SDM-BANK

Основы безопасной работы с системой «БАНК-КЛИЕНТ» в соответствии с рекомендациями Центрального Банка РФ

Введение

В настоящее время участились случаи неправомерного доступа к конфиденциальной информации пользователей системы «БАНК-КЛИЕНТ» путем применения технических средств, позволяющих производить эти действия удаленно.

Для профилактики мошеннических действий Центральный Банк РФ разработал рекомендации, основные тезисы которых представлены в данной презентации.

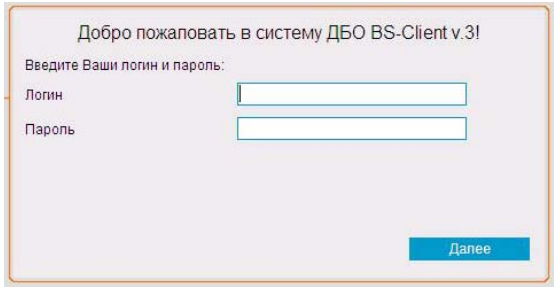
SDM-BANK

О системе «БАНК-КЛИЕНТ»

«БАНК-КЛИЕНТ» — это система дистанционного банковского обслуживания, позволяющая управлять своими банковскими счетами в любое время и в любом месте с помощью Интернета.

Основными компонентами, обеспечивающими безопасность системы «БАНК-КЛИЕНТ» являются:

•конфиденциальные данные клиента для входа в систему (логин и пароль);



•электронная цифровая подпись (электронный ключ).

SDM-BANK

ВАЖНО!

Банк не имеет:

- доступа к Вашему паролю на вход в систему;
- возможности подписания документов с помощью электронного ключа от имени Вашей организации.

За сохранность конфиденциальных данных ответственность несет Клиент.

SDM-BANK

Основные источники риска

1. Хакеры – компьютерные мошенники, которые распространяют вирусы и троянские программы, похищающие конфиденциальную информацию, и использующие ее для получения материальной выгоды.

2.Приходящие программисты (устанавливающие или обновляющие какие-либо программы).

3.Сотрудники Вашей фирмы, в особенности:

- Сотрудники, имеющие доступ к конфиденциальной информации и электронному ключу;
- Системные администраторы.

SDM-BANK

SDM-BANK

Способы хищения конфиденциальной информации и меры противодействия Злоумышленникам

Копирование конфиденциальных данных через Интернет

Действия Злоумышленников:

При посещении сайтов, особенно развлекательного характера, могут загружаться созданные хакерами специализированные программы-трояны, которые при подключению к Интернету копируют конфиденциальные данные и пересылают их Злоумышленнику.

Противодействие:

- запретить доступ с этого компьютера на все сайты, за исключением сайтов СДМ-БАНКА и других банков, чьими системами «БАНК-КЛИЕНТ» пользуется компания;
- не устанавливать на этом компьютере интернет-пейджеры (ICQ, Mail.ru-Агент и др.).

SDM-BANK

ВАЖНО!

Программы-трояны очень опасны, поскольку незаметно для пользователя происходит:

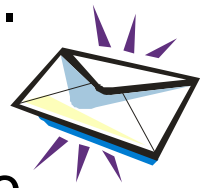
- заражение компьютера;
- хищение ими конфиденциальных данных.

SDM-BANK

Копирование конфиденциальных данных при посещении поддельного сайта Банка

Действия Злоумышленников :

Клиенту по электронной почте хакер направляет сообщения, в которых под какими-либо предлогами (техническое перевооружение организации и т.п.) предлагается пройти по ссылке на сайт банка (поддельный, очень похожий на настоящий), где предлагается ввести логин и пароль для входа в систему «БАНК-КЛИЕНТ».



Противодействие:

- не открывайте электронные письма от неизвестного адресата;
- не отвечайте на подозрительные письма с просьбой выслать электронный ключ, логин и пароль.

SDM-BANK

ВАЖНО!

Банк никогда и ни при каких обстоятельствах не запрашивает у клиентов:

- конфиденциальную информацию об электронных ключах;
- логины и пароли.

SDM-BANK

Копирование конфиденциальных данных с помощью специального программного обеспечения (ПО)

Действия Злоумышленников:

Сотрудник (системный администратор) или приходящий программист, имеющий доступ к компьютеру, устанавливают ПО, которое копирует конфиденциальную информацию и пересылает ее Злоумышленнику по Интернету.

Противодействие:

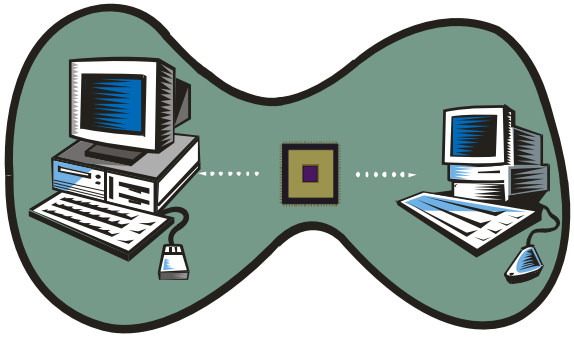
- не устанавливать на компьютер, с которого осуществляется работа с системой «БАНК-КЛИЕНТ», ПО, требующее обновления сторонними программистами;
- в случае наличия такого ПО, неотступно контролируйте действия приходящего программиста.

