+7 (495) 287-30-99
support@icbcmoscow.ru

РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СИСТЕМЕ ДБО

Соблюдение настоящих рекомендаций позволит обеспечить максимальную безопасность и контроль ваших счетов, снизить возможные риски при совершении электронных расчетов в Системе ДБО, противодействовать мошенничеству и неправомерным действиям злоумышленников, направленных на хищение денежных средств со счетов.

1. Клиент самостоятельно определяет порядок учета, хранения и использования носителей ключевой информации, генераторов СК, который должен полностью исключать возможность несанкционированного доступа к ним неуполномоченных лиц.

2. Никому, включая сотрудников Банка и родственников, ни при каких обстоятельствах, не сообщайте свой логин и пароль для входа в Систему ДБО, а также не передавайте им носитель ключевой информации или генератор СК. При получении такого запроса перезвоните в Банк по телефонам, указанным в настоящих рекомендациях, и сообщите о данном факте.

3. Банк, ни при каких обстоятельствах, не вправе потребовать от Вас конфиденциальную информацию (включая пароли и содержание поступающих СМС).

4. Логин, пароль, носитель ключевой информации, генератор СК необходимо хранить в тайне от третьих лиц, в том числе сотрудников Банка и родственников. Пароль на вход и PIN-код от носителя ключевой информации рекомендуется хранить отдельно.

5. Логин и пароль необходимо запомнить или, в случае если это является затруднительным, хранить их в неявном виде и недоступном для третьих лиц, в том числе сотрудников Банка и родственников, месте.

6. Не отправляйте свой логин и/или пароль с использованием SMS-сообщений, месенджеров и социальных сетей, а также почтой или электронной почтой.

7. Не вводите свой пароль доступа на сайтах, адрес которых отличен от адреса сайта Системы ДБО АйСиБиСи Банка (АО). Убедитесь в правильности адреса. Установление криптографически стойкого интернет-соединения должно быть подтверждено с помощью валидного ssl-сертификата Банка. В случае невозможности подключения к Системе ДБО, по его адресу, необходимо сообщать об этом в Банк.

8. Пароль доступа в Систему ДБО рекомендуется регулярно изменять, не хранить пароль в бумажном виде рядом с АРМом используемым для работы с системой ДБО.

9. Не следуйте по ссылкам, указанным в письмах (включая ссылки на сайт Банка), т.к. они могут вести на фишинговые сайты - двойники (наличие в адресе сайта дополнительных символов, содержание провокационной информации, отсутствие наименования разработчика сайта, а также электронный адрес для обратной связи или в качестве контактного адреса указан почтовый ящик на одной из бесплатных почтовых служб).

10. Остерегайтесь шпионских программ, которые могут проникнуть в ваш компьютер при открытии Интернет-страниц, содержащих заманчивые предложения или сенсации. Уделяйте повышенное внимание файлам, прикрепленным к сообщениям, полученным по электронной почте. Если не уверены в их происхождении, лучше не открывайте файлы с расширением .exe., .com., .bat., .pif., .vbs, .vbe, .cmd.

11. Доступ к компьютерам должен быть максимально ограничен только ответственным штатным IT-специалистам Клиента и только ответственным сотрудникам-владельцам ЭП. Носители ключевой информации следует закреплять за Уполномоченными лицами персонально, поскольку лишь в этом случае, Уполномоченное лицо уверено в абсолютной конфиденциальности Ключа ЭП и недоступности его даже для своих коллег, и в полной мере осознает ответственность за содержание ЭПД, подписанных его ЭП. Доступ неуполномоченных лиц к носителям с ключевой информацией, генераторам СК, логинам и паролям должен быть строго исключен. При обслуживании компьютера ИТ - сотрудниками, в т.ч. нештатными, приходящими по вызову, выполняющими профилактику и подключение к Интернет, установку и обновление бухгалтерских и справочных программ, установку и настройку другого ПО на компьютерах, с которых осуществляется работа по Системе ДБО, обеспечивать контроль над выполняемыми ими действиями.

12. При увольнении или смене ответственного сотрудника (включая смену генерального директора или главного бухгалтера), а также любых других действиях, затрагивающих изменение состава Уполномоченных лиц, имеющих доступ к Системе ДБО, необходимо незамедлительно в установленном порядке проинформировать об этом Банк и заблокировать ранее используемые этими лицами Ключи ЭП. Для новых Уполномоченных лиц должны быть сгенерированы новые Ключи ЭП. В этом случае рекомендуется также провести внеплановую смену оставшихся паролей и Кодового слова.

