Банк РостФинанс

Рекомендации по обеспечению информационной безопасности при работе в Системе ДБО

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

Сеть Интернет не всегда является безопасным каналом связи для передачи информации, и существуют риски, связанные с возможным нарушением конфиденциальности возникающие вследствие использования такого канала доступа.

Существует повышенный риск несанкционированного использования Системы ДБО, включая компрометацию ключей ЭП и несанкционированное удаленное управление Системой ДБО, при ненадлежащем соблюдении настоящих рекомендаций.

К случаям повышенного риска, связанным с использованием Системы ДБО, относится:

- использование Системы ДБО с помощью устройства доступа, размещенного в общественном месте;
- кража (утеря) мобильного устройства Уполномоченного лица Клиента, используемого для доступа в Систему ДБО;
- кража (утеря) устройства мобильной связи, на номер которого приходят SMS/PUSH-сообщения с разовыми паролями для подтверждения операций по счету посредством сервиса информирования Системы ДБО, либо SMS/PUSH-сообщения о проведенных платежах;
- невыполнение условий настоящих Рекомендаций;
- использование пароля на вход в устройство доступа и пароля доступа к ключам ЭП, не соответствующего минимальным требованиям к его безопасности указанным в настоящих Рекомендаций;
- получение доступа к Системе ДБО посредством браузера с устройства доступа, содержащего вредоносный или модифицированный код, а также на котором произведена модификация системы с целью получения доступа к файловой системе или иных прав, не предусмотренных разработчиками операционной системы.

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

Для обеспечения информационной безопасности ключа ЭП/ Пароля Вы должны:

- по завершении работы с Системой ДБО 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 ДБО, сменить Логины, Пароли доступа и криптографические ключи;

[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».

- 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. Обеспечить смену первичного пароля в соответствии с рекомендациями, указанными в договоре;
- при утрате мобильного устройства, на который Банк отправляет SMS-уведомления, разовые пароли, 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;
- не передавать мобильное устройство с зарегистрированным номером телефона третьим лицам.

Для обеспечения безопасности устройства, с которого осуществляется работа с Системой ДБО, рекомендуем:

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

- использовать вход в систему только с сайта **https://www.rostfinance.ru**/ и ни при каких обстоятельствах не вводить Логин и Пароль доступа Системы ДБО 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-уведомлений об исполнении платежей, об отправке платежных документов в банк, либо сервис SMS-уведомлений обо всех ваших входах в Систему ДБО.
- При получении SMS -уведомлений о действиях, которых Вы не совершали, незамедлительно сообщить в Банк для их отмены и объявления ключей ЭП /Логинов, 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 ДБО, в том числе при работе в мобильной версии системы ДБО / 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 ДБО;
- подозрение на несанкционированный доступ третьих лиц к счетам, программно-аппаратным средствам клиента, ключу ЭП/ Паролю;
- несанкционированные операции по банковскому счету Клиента с использованием системы ДБО;
- вирусное заражение устройства;
- нарушение печати на сейфе с ключевым носителем в момент нахождения в нем ключевых носителей.

Обязательная замена ключа ЭП/ Пароля проводится в следующих случаях:

- истек срок действия ключа ЭП;
- произошла компрометация ключа ЭП/ Пароля.

Внимание! До момента блокировки ключа ЭП/ Логина и Пароля ООО КБ «РостФинанс» 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/ Пароля, а также иных паролей при их наличии, вам необходимо незамедлительно обратиться к менеджеру, обслуживающему ваш счет, или к специалисту службы поддержки Системы ДБО по телефону 8-800-7777-001 и инициировать процедуру смены всех потенциально скомпрометированных ключей ЭП, а также Логинов и Паролей при их наличии, или блокировку Системы ДБО.