Рекомендации по обеспечению безопасности при работе с системой интернет-банкинга iBank

Используемые определения:

iBank - система интернет-банкинга для юридических лиц
ЭП - электронная подпись сотрудника организации.

Система интернет-банкинга iBank обеспечивает вас надежной системой безопасности для управления своими счетами. Однако Вам так же необходимо побеспокоиться о конфиденциальности информации (паролей и ЭП).

Данные рекомендации помогут Вам повысить уровень безопасности при работе с системой iBank.

Обеспечение подлинности и достоверности передаваемой в Банк информации достигается использованием в системе средств электронной подписи.

Электронная подпись формируется при регистрации Клиента (или сотрудника Клиента) в системе iBank на каждого сотрудника организации, указанного в банковской карточке Клиента (или в соглашении о количестве собственноручных подписей). В целях обеспечения профилактики безопасности системы, ЭП выписываются сроком на 730 дней. ЭП для работы в системе допускается формировать только на защищенных носителях, полученных Клиентом в Банке. Действие ЭП не подлежит продлению, по истечению срока действия ЭП следует сформировать новую подпись.

Соединение и работа с системой iBank осуществляется через сеть Интернет в защищенном режиме с помощью протокола SSL (Secure Sockets Layer).

Для всех платежей обязательно использование второго фактора подтверждения в виде sms-кода (первый фактор подтверждения – ваша ЭП). Вы можете установить лимит суммы операции, до превышении которой платежи можно осуществлять без обязательного ввода кода из sms. Или оформить в системе iBank шаблон платежа, при использовании которого подтверждение так же не потребуется.

При работе с iBank, для повышения безопасности, необходимо следовать следующим рекомендациям:

- Ни при каких условиях не сообщайте информацию о вашем пароле/ЭП никому, включая сотрудников Банка.
- Проверяйте, что соединение действительно происходит в защищенном режиме SSL, в правом нижнем углу или адресной строке вашего вэб-браузера должен быть виден значок закрытого замка.
- При переходе на сайт Банка по ссылке из поисковой системы обращайте внимание на специальный знак, отображающий достоверность ссылки на основе официальных данных с сайта Центрального Банка.
- В систему iBank переходите с официального сайта Банка (мошенники могут имитировать интерфейс входа в систему в целях получения доступа к вашей ЭП).
- Ни в коем случае не сохраняйте информацию о вашем пароле на любых носителях, включая компьютер, не осуществляйте отправку паролей по электронной почте. Если у вас возникли подозрения, что кто-либо владеет информацией о вашей

ЭП, Вам необходимо с помощью обращения в Банк (по тел. (495) 662-45-45 /760) заблокировать ЭП.

- После окончания работы в iBank обязательно закройте окно системы с помощью кнопки Выход.
- Убедитесь, что ваш компьютер не поражен какими-либо вирусами. Установите и активизируйте антивирусные программы. Старайтесь их постоянно обновлять. Обращаем внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам информации о вашей ЭП.
- Установите и используйте персональный брандмауэр (firewall) на вашем компьютере для входа в сеть Интернет, это позволит предотвратить несанкционированный доступ к информации на вашем компьютере.
- Периодически проверяйте перечень установленного программного обеспечения на компьютере, с которого осуществляете взаимодействие с системой iBank на предмет наличия программного обеспечения, установку которого вы не производили. Появление подобного программного обеспечения на вашем компьютере может свидетельствовать о доступе к нему посторонних лиц.
- Используйте только програмное обеспечение (интернет-браузеры) и операционные системы, для которых производитель обеспечивает поддержку и предоставление обновлений по устранению известных ошибок и уязвимостей.
- Для подписи платежных документов, используются ключи ЭП, хранимые в защищенном носителе (Рутокен ЭЦП 2.0, MS_KEY K Ангара), необходимо обеспечить хранение этих носителей в месте не доступном посторонним лицам.
- Для обеспечения безопасного хранения ключей ЭП на защищенных носителях обязательна смена пин-кода по умолчанию. Для токенов "Рутокен ЭЦП 2.0" смена PIN-кода осуществляется в панели управления токеном, которая была установлена вместе с драйвером токена. Для токенов MS_KEY K Ангара необходимо на странице администрирования ключей ЭП выбрать ссылку «Сменить PIN».
- В случае порчи или утери носителей, содержащих ЭП, потребуется получение нового носителя в Банке. Обязательно уведомите об этом Банк для блокировки ЭП.
- В случае утери пароля к сформированной на защищенном носителе ЭП, потребуется формирование и регистрация новой ЭП. Утерянный пароль невозможно сменить или восстановить без знания действующего пароля.