İŞBANK ИШБАНК

О рисках работы с системой дистанционного банковского обслуживания

1. К основным рискам, связанным с применением систем дистанционного банковского обслуживания для юридических лиц, могут быть отнесены: операционный (прямые или косвенные финансовые потери и убытки), правовой и репутационный риски.

1.1. Причинами возникновения операционного риска при применении систем интернет-банкинга могут являться:

- **ВАЖНО!** несанкционированное списание или хищение денежных средств Клиента;
- неправомерный доступ к информационным ресурсам, в том числе при (для) совершении(я) преступных действий;
- умышленные или не умышленные ошибки персонала организации;
- ненадлежащее обеспечение уровня информационной безопасности в организации: отсутствие средств антивирусной защиты, межсетевых экранов, механизмов управления и контроля доступа;
- недостаточная производительность и защищенность информационных систем и информационно-телекоммуникационных сетей организации, так и провайдеров, задействованных в информационном контуре интернет-банкинга;
- аварии, отказы, сбои оборудования и программного обеспечения в самой организации или на стороне провайдеров;

1.2. Причинами возникновения правового риска при применении систем интернет-банкинга могут являться:

- **ВАЖНО!** нарушения условий договоров дистанционного банковского обслуживания.
- неправомерный доступ к конфиденциальной информации во время ее обработки, передачи или хранения как в самой организации, так и у провайдеров, с которыми кредитной организацией заключены договоры на обслуживание;

1.3. Причинами возникновения риска потери деловой репутации (репутационного риска) при применении систем интернет-банкинга могут являться:

- **ВАЖНО!** вовлечение организации в противоправную деятельность с применением систем интернет-банкинга;
- утечка из организации конфиденциальной информации, в том числе нарушение банковской и коммерческой тайн (из-за сетевых атак, неправомерного доступа к информационным ресурсам организации и т.п.);
- не исполнение или не своевременное исполнение организацией своих обязательств перед контрагентами.

2. В целях снижения вышеуказанных рисков и соблюдения требований к обеспечению информационной безопасности, установленных договором на дистанционное банковское обслуживание, АО «ИШБАНК» рекомендует клиентам:

2.1. При работе в Системе ДБО:

- **Ознакомится с правилами работы системы ДБО** и требованиями к обеспечению информационной безопасности;

- **Регулярно контролировать** состояние своих счетов и незамедлительно сообщайте сотрудникам Банка обо всех подозрительных или несанкционированных операциях.

- **Обращать 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.

2.2. При управлении доступом:

- **Назначить сотрудников** из числа работников организации, уполномоченных работать в Системе ДБО;

- **Предоставление минимальных прав доступа** пользователю, работающему с Системой ДБО;

- **Исключить удалённый доступ** для администрирования и обслуживания компьютеров с установленной Системой ДБО. В случае привлечения сотрудников сторонних организаций для выполнения административных функций, исключить их доступ к Системе ДБО, паролям и носителям ключей электронной подписи;

2.3. При работе с программным обеспечением:

- **Используйте только лицензионное программное обеспечение** (операционная система, офисные приложения и т.п.)**.**
  Своевременно устанавливать обновления операционной системы, рекомендуемые компанией-производителем в целях устранения выявленных в нем уязвимостей. Регулярно выполнять обновления операционной системы и браузера, так как данные действия значительно повысит его уровень безопасности;

- **Исключить установку постороннего программного обеспечения**, не относящегося к работе систем дистанционного банковского обслуживания, в том числе средств удаленного управления (R-Admin, TeamViewer или аналогичных систем), администрирования и модификации ОС и ее настроек (службы терминалов, удаленных рабочих столов и аналогичного программного обеспечения);

- **В случае сбоев** в работе компьютера или его выхода из строя во время/после работы с Системой ДБО (проблемы с загрузкой операционной системы, выход из строя жесткого диска, и т.п.), следует **НЕМЕДЛЕННО извлечь ключи Электронной подписи** и выключить компьютер, а также **обратиться в Банк и убедиться, что от Вашего имени не производились несанкционированные операции.**

2.4. При работе со средствами защиты информации:

- **Установить лицензионное средство защиты от вредоносного кода и межсетевой экран** (антивирусное программное обеспечение и firewall) на компьютеры, с которых осуществляется доступ к системам дистанционного банковского обслуживания;
  Регулярно осуществлять обновление баз данных антивируса и проверку на наличие инфицированных объектов.

