Рекомендации Клиенту для обеспечения безопасности информации при использовании систем дистанционного банковского обслуживания

При работе с системами «Клиент-Банк», «СНГБ Онлайн Бизнес» или «СНГБ мобильный Онлайн Бизнес», Клиент в обязательном порядке должен соблюдать следующие рекомендации:

1. Рекомендации по защитным мерам для ПЭВМ

1) Для работы с системой «Клиент-Банк» рекомендуется использовать отдельный компьютер, доступ к которому имеют только лица, осуществляющие платежи в системе «Клиент-Банк».

2) Средствами BIOS компьютера следует исключить возможность загрузки операционной системы, отличной от установленной на жестком диске, т.е. должна быть отключена возможность загрузки с дискет, CD/DVD приводов, USB-flash дисков, загрузка по сети и т.п.

3) Доступ к изменению настроек BIOS должен быть защищен паролем.

4) ПЭВМ с системой «Клиент-Банк» / «СНГБ Онлайн Бизнес» по окончании рабочего дня рекомендуется выключать.

5) Не рекомендуется подключать к ПЭВМ с установленной системой «Клиент-Банк» / «СНГБ Онлайн Бизнес» внешние устройства, в том числе носители информации, не предусмотренные производственной необходимостью.

6) На компьютере, с которого осуществляется работа в системе «Клиент-Банк» / «СНГБ Онлайн Бизнес», необходимо использовать только лицензионное системное и прикладное ПО.

7) Рекомендуется своевременно проводить обновления системного и прикладного ПО.

8) На ПЭВМ с установленной системой «Клиент-Банк» / «СНГБ Онлайн Бизнес» должна быть установлена только одна операционная система.

9) В обязательном порядке должно быть установлено и регулярно обновляться антивирусное ПО (например, Kaspersky, Dr.Web, Symantec, Avira, ESET, NOD 32, McAfee) отдавайте предпочтение российским разработчикам. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов и другого вредоносного ПО.

10) Для работы с системой «Клиент-Банк» / «СНГБ Онлайн Бизнес» используйте только те ОС, которые **поддерживаются** производителем и для которых выходят регулярные обновления (например, Windows XP больше не поддерживается Microsoft).

11) Разработайте и утвердите в Вашей организации перечень программного обеспечения, разрешенного для установки и используемого на ПЭВМ. Стандартизировав ПО на ваших ПЭВМ, Вы значительно уменьшите потенциальные уязвимости на ПЭВМ.

12) Устанавливайте только то программное обеспечение, которое необходимо и достаточно для выполнения поставленных задач.

13) Следует принять меры, препятствующие несанкционированному вскрытию системных блоков ПЭВМ с установленной системой «Клиент-Банк» / «СНГБ Онлайн Бизнес». Заведите журнал опечатывания вычислительной техники. Опечатайте ПЭВМ с установленной системой «Клиент-Банк» / «СНГБ Онлайн Бизнес» с целью исключения неконтролируемого вскрытия ПЭВМ (защитные наклейки, пломбы и т.п.).

14) Рекомендуется полностью блокировать сетевой доступ к ресурсам ПЭВМ с установленной системой «Клиент-Банк» / «СНГБ Онлайн Бизнес».

15) На ПЭВМ с установленной системой «Клиент-Банк» / «СНГБ Онлайн Бизнес» рекомендуется ограничить использование сети Интернет пользователями системы «Клиент-Банк» / «СНГБ Онлайн Бизнес» т.е. ограничить список доступных для соединения адресов, например, разрешить только соединение с сервером системы «Клиент-Банк» / «СНГБ Онлайн Бизнес».

