Приложение 3
к Правилам дистанционного банковского обслуживания физических лиц,
в "Банк "МБА-МОСКВА" ООО,
редакция 01.001.002

ПАМЯТКА по соблюдению мер безопасности при пользовании Системой дистанционного банковского обслуживания физических лиц в "Банк "МБА-МОСКВА" ООО

"Банк "МБА-МОСКВА" ООО (далее - Банк) одной из приоритетных задач считает обеспечение современного, комфортного, качественного и безопасного дистанционного обслуживания своих Клиентов, предлагая одну из лучших систем дистанционного банковского обслуживания физических лиц (далее - Система ДБО). Однако, гарантией ее максимально безопасного использования являются совместные усилия Банка и Клиента. Поэтому Банк информирует Вас об основных правилах по соблюдению мер безопасности, выполнение которых позволит Вам максимально безопасно работать с Системой ДБО физических лиц, защитить себя от мошенничества и свести финансовые потери к минимуму.

1. Пожалуйста, внимательно прочитайте нижеизложенную информацию и следуйте нашим РЕКОМЕНДАЦИЯМ по работе с Системой ДБО:

1.1. Вход в Систему осуществляется только через корпоративный сайт Банка https://ibam.ru/ и/ или через официальное Мобильное приложение Банка «МБА-МОСКВА Онлайн».

1.2. Если Вам пришли письма, в том числе от имени Банка, содержащие требования (а также просьбы или предложения) зайти на сайт, адрес которого начинается не с адреса Банка, указанного в п. 1.1. настоящей Памятки, и/ или прислать логин или пароль доступа к Системе ДБО Банка, ни в коем случае не отвечайте. Вам нужно сообщить об этом событии в Банк как можно оперативнее по телефону +7 (495) 025-25-25 в рабочее время Банка. Банк никогда не рассылает Клиентам подобные электронные письма, а также не рассылает по электронной почте программы для установки на компьютеры.

1.3. Никогда не отлучайтесь от компьютера или мобильного устройства, пока работаете в Системе ДБО.

1.4. После завершения работы в Системе ДБО сразу нажимайте кнопку «Выход».

1.5. Вы должны обеспечить строго конфиденциальное использования Логина и Пароля доступа. Работникам Банка для вашего обслуживания и поддержки Системы ДБО в работоспособном состоянии пароли не требуются.

1.6. Обязательно применяйте средства антивирусной защиты с возможностью автоматического обновления антивирусных баз

1.7. Как можно быстрее производите смену Пароля доступа, как в случае его рассекречивания, так и по требованию Банка.

1.8. В целях безопасности, в системе ДБО необходимо осуществлять смену Пароля на любой другой, отличный от ранее используемых, с регулярностью изменения не реже 1 раза в квартал. При осуществлении первого входа в систему ДБО изменить временный Пароль для первичного входа на постоянный Пароль. Банк рекомендует изменять Пароль не реже 1 раза в месяц.

1.9. Не используйте для защиты данных очевидные пароли, которые легко угадать: имя супруга (супруги), ребенка, домашнего животного, номера телефонов, регистрационный номер машины, почтовый индекс и пр.

1.10. Не осуществляйте вход в систему ДБО в местах, где услуги Интернета являются общедоступными, и/или с использованием публичных беспроводных сетей, например, в Интернет-кафе или в общественном транспорте. После подобного использования рекомендуется сменить пароль. Не использовать незащищенное Wi-Fi подключение или защищенное «простым» паролем («сложным» считается пароль, длина которого — не менее 8 символов. Такой пароль в обязательном порядке должен включать буквы верхнего и нижнего регистра, цифры и спецсимволы (@, #, $, %, <, ^, &, *), не должен быть повторяющимся и содержать слова целиком).

1.11. В случае выявления явных или косвенных признаков рассекречивания Пароля доступа или наличия вредоносных программ в компьютере или на Мобильном устройстве, используемом для работы в Системе ДБО, Вам нужно уведомить об этом Банк как можно оперативнее по телефону +7 (495) 025-25-25 в рабочее время Банка, либо лично явиться в Банк, чтобы заблокировать Пароль доступа, с последующей заменой. О нарушении секретности могут свидетельствовать следующие события:

— обнаружение факта или угрозы использования (копирования) Пароля доступа;

— получение 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.

1.12. Устанавливайте Мобильное приложение «МБА-МОСКВА Онлайн» и его обновления только из магазина приложений App Store и Google Play.

1.13. Установите пароль доступа к Вашему мобильному устройству.

1.14. Не храните на Мобильном устройстве конфиденциальную информацию (PIN коды платежных карт, пароли доступа, кодовое слово и т.д.).

1.15. Удаляйте конфиденциальную информацию в случае передачи Мобильного устройства другим лицам (продажа устройства, передача в ремонт).

1.16. Исключите доступ посторонним лицам к компьютерам и Мобильным устройствам, используемым для работы в Системе ДБО.

1.17. При обслуживании компьютера и Мобильного устройства ИТ-специалистами рекомендуется контролировать все выполняемые ими действия.

