ПАМЯТКА

Обеспечение информационной безопасности

при работе с системой «Клиент-Банк»

Для повышения уровня информационной безопасности при работе с системой «Клиент-банк» необходимо комплексное использование следующих по обеспечению информационной безопасности на стороне Клиента:

- Подключайте свои носители криптографических ключей (USB-токен) к компьютеру **только во время работы с Банком**. Во всех остальных случаях USB-токен должен быть отключен от компьютера и храниться в недоступном для третьих лиц месте.
- Для подписания электронного документа рекомендуется использовать 2 подписи (первая и вторая).
- Доступ в систему «Клиент-Банк» должен быть разделен между двумя разными компьютерами: на одном из них должен осуществляться ввод электронного документа в систему «Клиент-Банк», а на другом - подписание электронного документа и его отправка.
- Держите в тайне свои учетные данные (логин и пароль) для входа в систему ДБО.
- Используйте только лицензионное программное обеспечение – это защитит Вас от программных закладок оставленных злоумышленниками в нелицензионном или «взломанном» программном обеспечении.
- Не устанавливайте на компьютер, с которого осуществляется работа с Банком, средства удаленного администрирования такие как «TeamViewer», «rAdmin» и подобные. Наличие этих программ может позволить злоумышленникам провести платеж от Вашего имени удаленно.
- Использовать только лицензионное, рекомендованное антивирусное программное обеспечение (Symantec, Kaspersky, DrWeb, NOD32). Следите за постоянными обновлениями антивирусных баз.
- Установленное антивирусное программное обеспечение должно обеспечивать проверку всех загружаемых из Интернета файлов и программ на наличие вирусов.
- Даже если у вас установлено антивирусное программное обеспечение, все равно периодически (1 раз в месяц) проводите полное сканирование утилитами других производителей (Kaspersky, CureIT и д.р.).
- По возможности пользуйтесь сетевыми средствами защиты, например, межсетевыми экранами, системами обнаружение и предотвращения вторжений.
- Ограничьте доступ пользователей к портам ввода/вывода (USB, CD, Floppy, Card reader). Отключите не используемые порты.

- Регулярно устанавливайте обновления на Вашу операционную систему.
- Для работы системы «Клиент-Банк» должна быть предусмотрена отдельная учетная запись для каждого пользователя операционной системы компьютера с ограничением прав пользователя.
- Никогда не отвечайте на письма, телефонные звонки или личные вопросы, в которых Вас просят указать свои учетные данные, пароли, идентификаторы, даже если они пришли с электронной почты Банка. Помните, что сотрудники Банка никогда **не будут требовать от Вас сообщить или указать где-либо свои учетные данные.**
- Отключайте в браузере функции автозаполнения форм. Для этого, выберите в Internet Explorer пункт меню Сервис -> Свойства обозревателя, далее перейдите на закладку Содержимое, затем в разделе Автозаполнение нажмите кнопку Свойства и сбросьте все галочки в открывшемся меню, после чего закройте окна настройки кнопкой ОК.
- При подключении к Банку проверяйте адрес сервера в адресной строке Internet Explorer. Он должен быть таким **https://ibank2.ru/**.
- Используйте встроенные в систему ДБО механизмы оповещения SMS о входе в систему и отправке документов в Банк.
- Запрещается работать в системе «Клиент-Банк» с общедоступных компьютеров, например, из интернет-кафе.

В случае компрометации ключа электронной подписи, а также повреждения программно – технических средств, на которых установлена Система (включая средства обработки, хранения и защиты информации) Клиент обязан выполнить следующие действия:

1. Прекратить использование ключей электронной подписи;

2. Обесточить компьютер, на котором установлена Система (принудительно отключить электропитание в обход штатной процедуры завершения работы; извлечь аккумуляторную батарею из ноутбука);

3. Отключить компьютер от информационных сетей (если было подключение по Ethernet, USB, Wi-Fi и др.);

4. Незамедлительно проинформировать об этом Банк с использованием Блокировочного слова по телефону и (или) электронным письмом;

5. Предоставить письменное подтверждение Банку не позднее следующего рабочего дня со дня наступления обстоятельства, свидетельствующего о компрометации.

Будьте внимательны, наступление следующих событий может свидетельствовать о компрометации ключевой информации:

- Утеря Ключевого носителя с последующим обнаружением и без;
- Обнаружения факта несанкционированного доступа к Ключевому носителю;
- Нарушение правил использования и хранения Ключевого носителя;
- Обнаружение нарушение целостности программного обеспечения на компьютере, на котором установлена система «Клиент-Банк»;
- Обнаружение вредоносного программного обеспечения на компьютере, на котором установлена система «Клиент-Банк» или ином компьютере входящим с ним в одну локальную сеть;
- Обнаружение нарушение топологии локальной сети клиента (временное или постоянное);
- Обнаружение попыток сетевых атак на компьютер, на котором установлена система «Клиент-Банк» или иной компьютер входящим с ним в одну локальную сеть;
- Невозможность входа в систему «Клиент-Банк» при наличии соединения;
- Невозможность входа в систему «Клиент-Банк» в результате неавторизированной смены пароля ключевого носителя;
- Нестабильное функционирование компьютера , на котором установлена система «Клиент-Банк» (медленная работа, произвольная перезагрузка и д.р.) или его выход из строя;
- Появление на экране сообщений с требованием ввода кодов, паролей не предусмотренных функциональными свойствами системы «Клиент-Банк»;
- DDoS-атаки на ИТ инфраструктуру клиента;
- Несоответствие порядковых номеров платежных документов;
- Иные подозрительные обстоятельства.

Если какие либо пункты Вам не понятны, пожалуйста, посоветуйтесь с Вашим IT специалистом. За любой дополнительной информацией по обеспечению безопасности, пожалуйста, обращайтесь по следующим координатам:

Контактный телефон: 725 10 20 доб. 194

E-mail: support.ru@denizbank.com.