** Приложение №7**

к Соглашению об обслуживании банковского счета

с использованием системы обмена электронными

документами при идентификации клиента

с помощью ЛОГИНА/ПАРОЛЯ

№ \_\_\_\_\_\_\_ от «\_\_\_»\_\_\_\_\_\_\_ 20\_\_\_г.

## **Памятка по безопасному использованию сервиса ДБО**

Для защиты Вашего компьютера от вредоносных программ и для снижения риска совершения противоправных действий со стороны злоумышленников настоятельно рекомендуем проявить бдительность и использовать общий комплекс мер безопасности.

1. **Рекомендации по защите компьютера, с которого осуществляется использование сервиса ДБО:**
   1. Старайтесь использовать современные версии операционных систем (далее - ОС). Как правило, они являются более защищёнными в отличие от предыдущих, зачастую устаревших, версий. Своевременно устанавливайте исправления и обновления для ОС и браузеров. Включите автоматическое обновление OC, которое будет устанавливать последние исправления, тем самым ликвидируя уязвимости.
   2. Размещение, специальное оборудование, охрана и организация режима в помещении, где размещено рабочее место для работы в системе ДБО «Банк-Клиент», должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.
   3. На компьютерах, используемых для работы в системе ДБО «Банк –Клиент», устанавливайте пароль на уровне BIOS и уровне операционной системы.
   4. Не вводите конфиденциальные данные, если окно для ввода отличается от стандартных окон Системы "Клиент-Банк" (логотип другого банка, другие надписи, шрифт и тому подобное) или отображается не так как всегда (нарушен порядок работы в системе)
   5. Внимательно следите за сообщениями, которые появляются на экране компьютера и проверяйте правильность адресной строки сайта (должна начинаться с <https://ibank.bankffin.ru>**.** Особое внимание уделяйте наличию протокола **https** в начале адреса, который свидетельствует о наличии защищенного соединения, так как злоумышленники часто используют ложные (фальсифицированные) ресурсы сети Интернет для хищения паролей и др. конфиденциальных данных.
   6. Используйте в работе только лицензионное программное обеспечение (далее - ПО).
   7. Не загружайте и не устанавливайте ПО, полученное из непроверенных источников. Используйте системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ (официальные поставщики или официальные сайты разработчиков). При этом необходимо обеспечить целостность получаемых на носителях или загружаемых из интернета установочных пакетов и обновлений.
   8. Установите и своевременно обновляйте на компьютере антивирусное ПО (Kaspersky Internet Security, BitDefender Internet Security, ESET Smart Security, Symantec Norton Internet Security, Avira Internet Security и т.д.).
   9. Антивирусное ПО должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов, уязвимостей и удаление обнаруженного вредоносного ПО.
   10. Используйте и оперативно обновляйте специализированное ПО для защиты информации: персональные межсетевые экраны, средства защиты от несанкционированного доступа и т.д.
   11. Соблюдайте регламент ограниченного физического доступа к данному компьютеру.
   12. Не подключайте к компьютеру непроверенные на наличие вирусов съёмные носители данных (флешки, диски, дискеты).
   13. Исключите обращения к интернет-ресурсам под пользователем, обладающим правами администратора ОС.
   14. Включите аудит системных событий ОС, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.
2. **Правила безопасной работы в Интернете:** 
   1. При выходе в интернет рекомендуется использовать лицензированный персональный межсетевой экран, разрешив доступ только к доверенным интернет-ресурсам. Не давайте разрешения неизвестным программам выходить в интернет.
   2. Запретите в межсетевом экране соединение с интернет по протоколам ftp, smtp. Разрешите соединения smtp только с конкретными почтовыми серверами, на которых зарегистрированы Ваши электронные почтовые ящики.
   3. Используйте компьютер в интернете только для работы с доверенными сайтами и получения электронной почты.
   4. Убедитесь в наличии символа замка в правом нижнем углу веб-страницы или справа/слева от адресной строки что веб-адрес в адресной строке начинается с "https". Этот указывает на то, что веб-сайт работает в защищенном режиме.
   5. Не нажимайте на всплывающие окна, которые содержат рекламу. Вы можете непреднамеренно загрузить на свой компьютер вирусы и шпионские программы. Желательно настроить ваш браузер на автоматическую блокировку таких окон.
   6. Не читайте подозрительных электронных писем от незнакомых людей, они могут содержать вирусы. Читайте темы сообщений внимательно; если не уверены, что письмо пришло из надежного источника, не открывайте его. Не доверяйте дружественному тону сообщений или срочности содержащейся в них просьбы. В подозрительных письмах не нажимайте на содержащиеся в письме ссылки, а также не открывайте вложенные файлы, особенно если в письме указано, что проблема безотлагательная, и при этом просят срочно открыть приложенный файл, который имеет файловое расширение "exe", ".scr" и т.д.