1.18. На компьютерах, используемых для работы с Системой ДБО, исключите посещение интернет- сайтов сомнительного содержания, загрузку и установку нелицензионного ПО.

1.19. В случае утери мобильного устройства с установленным Мобильным приложением «МБА-МОСКВА Онлайн» или обнаружения блокировки SIM-карты без Вашего ведома, как можно оперативнее заблокируйте SIM-карту у оператора сотовой сети и заблокируйте доступ к Системе ДБО, позвонив в Банк по телефону +7 (495) 025-25-25 в рабочее время Банка.

1.20. Вводите Одноразовые пароли (SMS-коды) только в том случае, если операция инициирована Вами. При получении SMS-сообщения с Одноразовым паролем внимательно ознакомьтесь с его содержанием, обязательно проверьте детали и составляющие операции, которую Вы подтверждаете одноразовым SMS-кодом. Вводить SMS-код в систему следует только тогда, когда реквизиты и детали Вашей операции в системе ДБО соответствуют реквизитам в полученном SMS — сообщении.. Никогда не вводите код подтверждения, не соответствующий операции.

1.21. В целях повышения безопасности, рекомендуем не пользоваться системой ДБО с того же мобильного устройства, на который приходят SMS-сообщения с подтверждающим Одноразовым паролем.

1.22. В качестве дополнительных мер по обеспечению безопасности воспользоваться предоставляемой Банком возможностью установки ежедневных лимитов.

1.23. Соблюдайте общие правила безопасного использования мобильного устройства:

— регулярно менять Пароль на вход в операционную систему, на которой установлена Система ДБО;

— необходимо использовать лицензионное программное обеспечение, межсетевые экраны и средства защиты от несанкционированного доступа, обеспечить автоматическое обновление системного и прикладного ПО;

— необходимо установить и активировать антивирусные программы, специализированные программные средства безопасности: персональные файрволы, антишпионское программное обеспечение и т.п., обеспечить возможность автоматического обновления антивирусных баз, а также еженедельно проводить антивирусную проверку. Обратите внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам информации о Вашем Пароле и ключах ЭП;

— При скачивании контента надо внимательно читать условия использования сервиса, а также информацию, размещенную с символом «звездочка» (*);

— избегайте настроек типа **root** и **jailbreak**;

— необходимо быть осторожным при всплывающих окнах и не переходить по неизвестным ссылкам и адресам.

2. Запрещается:

2.1. Использовать переадресацию SMS на другое устройство - при получении Одноразовых паролей для работы с Системой ДБО.

2.2. Сообщать кому-либо, записывать куда-либо (кроме соответствующих окон Системы ДБО) Одноразовые пароли из SMS для работы с Системой ДБО.

2.3. Записывать (кроме соответствующего окна Системы ДБО) постоянный Пароль для Системы ДБО на любой электронный носитель или в любое электронное устройство; постоянный пароль рекомендуется помнить, но если это совершенно исключено, то пароль следует записать только на небольшой лист бумаги, без указания рядом слов Система ДБО Банка, «МБА-МОСКВА Онлайн» или похожих на них, номера телефона, использующегося для входа в Систему ДБО; такой лист необходимо хранить в недоступном для посторонних месте, никогда не копируя, не фотографируя и не допуская попадания его на видео.

2.4. Сообщать постоянный Пароль для Системы ДБО кому-либо, в том числе ближайшим родственникам, своим доверенным лицам, представителям Банка и правоохранительных органов.

2.5. Вводить постоянный Логин / Пароль в Систему ДБО под наблюдением любых лиц или в зоне фиксации видеокамер.

2.6. Использовать для входа в Систему ДБО простой постоянный пароль или пароль, использующийся в иной системе (социальные сети, личном кабинете и т. д.).

2.7. Оставлять без присмотра в доступном недоверенным лицам месте устройство, получающее SMS-коды для подтверждения операций в Системе ДБО.

2.8. Не рекомендуется использовать средства сохранения постоянного Пароля в устройстве (использовать галочку «Запомнить пароль» в окне ввода Пароля при ее наличии).

Соблюдение рекомендаций, содержащихся в настоящей Памятке, являющейся неотъемлемой частью Правил дистанционного банковского обслуживания физических лиц в "Банк "МБА-МОСКВА" ООО с использованием Системы ДБО и Мобильного приложения «МБА-МОСКВА Онлайн», позволит обеспечить максимальную сохранность денежных средств, а также снизит возможные риски при совершении операций в Системе ДБО, в частности, при осуществлении платежей в пользу поставщиков услуг (мобильные операторы, интернет-провайдеры и т.д.), переводах денежных средств как внутри Банка, так и на счета, открытые в других кредитных организациях.

В случае невыполнения Вами основных правил по соблюдению мер безопасности, содержащихся в настоящей Памятке Вы утрачиваете право предъявления Банку претензий в связи с кражей Ваших денежных средств или ограничением Банком Вашего доступа в Систему ДБО по причине такого нарушения.