SDM-BANK

Копирование конфиденциальных данных через локальную сеть

Действия Злоумышленников:

Сотрудник Компании или приходящий программист через локальную сеть копирует конфиденциальную информацию.



Противодействие:

Запретить доступ по локальной сети на компьютер, с которого осуществляется работа с системой «БАНК-КЛИЕНТ».

SDM-BANK

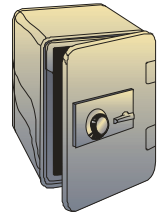
Копирование или физическая кража конфиденциальных данных

Действия Злоумышленников:

Сотрудник или посетитель Компании копирует конфиденциальную информацию (электронный ключ, логин и пароль) к себе на носитель (флэшку) или же просто их крадет.

Противодействие:

- не оставлять в общедоступном месте конфиденциальную информацию;
- электронный ключ вставлять в компьютер только при работе с системой «БАНК-КЛИЕНТ»;
- После завершения сеанса убирать электронный ключ в недоступное место (сейф).



SDM-BANK

SDM-BANK

Меры по профилактике хищения конфиденциальной информации

Организационные меры

1. Сотрудники, имеющие доступ к конфиденциальной информации и к компьютеру, с которого осуществляется работа с системой «БАНК-КЛИЕНТ» (бухгалтер, системный администратор и др.), должны быть проверенными сотрудниками.
2. Никогда не копируйте электронный ключ на жесткий диск компьютера.
3. Не используйте носитель с электронным ключом (флэшку) для хранения какой-либо другой информации.
4. Ограничите доступ к компьютеру, на котором осуществляется работа с системой «БАНК-КЛИЕНТ» (в том числе и по локальной сети).
5. Регулярно, не реже одного раза в месяц, производите смену пароля и не реже одного раза в год производите смену электронного ключа.
6. Не используйте компьютер для входа в систему «БАНК-КЛИЕНТ», находящийся в Интернет-кафе и в других общественных местах.

SDM-BANK

ВАЖНО!

Обязательно производить смену электронного ключа и пароля системы «БАНК-КЛИЕНТ» при:

- смене ответственных лиц, имеющих доступ к электронным ключам;
- смене системного администратора;
- компрометации электронного ключа или подозрении на нее.

SDM-BANK

Меры по защите компьютера

1. Устанавливайте на компьютере, на котором будет осуществляться работа с системой «БАНК-КЛИЕНТ», только необходимое программное обеспечение (ПО).
2. Операционная система и ПО, установленные на компьютере, должны быть лицензионными и регулярно обновляться.
3. Обязательно установите антивирусную программу и ПО защиты от несанкционированного доступа извне (firewall). Регулярно обновляйте антивирусную базу.
4. Рекомендуем установить пароль на электронный ключ, состоящий из букв и цифр и содержащий в себе не менее 8 символов.
5. Используйте для хранения электронного ключа устройство «eToken».

SDM-BANK

Что такое «eToken»?

«eToken» – это устройство предназначенное для хранения электронного ключа системы «БАНК-КЛИЕНТ», защищенное криптографической системой.

Преимущества «eToken»:

- ***Безопасное использование*** – воспользоваться им может только его владелец, знающий PIN-код авторизации;
- ***Невозможность*** прямого копирования электронного ключа;
- ***Удобство работы*** – ключ выполнен в виде брелока со световой индикацией режимов работы и напрямую подключается к USB-портам;
- ***Наличие сертификатов*** ФСТЭК (Гостехкомиссии) РФ, Microsoft и др.

SDM-BANK

ВАЖНО!

В СЛУЧАЕ ЕСЛИ:

- Компьютер неожиданно «зависает»;
- Компьютер самопроизвольно перезагружается;
- Пропаже данных;
- Появляются всплывающие окна;
- И прочих случаях необъяснимого или нехарактерного поведения компьютера.

Полностью воздержитесь от использования системы «БАНК-КЛИЕНТ» и обратиться в Службу технической поддержки Банка по тел.: 745-26-72.

SDM-BANK

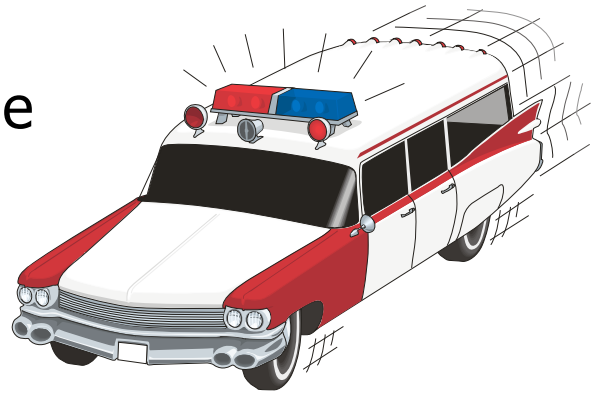
В ЭКСТРЕННЫХ СЛУЧАЯХ:

При обнаружении попыток несанкционированного доступа к счету или в случае опасений, что такие попытки могут быть осуществлены, необходимо сделать следующее:

1.Незамедлительно заблокировать электронный ключ и систему «БАНК-КЛИЕНТ» по телефону: **956-79-01**;

2.Проверить состояние Вашего счета;

3.Предоставить в Банк подробное описание инцидента.



SDM-BANK