   7. По окончании работы с сервисом ДБО обязательно завершите сеанс работы нажатием ссылки «Выйти».
   8. Максимально ограничьте использование интернет-пейджеров (ICQ и подобные).
   9. При работе в интернет не соглашайтесь на установку каких-либо дополнительных программ.
   10. Старайтесь избегать использования сервиса ДБО в местах с общественным доступом в интернет, например, в интернет-кафе или через подключение к общественным точкам с незащищенным WI-FI соединением (в кафе, гостиницах, торговых центрах и т.д.). После подобного использования рекомендуем сменить пароль, используя ваш персональный компьютер.
   11. Будьте внимательнее к странным или непонятным сообщениям об ошибках браузера. В случае возникновения подозрений просканируйте свой компьютер на наличие вирусов или шпионского программного обеспечения.
3. **Управление паролями**
   1. Пароль должен содержать не менее 8 символов
   2. Пароль должен включать буквы верхнего и нижнего регистра, цифры и спецсимволы (@, # , $ , % , < , ^ , & , \* ). Например “Fktr?<2015>”.
   3. Для использования ДБО следует применять уникальный пароль. Опасно применять простые вариации одного и того же пароля от почты, социальных сетей и прочих интернет-сервисов. Например, «Vasiliy01», «Vasiliy02», «Vasiliy03».
   4. Не стоит в пароле применять слова, очевидно ассоциирующиеся с вами, особенно если вы пишете что-то о себе в социальных сетях – злоумышленники смогут найти эту информацию без особых хлопот. Поэтому имя кота, ребенка, дата рождения, – очень неудачный и нестойкий пароль.
   5. Не производите установку галочки «Запомнить пароль». Делайте это, только если вы абсолютно уверены в том, что никто не воспользуется вашим компьютером без Вас. Лучше набирать логин и пароль всякий раз, при входе в сервис ДБО.
   6. Используйте виртуальную клавиатуру при вводе пароля.
   7. Подключите дополнительные средства защиты: разовые SMS-пароли, которые будут приходить на указанный вами номер мобильного телефона. Пароль необходимо вводить для подтверждения входа в сервис ДБО и платежей, относимых системой контроля сервиса ДБО к категории потенциально рисковых.
   8. Ни при каких обстоятельствах не передавайте и не сообщайте никому (в том числе родственникам и друзьям) данные для входа в сервис ДБО, пароли для подтверждения платежей.
   9. Никогда не отвечайте на электронные письма, входящие звонки, SMS-сообщения, письменные/устные обращения, в которых запрашивается ваша персональная информация и особенно учетные данные и пароли. Злоумышленники могут представляться сотрудниками банка, государственных органов, служб, сотовых компаний и др.
   10. Никогда ни при каких обстоятельствах не называйте свой пароль, даже если вы сами звоните по контактному телефону службы технической поддержки сервиса ДБО, а также помните, что администрация сервиса не рассылает сообщений по e-mail и не звонит клиентам по телефону с просьбой предоставить пароль для совершения каких-либо действий.
   11. Никогда не входите в сервис ДБО и не набирайте пароль с незнакомого компьютера, или с компьютера, на который имеют доступ лица, незнакомые вам или не вызывающие полного доверия.
   12. Избегайте регистрации номера вашего мобильного телефона, на который приходят SMS с разовым паролем, в социальных сетях и других открытых источниках.
   13. В случае утери мобильного телефона, на который направлялись разовые пароли, немедленно заблокируйте SIM-карту.
   14. В случае обнаружения подозрительных действий, совершенных от вашего имени в ДБО (в выписке обнаружены несанкционированные Вами расходные операции, либо Вы получили SMS или e-mail-уведомление об операции, которую не совершали.), незамедлительно смените логин и пароль, а также обратитесь в банк.
   15. Дополнительные специализированные рекомендации по обеспечению безопасности вы сможете найти на официальном интернет-ресурсе разработчиков ДБО **faktura.ru** в разделе «Безопасность» и на интернет-ресурсе банка **bankffin.ru** раздел «Ваша безопасность».
   16. Выходите из системы ДБО "Банк-Клиент" при перерывах и завершении работы в системе ДБО**. (*С помощью вредоносных программ со встроенным механизмом удаленного управления (RAdmin, TeamViewer, VNC и др.) злоумышленники могут подключиться к консоли инфицированного компьютера, подключиться к порталу банка и использовав ранее перехваченный пароль доступа злоумышленники от имени клиента могут зайти в систему ДБО «Банк-Клиент», создать платежные поручения, подписать их и отправить в банк.)***
   17. Незамедлительно сообщайте в Банк о факте невозможности получения доступа к Системе "Клиент-Банк", по причине несовпадения пароля на вход в систему. Обычной практикой злоумышленников является смена пароля для маскировки своих действий и получения дополнительного времени для успешного выполнения операций от имени Клиента.
   18. При компрометации или попытке компрометации ЛОГИНА/ПАРОЛЯ, увольнения ответственного сотрудника или ИТ специалиста, который имел доступ к компьютеру, **срочно** обратитесь в Банк для блокировки ЛОГИНА/ПАРОЛЯ и генерации новых.