Памятка
Клиентам Банка ВТБ (ПАО) – Юридическим лицам по обеспечению информационной безопасности в системе дистанционного банковского обслуживания

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

Обеспечение безопасности компьютера, с использованием которого осуществляется работа в системе ДБО:

Установите и регулярно обновляйте лицензионное программное обеспечение, а также антивирусное программное обеспечение на Вашем компьютере. Действие вредоносных программ может быть направлено на перехват Вашей персональной информации и передачу её третьим лицам.
Своевременно устанавливайте обновления операционной системы своего компьютера, рекомендуемые компанией-производителем в целях устранения выявленных в нем уязвимостей. Регулярно выполняйте обновления (патчи) операционной системы и браузера Вашего компьютера, что значительно повысит его уровень безопасности.
Установите и настройте персональный брандмауэр (firewall) на Вашем компьютере. Это позволит Вам запретить 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 (https://i.vtb.ru) и системы Личный кабинет (https://dbo.vtb.ru https://tls.dbo.vtb.ru).
Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты Вашего компьютера – программы поиска шпионских компонент, программы защиты от «спам» - рассылок.
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 компьютеров 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 рекомендуется работать с системой ДБО с компьютеров, не заслуживающих доверия (интернет-кафе) или с использованием общественных каналов связи (бесплатный Wi-Fi и т.п.), 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.
На компьютере не рекомендуется устанавливать иное программное обеспечение, кроме необходимого для работы в системе ДБО. Рекомендуется использовать для работы с Банком выделенный компьютер.
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.

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 рекомендуется установить на него пароль.
ВАЖНО: Не сообщайте никому пароль для доступа к съемному ключевому носителю (включая сотрудников Банка и сотрудников Вашей организации или Ваших родственников)!
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.

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 следует сообщать 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.

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.), следует НЕМЕДЛЕННО извлечь ключи ЭП и выключить компьютер, а также обратиться в Банк и убедиться, 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 функционировании системы ДБО. При возникновении любых сомнений в правильности функционирования системы ДБО незамедлительно 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://i.vtb.ru/).
Настоятельно не рекомендуется переходить на данную страницу по ссылке с Интернет-ресурсов (за исключением официального ресурса Банка www.vtb.ru) или поступивших по электронной почте писем.
В случае появления предупреждений браузера о перенаправлении Вас на другой сайт при подключении к системе ДБО Банка, отложите совершение операций и обратитесь в службу поддержки Банка.
Банк рекомендует осуществлять смену пароля доступа к сервису «Мобильный Клиент» не реже 1 раза в 3 месяца.
В случае утраты ключевого носителя, утраты 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, необходимо незамедлительно обратиться 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.