенных» источников, не открывать письма и вложения от неизвестных отправителей и пр).

Для обеспечения информационной безопасности при работе в Системе «Банк-Клиент» рекомендуем:

- использовать вход в систему только с сайтов **www.expobank.ru** или www.faktura.ru и ни при каких обстоятельствах не вводить логин и пароль доступа Системы «Банк-Клиент» на других сайтах. Обращайте внимание на правильность адреса (ссылки) сайта Банка. При выявленном несоответствии – немедленно прекратите проведение операций и проинформируйте Банк;
- подключить сервис «Дополнительный пароль на вход в систему»;
- обратиться в Банк для подключения сервисов SMS- и/или Email-уведомлений об исполнении платежей, об отправке платежных документов в банк, либо сервис SMS-уведомлений обо всех ваших входах в Систему «Банк-Клиент».
  При получении SMS-, Email-уведомлений о действиях, которых Вы не совершали, незамедлительно сообщить в Банк для их отмены и объявления ключей ЭП /паролей скомпрометированными.
- ежедневно контролировать состояние счета (путем просмотра выписки). При выявлении расхождений – немедленно прекратите проведение операций и проинформируйте Банк;
- обращать внимание на дату и время последних входов в систему (данные фиксируются на первой странице после входа в систему, а также в специальном разделе «Безопасность» - «Журнал сеансов работы»);
- для корректного закрытия сессии совершать выход из системы «Банк-Клиент», в том числе при работе в мобильной версии системы «Банк-Клиент» / мобильном приложении, с помощью кнопки «Выход».

Некоторые признаки нарушений режима безопасности:

- хищение, утеря (безвозвратная или с последующим обнаружением), повреждение ключевого носителя;
- увольнение сотрудников, имевших доступ к ключам ЭП, изменения функциональных обязанностей сотрудника клиента, имевшего доступ к распоряжению счетом;
- возникновение подозрений на утечку информации или ее несанкционированное изменение в системе «Банк-Клиент»;
- подозрение на несанкционированный доступ третьих лиц к счетам, программно-аппаратным средствам клиента, ключу ЭП;
- несанкционированные операции по банковскому счету Клиента с использованием системы «Банк-Клиент»;
- вирусное заражение устройства;
- нарушение печати на сейфе с ключевым носителем в момент нахождения в нем ключевых носителей.

Обязательная замена ключа ЭП проводится в следующих случаях:

- истек срок действия ключа ЭП;

- произошла компрометация ключа ЭП.

Внимание! До момента блокировки ключа ЭП ООО «Экспобанк» не несет ответственности за платежи, совершенные с использованием этого ключа, даже в случае его компрометации, в т.ч. при воздействии на клиентское АРМ вредоносных кодов.

В случае возникновения подозрения о компрометации ключа ЭП, а также паролей при их наличии, вам необходимо незамедлительно обратиться к менеджеру, обслуживающему ваш счет, или к специалисту службы поддержки Системы «Банк-Клиент» по телефону 8-800-500-07-70 и инициировать процедуру смены всех потенциально скомпрометированных ключей ЭП, а также логинов при их наличии, или блокировку Системы «Банк-Клиент».

**(Следующий абзац применяется для случаев, когда Рекомендации составлены на русском и английском языках*)
Рекомендации составлены на русском и английском языках. В случае расхождений между текстами на русском и английском языках, текст на русском языке имеет преимущественную силу.