Приложение № 2
к Правилам дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в «ИНТЕРПРОГРЕССБАНК» (Акционерное общество) с использованием системы «Бизнес-Онлайн»

Правила безопасного использования Системы ДБО

Уважаемый Клиент,

Безопасность дистанционного банковского обслуживания, а значит, и сохранность Ваших денежных средств зависит от соблюдения Вами следующих мер и правил безопасности при работе в Системе ДБО:

1. После первого входа в Систему ДБО обязательно смените выданный Вам в Банке пароль для входа в систему. Длина пароля должная быть не менее 8 символов, в пароле должны быть использованы цифры, большие и маленькие буквы английского алфавита. Крайне НЕ рекомендуется использование в качестве пароля легко вычисляемых слов (например, имена, фамилии, номера телефонов, год рождения и т.д.).
2. Регулярно, не реже 1 (одного) раза в 30 (тридцать) календарных дней меняйте свой пароль, хотя никто не запрещает Вам его менять и чаще, на свое усмотрение.
3. Не разглашайте свой пароль от Системы ДБО и другие идентификационные данные никому, даже если к Вам с этой просьбой обратятся коллеги по работе и/или лица, представившиеся сотрудниками Банка. Помните, сотрудники банка не запрашивают данную информацию.
4. Если Вы предполагаете, что Ваш пароль от Системы ДБО был скомпрометирован, незамедлительно смените его на новый и немедленно проинформируйте об этом Банк любым доступным способом.
5. Не отвечайте на электронные письма, которые запрашивают Вашу конфиденциальную информацию, даже если они отправлены от имени Банка. Банк никогда не рассылает писем с подобными просьбами. Не пересылайте файлы с конфиденциальной информацией Системы ДБО по электронной почте, за исключением запросов на сертификат и открытых ключей.
6. Во избежание потерь Ваших денежных средств Банк предлагает своим Клиентам использовать для безопасного хранения ключей специализированные ключевые носители USB Рутокен. Ключевой носитель USB Рутокен (в виде USB-флешки) предназначен для безопасного, защищенного хранения ключей шифрования и ключей электронной подписи, позволяет выполнять криптографические операции таким образом, что закрытая ключевая информация никогда не покидает пределы устройства. Следовательно, исключается возможность копирования ключа и использования его злоумышленником для осуществления несанкционированного перевода денежных средств от имени клиента и увеличивается общая безопасность Системы ДБО.
7. Размещение и использование ключевой информации на сменном носителе (дискета, flash-накопитель) или на жестком диске компьютера, на котором установлена Система ДБО, существенно повышает риск несанкционированного доступа к ней третьими лицами.
8. Носитель с ключевой информацией должен использоваться только владельцем ключевой информации, либо лицом, уполномоченным на использование данного сменного носителя, и храниться в месте недоступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик).
9. Заменяйте ключи ЭП во всех случаях увольнения или смены руководителей, ответственных лиц, которые подписывали распоряжения (доверенность) о предоставлении полномочий для подписи электронных документов с применением ЭП, а также при любых подозрениях на компрометацию ключа ЭП.
10. Носитель с ключевой информацией должен быть установлен в считывающее устройство только на время проведения операций обмена с Банком. Постоянное нахождение ключевого носителя в считывателе существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.
11. После завершения сеанса работы с Банком необходимо выгрузить (отключить) Систему ДБО и извлечь ключевой носитель, а по окончании рабочего дня выключить компьютер.
12. На компьютере с установленной Системой ДБО:
    - должно быть установлено только лицензионное программное обеспечение (ПО);
    - должно быть настроено автоматическое обновление и регулярно устанавливаться обновления операционной системы;
    - должно быть установлено лицензионное антивирусное программное обеспечение с регулярно и автоматически обновляемыми антивирусными базами данных;
    - необходимо регулярно выполнять антивирусную проверку компьютера для своевременного обнаружения вредоносных программ;
    - на учетные записи пользователей операционной системы должны быть установлены пароли по требованиям пункта 1 настоящего Приложения и включена автоматическая блокировка экрана;
    - запрещается установка дополнительного ПО удаленного доступа, удаленного администрирования и управления;
    - запрещается посещение сайтов сомнительного содержания и любых других Интернет- ресурсов непроизводственного характера (социальные сети, конференции, чаты и т.п.), чтение почты из

публичных почтовых серверов (mail.ru, yandex.ru и т.п.), и открытие почтовых вложений от недоверенных источников.

13. Не используйте для доступа к Системе ДБО рабочие места, необеспечивающие должный уровень безопасности работы ("чужой" компьютер, интернет-кафе и т.д.).
14. Если Вы столкнулись с тем, что ранее действующий пароль не срабатывает и не позволяет Вам войти в Систему ДБО, или компьютер Системы ДБО внезапно перестал загружаться, немедленно проинформируйте об этом Банк любым доступным способом.

Помните!

Если Вы предоставляете кому-либо доступ к своим личным сведениям или средствам безопасности, Вы даете такому лицу возможность злоупотребления этими данным или передачи их третьему лицу.