13. Для хранения носителей ключевой информации в помещении Клиента рекомендуется устанавливать металлические хранилища (сейфы), оборудованные надежными запирающими устройствами. Хранение носителей ключевой информации допускается в одном хранилище с другими документами в отдельном контейнере, опечатываемом Уполномоченным лицом.

14. Размещение технических средств в помещении, оборудованном АРМом Клиента, должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых они отражаются, через окна и др. проемы, средства видеофиксации над рабочим местом. Рекомендуется оборудовать системные блоки компьютеров, содержащие программное обеспечение СЭП (далее Средства Электронной Подписи), средствами контроля вскрытия. Вход в компьютер должен осуществляться только с использованием аутентификационных данных (имя пользователя/пароль). Не рекомендуется использовать учетную запись администратора компьютера для работы с Системой ДБО.

15. Ремонт и/или последующее использование системных блоков должны осуществляться после удаления с них программного обеспечения СЭП или демонтаж средств хранения информации.

16. В целях повышения безопасности проведения электронных платежей в Системе ДБО, предотвращения несанкционированного доступа с других рабочих мест и противодействия совершению мошеннических действий в отношении денежных средств на счетах Клиента - Банк настоятельно рекомендует воспользоваться бесплатно предоставляемой им услугой фильтрации IP-адресов и MAC-адресов компьютеров Клиента, с которых осуществляется работа в Системе ДБО. Для этого Клиентам, работающим по выделенному Интернет-каналу со статических IP - адресов, Банк рекомендует согласовать их список, исключительно с которых будет разрешена работа Клиента в

Системе ДБО. Со всех других IP-адресов, не вошедших в список разрешенных, работа по Системе ДБО данного Клиента будет запрещена. Клиентам при подключении необходимо заполнить и направить в Банк в письменном виде за подписью руководителя организации с удостоверяющей её печатью Заявление на ограничение работы в Системе ДБО с определенных адресов (Приложение № 9 к Условиям). Указанная услуга осуществляется в соответствии с Письмом Банка России от 30.01.2009 № 11-Т «О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга».

17. Банк информирует всех своих Клиентов, что не осуществляет рассылку электронных писем (а также не обращается по телефону) с просьбой прислать Ключ ЭП и пароль и не рассылает по электронной почте никакие программы. Любые письма подобного содержания от имени сотрудников Банка являются фальсификацией, после получения которых следует обратиться в банк к персональному менеджеру или сотруднику технической поддержки, а также донести информацию непосредственному руководителю.

18. Банк напоминает - вся ответственность за конфиденциальность Ключей ЭП Клиента, а также за ЭПД с корректными ЭП Клиента полностью лежит на Клиенте, как единственном владельце Ключей ЭП.

19. При Компрометации Ключей ЭП Клиент обязан предпринять все меры для прекращения любых действий в Системе ДБО, а также немедленно устно с помощью телефонной связи по телефону (495)-287-30-99 с предъявлением Кодового слова проинформировать службу техподдержки Системы ДБО Банка о данном факте.

20. По факту Компрометации Ключей ЭП Клиенту необходимо подать в Банк письменное заявление лично, либо по электронной почте, о блокировке его работы в Системе ДБО, а также организовать внутреннее расследование, результаты которого отражаются в акте служебного расследования.

21. Во избежание Компрометации Ключей ЭП рекомендуется при кратковременных перерывах в работе, а также по окончании рабочего дня производить блокировку компьютера; возобновление активности компьютера производить с использованием пароля доступа. Рекомендуется извлекать носитель ключевой информации из мест хранения только в моменты непосредственного предъявления его в компьютер для установки ЭП; все остальное время в течение сессии работы в Системе ДБО носитель ключевой информации рекомендуется хранить в защищенном месте.

22. Не допускается:

- пытаться записывать на носитель ключевой информации посторонние данные и файлы;
- совершать попытки снятия копии Ключей ЭП с носителя ключевой информации;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным;
- выводить содержимое Ключей ЭП на дисплей, принтер или другие внешние устройства отображения информации;
- вставлять носитель ключевой информации в устройство считывания в режимах, не предусмотренных штатным режимом работы Системы ДБО, а также в устройства считывания других компьютеров, не предназначенных для работы в Системе ДБО;

- оставлять ключевые носители без присмотра в устройствах считывания компьютера или на столе.