Категорически запрещено:

a. посещать социальные сети (например, ВКонтакте, Одноклассники, Facebook и др.), и другие ресурсы, не связанные с должностными обязанностями работника;

b. устанавливать и использовать программы мгновенного обмена сообщениями (например, ICQ, QIP, Mail.ru agent, Miranda);

c. устанавливать и использовать ПО для облачного хранения данных (например, GoogleDisk, YandexDisk, DropBox, Mail cloud и др.);

d. устанавливать и использовать программы, обеспечивающие голосовую и видео связь (Skype, Viber, Microsoft Lync и т.п.);

ВАЖНО: Возможность подключения к личным почтовым ящикам, интернет-системам обмена экспресс-сообщениями, а также сайтам социальных сетей должна быть исключена.

16) Рекомендуется ограничить или полностью отказаться от приема внешней (из сети Интернет) электронной почты. В обязательном порядке получаемая почта должна проверяться антивирусными средствами.

17) Пользователи системы «Клиент-Банк» / «СНГБ Онлайн Бизнес», работающие с системой не должны обладать правами администратора на ПЭВМ с установленной системой «Клиент-Банк» / «СНГБ Онлайн Бизнес», с целью ограничения возможностей установки под этими учетными записями программного обеспечения на ПЭВМ. Доступ к файловым ресурсам компьютера, особенно на запись, должен быть ограничен минимально необходимыми правами. Пользователи должны запускать только те приложения, которые им разрешены.

18) Локальными (или доменными) политиками на ПЭВМ рекомендуется ограничить список пользователей, имеющих возможность входа в операционную систему.

19) **ЗАПРЕЩЕНО: устанавливать, запускать, использовать на ПЭВМ с установленной системой «Клиент-Банк» / «СНГБ Онлайн Бизнес» ПО для удаленного управления (Например, RDP, TeamViewer, Radmin, Ammyy Admin др.).**

20) Для доступа к системе «Клиент-Банк» / «СНГБ Онлайн Бизнес» не используйте общедоступные компьютеры (например, установленные в интернет-кафе, гостинице), публичные беспроводные сети (бесплатный Wi-Fi и прочее).

2. Рекомендации по защитным мерам для мобильного устройства

1) Установить Приложение на мобильное устройство можно только из официальных репозиториев производителей мобильных платформ: AppStore и Google Play.

2) Установите на мобильное устройство антивирус и своевременно его обновляйте. Для платформы Android рекомендуем бесплатные приложения Dr.Web Light и Kaspersky Mobile Antivirus: AppLock & Web Security (доступны для загрузки из Google Play:).

3) Своевременно устанавливайте обновления безопасности операционной системы.

4) Не взламывайте свой телефон (например, через Jailbreaking, реинжиниринг, принудительное получение root-прав), так как это отключает защитные механизмы, заложенные производителем мобильной платформы. В результате ваш телефон становится уязвимым к заражению вирусным ПО.

5) Не отключайте и не взламывайте встроенные механизмы безопасности вашего устройства.

6) При наличии технической возможности включите шифрование данных на своём устройстве.

7) Помните, что Банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS/MMS/Email — сообщения.

8) Установите парольную защиту на мобильное устройство, данная возможность доступна для любых современных моделей мобильного устройства.

9) Завершайте работу с мобильным приложением через завершение сессии (кнопка «Выход»).

10) Отключайте в настройках вашего iPhone возможность использовать голосовое управление Siri на заблокированном экране.

11) Сохраняйте в тайне Ваши имя пользователя (логин), пароль для доступа в системы «СНГБ Онлайн Бизнес» / «СНГБ мобильный Онлайн Бизнес» и СМС-коды. Не сообщайте эти данные даже сотрудникам Банка.

3. Рекомендации по парольной защите

Учетные записи операционной системы с установленной системой «Клиент-Банк» должны быть защищены паролями с учётом следующих параметров:

1) Длинна пароля должна быть не менее 8 символов.

2) В пароле обязательно должны присутствовать заглавные и прописные (верхнего и нижнего регистра) символы, цифры, а также специальные символы (например, #, %, ^, * и т.п.); примеры паролей (hjf#48dft, 5$ma(fq5er, %der*2fvw2).

