ПАМЯТКА КЛИЕНТАМ БАНКА АВТО ФИНАНС БАНК – ЮРИДИЧЕСКИМ ЛИЦАМ

по обеспечению информационной безопасности в системе дистанционного банковского обслуживания (ДБО)

Важнейшим фактором, способствующим обеспечению безопасности, является личная заинтересованность Клиента. Банк считает необходимым соблюдение Клиентами следующего комплекса мер по защите информации.

1. Обеспечение безопасности компьютера, используемого для работы в системе ДБО

– Установите на используемый Вами для работы с системой ДБО компьютер лицензионную операционную систему и лицензионное антивирусное программное обеспечение и регулярно обновляйте их. В противном случае действие вредоносных программ может быть направлено на перехват Вашей персональной информации и передачу её третьим лицам. Рекомендуем использовать для работы с системой ДБО выделенный компьютер.

– Установите персональный брандмауэр (firewall) на Вашем компьютере, в настройках запретите несанкционированный удаленный доступ к Вашему компьютеру из сети Интернет и Вашей локальной сети с использованием удаленного управления компьютером и терминального доступа. Дополнительно можно настроить брандмауэр на доступ только по адресам системы ДБО и системы Личный кабинет (https://lk-dbo.autofinancebank.ru/f2b).

– В обязательном порядке следует отключать автозапуск в операционной системе (для OS Windows: «Панель управления» -> «Администрирование» -> «Службы»; необходимо найти в закладке «Расширенный» службу «Определение оборудования оболочки» и установить «Отключено»).

– Исключите посещение с компьютера сайтов сомнительного содержания и любых других Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы и т. д.), а также чтение почты и открытие почтовых документов от недостоверных источников.

– Категорически не рекомендуем работать с системой ДБО с компьютеров, не заслуживающих доверия (интернет-кафе) или с использованием общественных каналов связи (не подключайтесь к открытым сетям Wi-Fi без шифрования), т. к. это существенно увеличивает риск кражи Ваших персональных данных.

– Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте сотрудникам Банка обо всех подозрительных или несанкционированных операциях.

– Права пользователя, работающего с системой ДБО, на данном компьютере должны быть минимально необходимыми (наличие прав администратора нежелательно).

– Не привлекайте для администрирования и обслуживания компьютера с системой ДБО технических специалистов на условиях предоставления им удаленного доступа к компьютеру.

2. Соблюдение правил безопасности при работе с ключевыми носителями.

– Храните ключи только на съемном носителе. По возможности используйте съемные защищенные носители. Хранение ключевых носителей должно быть организовано в месте, недоступном для посторонних лиц. Установка ключевых носителей на рабочее место допускается только непосредственно на время работы с системой ДБО.

ВАЖНО! После окончания сеанса работы в системе ДБО съемный ключевой носитель должен быть незамедлительно извлечен из компьютера.

– Если Вы используете несколько ключей ЭП при работе в системе ДБО, не переносите эти ключи ЭП на один ключевой носитель, а также не подключайте одновременно различные ключевые носители к компьютеру. Банк не рекомендует изготовление дубликатов ключей.

– Для контроля доступа к съемному ключевому носителю рекомендуем установить на него пароль.

ВАЖНО! Пароль для доступа к съемному ключевому носителю должен быть известен только лицу, уполномоченному (допущенному) к работе с системой ДБО.

– Генерацию ключей ЭП осуществляйте лично с записью ключевой информации на съемный носитель. Не допускайте копирования сгенерированных ключей ЭП.

– После окончания работы в системе ДБО обязательно корректно завершите работу (выйдите из системы ДБО с использованием кнопки «Выход») и/или закройте приложение Internet Explorer.

ВАЖНО! Извлеките из компьютера съемный ключевой носитель.

– Производите замену ключей ЭП до истечения срока их действия. Кроме того, проводите замену ключей ЭП во всех случаях увольнения и/или смены лиц, имеющих доступ к системе ДБО, а также руководителей с правом подписи доверенностей на получение ключей ЭП, и в случае подозрений на их компрометацию.

3. Соблюдение правил безопасности при использовании средств доступа (логинов/паролей)

– Логины и пароли для работы в системе ДБО – это Ваша персональная конфиденциальная информация. Ни при каких обстоятельствах не раскрывайте свой логин и пароль никому, включая сотрудников Банка. При обращении от имени Банка по телефону, электронной почте, через SMS лиц с просьбами сообщить конфиденциальную информацию (пароли, кодовые слова, и т. д.) ни при каких обстоятельствах не сообщайте данную информацию.

– Не сохраняйте Ваш логин и пароль в текстовых файлах на компьютере либо на других электронных носителях информации, т.к. при этом существует риск его кражи и компрометации.

4. Выполнение правил безопасности при работе в системе ДБО

– В случае сбоев в работе компьютера или его поломки во время работы в системе ДБО или сразу после сеанса (проблемы с загрузкой операционной системы, выход из строя жесткого диска, и т. п.), НЕМЕДЛЕННО извлеките ключи ЭП и выключите компьютер, а также обратитесь в Банк и убедитесь, что от Вашего имени не производились несанкционированные операции (путём сверки операций за день).

– Обращайте внимание на любые изменения в привычных для Вас процессах установления соединения с системой ДБО или в ее функционировании. При возникновении любых сомнений в правильности функционирования системы ДБО НЕМЕДЛЕННО извлеките ключи ЭП и обратитесь в Банк.

– При работе с системой ДБО (сервис «Интернет-Клиент») убедитесь, что защищенное соединение по протоколу https установлено именно с официальным сайтом услуги (https://lk-dbo.autofinancebank.ru/f2b). Настоятельно не рекомендуем переходить на данную страницу по ссылке с Интернет-ресурсов (за исключением официального ресурса Банка https://autofinancebank.ru/) или поступивших по электронной почте писем.

– При появлении предупреждений браузера о перенаправлении Вас на другой сайт при подключении к системе ДБО Банка, отложите совершение операций и обратитесь в службу поддержки Банка.

– Рекомендуем осуществлять смену пароля доступа к системе ДБО не реже 1-го раза в 3 месяца.

– В случае утраты ключевого носителя, ключей от хранилища в момент нахождения в нем ключевого носителя, а также в случае возникновения ситуации, связанной с временным доступом посторонних лиц к ключевому носителю либо в связи с подозрением, что такой доступ имел место, незамедлительно обратитесь в Банк в связи с компрометацией ключа ЭП.

ВНИМАНИЕ!

Незамедлительное обращение в Банк с предоставлением полной информации о несанкционированном списании денежных средств со счетов может позволить оперативно приостановить транзакцию и предотвратить финансовые потери.