23. Рекомендуется устанавливать на все компьютеры, используемые при работе с Системой ДБО, лицензионное ПО, в том числе антивирусное, поддерживать в актуальном состоянии антивирусные базы, регулярно устанавливать обновления ОС Windows.

24. Обеспечить доверенную среду на компьютере, предназначенном для работы с Системой ДБО. Для чего:

- Выделять компьютер(ы), который(е) не будет(ут) использоваться Клиентом в иных целях, кроме как для работы в Системе ДБО.
- Установить на компьютере или на корпоративном сервере брандмауэр (firewall), запрещающий выход в Интернет с этого компьютера на иные сайты, за исключением информационного сайта Банка, операционного сайта Системы ДБО Банка и (при необходимости) сайтов Систем ДБО других банков, а также предотвращающий атаки на этот компьютер из сети Интернет и локальной сети, а также несанкционированный доступ к нему из сети.
- В случае необходимости подключить этот компьютер к локальной сети организации для обмена с бухгалтерскими системами, например, 1С, обеспечить защищенное и ограниченное по правам подключение данного компьютера к сетевому ресурсу БД 1С.
- Отключить возможность захвата удаленного управления с помощью терминального соединения компьютерами, используемыми для работы в Системе ДБО, заблокировав на Firewall порты 3389/tcp (RDP Remote desktop) и 5900/tcp (VNC) и отключив на этих компьютерах службу “Удаленного помощника”.
- Настоятельно не рекомендуется использовать для работы с системой ДБО программы подключения к удаленному рабочему столу, как пример anydesk, team vewer и тд. Это может повлечь за собой компрометацию используемой ЭП.
- Отключить "Гостевой доступ", заблокировав локальную учетную запись Guest на компьютере, работающем в Системе ДБО, а также не пользоваться при штатной работе административной учетной записью.
- Включить в операционной системе ведение журнала безопасности Windows, установить лицензионный антивирус и регулярно обновлять антивирусные базы, поддерживая их в актуальном состоянии.
- Иметь запасной компьютер, с которого можно будет осуществить оперативный вход в Систему ДБО в случае вирусной или иной атаки на основной компьютер.
- Не использовать помещения интернет-кафе или иных гостевых мест с выходом в Интернет в качестве временных рабочих мест Системы ДБО.

25. Рекомендуется осуществлять на регулярной основе (несколько раз в день) дополнительный контрольный вход в Систему ДБО для проверки состояния своих расчетных счетов по выпискам и отслеживания исходящих ЭПД за текущий день.

26. При невозможности входа в Систему ДБО или обнаружении подозрительных ЭПД, не созданных Клиентом, необходимо незамедлительно устно с помощью телефонной связи (телефон (495) 287-30-99) с предъявлением Кодового слова проинформировать Банк о данном факте.

В этом случае Банк заблокирует ЭПД, находящиеся в статусе "В обработке" до выяснения обстоятельств.

27. По факту блокировки входа в Систему ДБО и подозрительных ЭПД Клиенту также необходимо лично явиться в Банк, подав письменное заявление о блокировке и/или отзыве подозрительного платежа и получив в бумажной форме выписку по счетам.

28. Некоторыми характерными признаками проведения хакерской атаки на компьютер Клиента, задействованного в работе с Системой ДБО, являются:

- Сайт Системы ДБО Банка выглядит непривычным образом или в адресной строке браузера содержится ссылка на иной сайт, нежели сайт Системы ДБО Банка. При этом браузер на сертификат безопасности сайта выдает ошибку.
- Отсутствие возможности осуществить очередной вход в Систему ДБО с известным Клиенту паролем (при отсутствии иных причин для блокировки).
- Ключевой носитель не содержит контейнера с файлами ЭП или носитель внезапно поврежден/испорчен.
- В ОС Windows антивирусом обнаружен вирус/троян и т.п., либо антивирус выдает ошибку и не запускается.
- Необычное и нехарактерное поведение компьютера (спонтанные перезагрузки, особенно в сочетании с невозможностью последующей штатной загрузки, частые зависания в течение короткого промежутка времени, в т.ч. т.н. “синий экран смерти”).

29. Во всех вышеперечисленных случаях Клиенту следует незамедлительно прекратить попытки использования данного компьютера для работы с Системой ДБО, не пытаться самостоятельно устранить неисправность компьютера или вылечить вирус и обратиться в Банк с устным и письменным заявлениями о блокировке работы в Системе ДБО до выяснения всех обстоятельств и устранения причин, приведших к порче компьютера и/или ключевого носителя.