3) В качестве пароля не следует использовать имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе.

4) В качестве пароля не следует использовать повторяющуюся комбинацию из нескольких символов, либо комбинацию символов, набираемых в закономерном порядке;

5) Пароль должен меняться не реже 1 раза в 3 месяца, а также при компрометации (или подозрении в компрометации) пароля.

6) При смене пароля новый пароль не должен совпадать с ранее используемыми паролями.

7) Запрещено произносить вслух, записывать и хранить в любом доступном посторонним лицам месте пароли доступа к ПЭВМ и системе «Клиент-Банк» / «СНГБ Онлайн Бизнес» (например, на мониторе компьютера, под клавиатурой, на столе, в записной книжке и т.п.).

8) Запрещено: использовать стандартные пароли доступа к системам «Клиент-Банк» / «СНГБ Онлайн Бизнес» т.е., те, которые назначены по умолчанию производителем/разработчиком, они должны быть незамедлительно изменены.

9) Блокировать операционную систему, в случае перерыва в работе с ПЭВМ, одним из двух нижеприведенных способов:

– блокировать операционную систему (одновременно нажав клавиши ctrl+alt+del, далее в диалоговом окне нажать «блокировать компьютер»);

– блокировать операционную систему (одновременно нажав клавиши «windows» + L).

10) После 6 неудачных попыток получения доступа к ПЭВМ «Клиент-Банк» учетная запись пользователя должна быть заблокирована на 30 минут или до момента разблокировки учетной записи соответствующим администратором.

11) Принудительно завершайте сессию работы с системой «Клиент-Банк» / «СНГБ Онлайн Бизнес», выходом из системы.

12) Не храните логин и пароль в мобильном телефоне, смартфоне.

13) При отсутствии активности работника на ПЭВМ после авторизации, в течение 5 минут сеанс работы должен быть заблокирован или завершен.

4. Рекомендации по эксплуатации внешнего ключевого носителя

1) Для повышения уровня безопасности хранения ключей ЭП используйте устройства строгой аутентификации и хранения данных, такие как смарт-карта. Использование смарт-карты позволяет существенно снизить вероятность хищения ключей ЭП злоумышленниками.

2) Для надежной защиты ключа ЭП на смарт-карте рекомендуется установить надежный пароль согласно рекомендаций раздела 2 настоящего приложения.

3) Список лиц, имеющих доступ к внешнему ключевому носителю, определяется приказом или распоряжением руководства Клиента, согласно закрепленными за ними функциями и полномочиями.

4) Порядок хранения и использования внешнего ключевого носителя с ключом ЭП должен исключать возможность несанкционированного доступа к ним.

5) Внешний ключевой носитель должны храниться только у тех лиц, которым они принадлежат.

6) Во время работы с внешним ключевым носителем доступ к ним посторонних лиц должен быть исключен.

7) Внешний ключевой носитель должен быть установлен в ПЭВМ с системой «Клиент-Банк» / «СНГБ Онлайн Бизнес» только в момент подписания и при получении информации из Банка.

8) Для хранения внешнего ключевого носителя должны применяться надежные металлические сейфы.

9) По окончании рабочего дня, а также вне времени сеансов связи с системой «Клиент-Банк» / «СНГБ Онлайн Бизнес» внешний ключевой носитель должен храниться в сейфе.

10) Хранение внешнего ключевого носителя допускается в одном сейфе с другими документами, при этом отдельно от них и в упаковке, исключающей возможность негласного доступа к ним посторонних лиц (произвести опечатывание упаковки).

11) Уничтожение ключей ЭП может производиться путем физического уничтожения внешнего ключевого носителя, на котором они расположены, или путем стирания без повреждения внешнего ключевого носителя (для обеспечения возможности его многократного использования).

