МОСКОМБАНК
Commercial Bank of Moscow

ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В целях обеспечения информационной безопасности при работе в Системе ДБО **Клиент обязуется**:

1. Осуществлять вход в Систему ДБО только через Сайт (Интернет-банк), либо через мобильное приложение (Мобильный банк), которое может быть установлено на мобильное устройство из рекомендуемых Банком интернет-магазинов (репозиториев), таких как AppStore, Google Play, NashStore и другие, или путем загрузки и установки аналогичного официального приложения с официального Сайта Банка.
2. Не отвечать на письма, в том числе от имени Банка, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену Банка: https://moscombank.ru или Системы ДБО https://dbo.moscombank.ru, сменить пароль доступа к нему, а немедленно сообщить о подобном факте в рабочие часы Банка по телефону (495) 109-00-14. Банк не осуществляет рассылку подобных электронных писем, а также не рассылает по электронной почте программы для установки на компьютеры Клиентов. Связь с Клиентами поддерживается по телефону лично или средствами Системы ДБО.
3. Не отлучаться от устройства с установленным ДБО в период активной сессии с Системой ДБО, либо завершить активную сессию ДБО.
4. Не передавать логины, пароли, пин-коды и коды доступа другим лицам, в том числе сотрудникам Банка для проверки работоспособности или настройки Системы ДБО, хранить их в надежном месте, исключающем доступ к ним посторонних лиц. Вся ответственность за сохранность и использование паролей, логина, пин-кода иного кода доступа для доступа в Систему ДБО, полностью лежит на Клиенте как единственном их владельце.
5. В случае выявления явных или косвенных признаков компрометации Логина или Пароля, а также обнаружения вредоносных программ в компьютере, используемом для работы в Системе ДБО, незамедлительно уведомить об этом Банк по телефону: (495) 109-00-14 либо лично явиться в Банк с целью блокирования скомпрометированных данных с последующей их заменой. К событиям, связанным с компрометацией, относятся, включая, но не ограничиваясь, следующие:
   - обнаружение факта или угрозы использования (копирования) идентификаторов учетной записи или паролей доступа к Системе ДБО неуполномоченных лиц (несанкционированная отправка электронных документов);
   - обнаружение ошибок в работе Системы ДБО, в том числе возникающих в связи с попытками нарушения информационной безопасности;
   - обнаружение воздействия вредоносного кода в компьютере, планшете, мобильном устройстве, мобильном телефоне, используемом для работы в Системе ДБО.
6. В случае выявления явных или косвенных признаков компрометации пароля учетной записи Клиент обязан менять данный пароль самостоятельно.
7. Обеспечивать конфиденциальность использования логина, паролей, пин-кодов, кодов доступа, которые не требуется сотрудникам Банка для обслуживания Клиента и поддержки Системы ДБО в работоспособном состоянии.
8. Применять на устройствах, используемых для работы Системы ДБО, лицензионные средства антивирусной защиты с возможностью автоматического обновления антивирусных баз и специализированные программные средства безопасности: персональные файерволы, антикейлоггеры, антиспам-фильтры.
9. Производить периодическую (не реже 1 раза в 3 месяца) смену долговременного пароля, а также по требованию Банка и в случае компрометации. Не использовать простые па-

роли (например, 123, qwerty, имена, даты рождения, простые слова, фамилии, клички животных, бренды).
10. Самостоятельно убедиться, либо что используемое оборудование и программное обеспечение настроено для работы с сетью Интернет по защищенному протоколу https.
11. Не использовать на своем устройстве любые средства удаленного (дистанционного) доступа, которые обычно практикуют IT-специалисты для удаленной (дистанционной) поддержки (например, TeamViewer, AnyDesk, Ammy Admin и т.п.). Удалить или заблокировать возможность использования таких средств с помощью межсетевого экрана (программного и/или аппаратного).
12. При использовании мобильного устройства установить на него антивирусное программное обеспечение и пароль доступа к устройству, не использовать мобильное устройство с расширенными правами (Jailbreak/Root), так как это значительно снижает уровень обеспечения безопасности устройства. Регулярно устанавливать обновления для Вашего устройства и установленного антивирусного программного обеспечения, защитить свое мобильное устройство кодом блокировки экрана, паролем или отпечатком пальца.
13. Не устанавливать на мобильное устройство, используемое для приема СМС-сообщений или Пуш-уведомлений с подтверждающим одноразовым Паролем, приложения, полученные от неизвестных Вам источников. Помните, что Банк не рассылает своим Клиентам ссылки или указания на установку приложений.
14. При утрате мобильного устройства или SIM-карты, используемых для приема СМС-сообщений или Пуш-уведомлений с подтверждающим одноразовым Паролем, немедленно обратиться к своему оператору сотовой связи и заблокировать SIM-карту. После этого связаться с Банком для временного прекращения предоставления доступа к Системе ДБО и проверки последних платежей.
15. Принимать звонки и СМС от Банка только номеров телефонов Банка: +74951090014, +74956091919, +73833358811.

Помимо указанных выше требований Банк рекомендует:

1. Перед началом работы проверить наличие защищенного (шифрованного) соединения с сервером Системы ДБО. Признаком установки защищённого соединения является наличие информации о протоколе https в адресной строке используемого клиентом браузера, в некоторых браузерах при защищенном соединении адресная строка будет подсвечена зеленым цветом.
2. Использовать виртуальную клавиатуру. Виртуальная клавиатура повышает степень защищенности Вашего пароля от перехвата злоумышленниками. Виртуальная клавиатура появляется при входе в Систему ДБО. При входе в Систему наберите Ваш Логин на обычной клавиатуре. Затем для ввода Пароля используйте виртуальную клавиатуру: при помощи указателя мыши введите на виртуальной клавиатуре пароль доступа к Системе ДБО (если пароль содержит заглавную букву или символ, нажмите клавишу Shift, переключение между русским и английским алфавитом - клавиша Рус/Lat, для удаления предыдущего символа используется стрелочка), по окончании ввода пароля нажмите Enter.
3. Исключить доступ посторонних лиц к компьютеру или мобильному устройству, использующемуся для работы в Системе ДБО. Осуществлять постоянный контроль отправляемых платежных электронных документов при работе в Системе ДБО, а также состояние своего личного счета.
4. Избегать работы в Системе ДБО при подключении к публичным точкам доступа Wi-Fi, в интернет-кафе и на других компьютерах общего пользования, контролировать информацию об IP-адресе, с которого осуществлялся предыдущий вход в Систему ДБО.
5. Не записывать используемый Пароль там, где доступ к нему могут получить посторонние лица.
6. Использовать только лицензионное, поддерживаемое производителем программного обеспечения (операционные системы, офисные пакеты), обеспечить автоматическое об-

новление системного и прикладного программного обеспечения, исключить использование самодельных «сборок» и взломанного программного обеспечения.
7. Использовать дополнительные средства безопасности программного обеспечения - антивирусные программы, программы защиты от спам-рассылок и пр.

8. В качестве дополнительной меры по обеспечению информационной безопасности воспользоваться предоставляемой Банком возможностью IP-фильтрации (разрешение доступа к Системе ДБО только с указанных Клиентом IP-адресов/сетей).