В случае детектирования вредоносного программного обеспечения немедленно прекратить работу в системе ДБО, принять меры по устранению заражения компьютерным вирусом, а также сообщить об этом в банк по установленным в договоре каналам связи;

2.5. При работе в сети Интернет:

- **Ограничить доступ к сети Интернет** на компьютерах, используемых для работы в Системе ДБО и исключить посещение любых Интернет-сайтов (социальные сети, форумы, чаты, телефонные сервисы, личная почта и т.д.), кроме страницы входа в Систему ДБО. Перед началом работы в Системе ДБО закрывайте все открытые интернет-страницы. По окончанию работы с системой также следует закрыть окно интернет-браузера;

- **Исключить работу с Системой ДБО с использованием общедоступных каналов связи** (бесплатный Wi-Fi, Интернет-кафе и т.п.), так как это существенно увеличивает риск кражи Ваших конфиденциальных данных (логины, пароли и т.п.).

- **При работе с Системой ДБО убедитесь**, что защищенное соединение с официальным сайтом услуги ДБО (**https://dbo.isbank.com.ru/** или **https://ibank2.ru/**) установлено по протоколу **https**.
  Не переходите на данную страницу по ссылкам иных Интернет-ресурсов, кроме перехода по ссылкам официального ресурса Банка (**www.isbank.com.ru**);

- **Завершайте работу в Системе ДБО корректно.** Выйдите из Системы ДБО с использованием кнопки «Выход» и/или закройте Интерне-браузер;

2.6. При работе и хранении ключей электронной подписи:

- **Установка ключевых носителей** на рабочее место допускается только непосредственно на время работы с системой ДБО. После окончания сеанса работы в Системе ДБО съемный ключевой носитель должен быть незамедлительно извлечен из компьютера!

- **Хранить носители ключей электронной подписи (USB, MAC токены) в месте, недоступном для посторонних лиц**, и обеспечивающим их безопасность и надежную защиту от несанкционированного доступа (сейф, металлический запирающийся шкаф и т.д.).

- **Исключить хранение ключей электронной подписи на жёстких дисках** и иных незащищённых хранилищах;

- **Исключить несанкционированное копирование ключей** электронной подписи. Копирование ключевых носителей возможно только в целях создания резервных копий, при этом резервные носители должны храниться в недоступном для посторонних лиц месте и использоваться только в случае выхода из строя основного носителя;

- **Защита ключевых носителей сложным паролем.** Запрет передачи паролей посторонним лицам, в том числе сотрудникам банка.

2.7. При парольной защите:

- **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**.

- **Производить периодическую смену паролей доступа** к рабочему месту системы ДБО, а также в случае увольнения персонала, имевшего доступ к системе ДБО или при подозрении на компрометацию доступа к информационным системам;

- **Использовать сложные пароли** не менее 8 символов, состоящие из цифр, бук в верхнем и нижнем регистрах, спец. символов. Использовать при создании паролей парольные фразы. Не использовать в качестве паролей

имена, явки, фамилии, даты рождений, паспортные данные и т.п., связанные с владельцем ключа электронной подписи;

- **Не сохраняйте Ваш логин и пароль в письменном виде**, а также в текстовых файлах на жестком диске компьютера, либо на других электронных носителях информации, т.к. при этом существует риск его кражи и компрометации;

- **Не записывайте на носитель, содержащий секретные ключи ЭП**, какую-либо другую информацию. Не пишите на ключевом носителе свой логин и пароль для входа в Систему ДБО;