5. Рекомендации по использованию средства контроля целостности программного обеспечения

1) Для установки системы «Клиент-Банк» необходимо использовать файлы дистрибутивов, предоставленные Банком.

2) Вместе с пакетом программного обеспечения системы «Клиент-Банк» Банк предоставляет утилиту cpverify.exe, которая позволяет проверить целостность предоставляемых Банком дистрибутивов программного обеспечения системы «Клиент-Банк» и дистрибутива криптографического средства, сравнив со значениями контрольных сумм, указанными на официальном web-сайте Банка в сети Интернет по адресу: https://clbank.sngb.ru/v10/help/russian/html/control_hash.pdf. Для проверки значения контрольной суммы файла дистрибутива необходимо в командной строке ввести:

cpverify.exe – errwnd filename hashvalue

где ***filename*** - имя проверяемого файла; ***hashvalue*** – эталонное значение хэш-функции, 64 символа.

Если значения контрольных сумм не совпадают с эталонными, то на экран будет выведено окно с надписью ***"Integrity check failed"***.

3) **ВНИМАНИЕ! если контрольные суммы не совпадают с эталонными, запрещается устанавливать систему «Клиент-Банк», а также необходимо сообщить об этом в службу технической поддержки Банка. Возможно это является результатом мошеннических действий, направленных против вашей организации, и файлы дистрибутивов были подменены.**

6. Рекомендации по работе с системой «Клиент-Банк» / «СНГБ Онлайн Бизнес»

1) Вход в систему «СНГБ Онлайн Бизнес» осуществляйте только с официального web-сайта Банка в сети Интернет по адресу: https://biz.sngb.ru;.

Банк никогда не помещает ссылки на страницу входа в систему «СНГБ Онлайн Бизнес» в исходящей корреспонденции Клиентам.

Не входите в систему «СНГБ Онлайн Бизнес» из источников в Интернет, т.к. мошенники часто фабрикуют фишинговые сайты (сайты-двойники) для хищения Вашей аутентификационной (логин, пароль) и, как следствие, финансовой информации. При обнаружении сайта-двойника немедленно сообщите об этом в службу технической поддержки Банка и перешлите ссылку, с которой осуществлялся вход на него, для проведения расследования специалистами Банка.

2) При одновременном использовании двух ключей ЭП (например, ключа ЭП руководителя и ключа ЭП главного бухгалтера) желательно осуществлять работу с системой «Клиент-Банк» / «СНГБ Онлайн Бизнес» на двух разных ПЭВМ с хранением ключей ЭП на двух отдельных внешних ключевых носителях.

3) При работе нескольких пользователей в системе «Клиент-Банк» / «СНГБ Онлайн Бизнес» настроить строгое разграничение прав доступа к системе. Для получения рекомендаций по настройке разграничения прав доступа обратитесь в службу технической поддержки Банка.

4) Включить аудит пользователей в системе «Клиент-Банк». В этом случае все значимые действия пользователей в системе «Клиент-Банк» протоколируются. Администратор имеет возможность в любой момент просмотреть перечень произведенных пользователями действий в системе.

5) Подключить дополнительное средство защиты подтверждения платежа, в виде автономного генератора одноразовых паролей (устройство eToken PASS);

6) Подключить сотовой связи и/или электронной почты информацию о совершенных с использованием системе «Клиент-Банк» / «СНГБ Онлайн Бизнес» операциях по банковскому счету / «СНГБ мобильный Онлайн Бизнес».

7) Обязательно контролируйте движение денежных средств по выписке, предоставляемой по системе «Клиент-Банк» / «СНГБ Онлайн Бизнес» / «СНГБ мобильный Онлайн Бизнес».

8) Рекомендуется просматривать созданные и отправленные в течение дня ЭД в системе «Клиент-Банк» / «СНГБ Онлайн Бизнес» / «СНГБ мобильный Онлайн Бизнес» на предмет отсутствия несанкционированных распоряжений на перевод денежных средств (платежных поручений). В случае обнаружения таких платежей незамедлительно обратитесь в Банк.

9) Незамедлительно заблокируйте Вашу учетную запись, если обнаружили операции, которые Вы не совершали, успешные или неуспешные попытки входа с неизвестных Вам IP-адресов или в отличное для Вас время суток.

7. Рекомендации по организационным документам в области информационной безопасности

1) Соблюдайте правила информационной безопасности, регламент доступа к компьютерам для работы в системе «Клиент-Банк» / «СНГБ Онлайн Бизнес», регламент работы с ключами ЭП, в случае отсутствия таких документов, разработайте и утвердите.

2) Разработайте и утвердите регламент последовательности действий Клиента, осуществляемых при возникновении внештатной ситуации или при подозрении на неё (например, при обнаружение платежей, не созданных Клиентом, хищения внешнего ключевого носителя, компрометации ключа ЭП, смене должностного лица и т.п.).

3) Разработайте и утвердите регламент доступа к компьютерам и ключам ЭП, который в обязательном порядке должен содержать:

a. перечень событий, наступление которых должно повлечь за собой немедленную замену/изъятие ключей ЭП;

b. предупреждающую информацию об увеличении риска хищения и дальнейшего неправомерного использования ЭП при доступе к системе «Клиент-Банк» с рабочих ПЭВМ не настроенных в соответствие с правилами информационной безопасности.

4) Пользователи «Клиент-Банк» / «СНГБ Онлайн Бизнес» должны быть в обязательном порядке проинструктированы по вопросам соблюдения основных требований информационной безопасности и, в особенности, по вопросам использования антивирусных программ.

5) Для пользователей системы «Клиент-Банк» / «СНГБ Онлайн Бизнес» / «СНГБ мобильный Онлайн Бизнес» должны быть разработаны памятки на основе рекомендаций по информационной безопасности, приведенных в настоящем приложении.

6) Рекомендуется разработать следующие внутренние регламентирующие документы:

a. политика информационной безопасности;

b. положение по антивирусной защите;

c. правила соблюдения требований информационной безопасности;
d. положение о порядке предоставления доступа к ресурсам глобальной сети.

8. Работа с сообщениями

1) Не отвечайте на сообщения, требующие предоставить, подтвердить или уточнить вашу конфиденциальную информацию: пароли, логины, фамилию, имя, отчество, паспортные данные, номер мобильного телефона, на который поступают одноразовые пароли и другие данные. Банк никогда не связывается по телефону и не осуществляет рассылок сообщений по SMS или e-mail с таким запросом.

2) Не открывайте подозрительные файлы, поступившие Вам по электронной почте. Банк никогда не рассылает программы в своих электронных письмах и не связывается с просьбой установить или обновить программное обеспечение.

Не отвечайте на полученное подозрительное сообщение от имени Банка и не переходите по ссылкам, указанным в сообщении.

Помните!!!

Работники Банка никогда не будут спрашивать информацию о логине и пароле к системе ДБО. Если Вам позвонили, представились сотрудником Банка и в ходе дальнейшего разговора попросили сообщить информацию о логине и пароле, прекратите разговор и сообщите о случившемся в Банк.

Также будьте крайне внимательны, т.к. мошенники используют технологию подмены номера, т.е. Вам могут звонить с номера Банка, но это будет не Банк. Если Вы подозреваете, что Вам позвонил мошенник, положите трубку и перезвоните сами в Банк, по номерам, которые указаны на Вашей карте.

Если Вы заметили, что Вам приходят SMS/ PUSH-сообщения об операциях, которые Вы не совершали срочно обратитесь в Банк!

Обязательно проверяйте любую информацию относительно Ваших счетов и получаемых Вами услуг в Банке, поступившую от неизвестных лиц.

О подозрительных действиях сообщайте по телефонам 8 (3462) 39-88-04, 8-800-775-88-04 или 8-800-200-88-04.