

ПАМЯТКА КЛИЕНТА

по обеспечению информационной безопасности при работе с системой "Клиент-Банк"

В последнее время в сети Интернет участились попытки неправомерного получения персональной информации пользователей системы дистанционного банковского обслуживания "Клиент-Банк": логинов, паролей, секретных ключей средств шифрования. Для реализации данных преступных посягательств всё чаще применяются специальные программные, технические или программно-технические средства, позволяющие удалённо, путём хакерских, вирусных или иных атак осуществить хищение персональной информации пользователей системы дистанционного банковского обслуживания "Клиент-Банк".

ЗАО КБ "Мираф-Банк" стремится предоставить своим клиентам удобный и безопасный способ управления своим счётом, поэтому, обращает Ваше внимание, на **НЕОБХОДИМОСТЬ** соблюдения следующих рекомендаций по обеспечению информационной безопасности при использовании системы "Клиент-Банк".

1. Рекомендации по обеспечению информационной безопасности компьютера, на котором установлена система "Клиент-Банк".

- для работы с системой "Клиент-Банк" используйте чистую лицензионную операционную систему;
- осуществляйте своевременную (по возможности, автоматическую) загрузку и установку всех последних обновлений операционной системы, а также регулярное обновление другого системного и прикладного программного обеспечения по мере появления новых версий (Интернет обозреватели - Explorer, Opera, Firefox и др., почтовые клиенты и т.п.);
- на компьютере, на котором установлена система "Клиент-Банк", должна быть установлена и регулярно обновляться программа антивирусной защиты (рекомендуется использовать антивирусные программы следующих производителей: Kaspersky, Dr.Web, Eset Nod32). Осуществляйте еженедельную полную антивирусную проверку компьютера. Антивирусное программное обеспечение должно быть запущено постоянно с момента загрузки компьютера;
- при работе в Интернет не соглашайтесь на установку каких-либо дополнительных программ с неизвестных Вам сайтов;
- не используйте компьютер, на котором развёрнута система "Клиент-Банк" для развлекательных целей (посещение Интернет ресурсов, не относящихся к системе "Клиент-Банк", воспроизведение мультимедиа файлов и т.п.);
- при работе с электронной почтой не открывайте письма и прикрепленные к ним файлы, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам;
- на компьютере, на котором установлена система "Клиент-Банк" рекомендуется использовать учётную запись с правами администратора, которая должна быть защищена паролем;
- по возможности применяйте специализированные программные средства безопасности:
 - персональные файерволы (Personal Firewall)
 - антишпионское программное обеспечение (Anti-Malware software) и другое специализированное ПО, используемое для обеспечения информационной безопасности

При настройке файервола разрешайте доступ только к доверенным ресурсам сети Интернет и только для доверенных приложений.

- не используйте компьютер с системой "Клиент-Банк" в публичных (проводных/беспроводных) сетях, предоставляющих доступ к сети Интернет, так как в таких сетях значительно повышается риск хищения и последующего

неправомерного использования персональной информации пользователей системы дистанционного банковского обслуживания "Клиент-Банк";

- рекомендуется ограничить список компьютеров и точек входа в сеть Интернет, с которых разрешена работа с системой "Клиент-Банк". Для этого необходимо заполнить [Заявление](#), в котором необходимо указать диапазон допустимых IP-адресов с которых производится вход в систему "Клиент-Банк" через сеть Интернет.

2. Рекомендации по обеспечению информационной безопасности при работе с системой "Клиент-Банк"

Электронная цифровая подпись (ЭЦП)- реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе (ст.3 Федерального закона №-258 "Об электронной цифровой подписи" от 08.11.2007). Поэтому ЭЦП является юридически значимым аналогом Вашей собственноручной подписи.

- не храните логин и пароль для доступа к системе "Клиент-Банк" на компьютере (в электронном виде) и там, где злоумышленник может их легко обнаружить вне компьютера;
- осуществляйте регулярную (минимум - 1 раз в месяц) смену паролей, используемых в системе "Клиент-Банк";
- не передавайте неуполномоченным лицам ключевые носители, логины и пароли доступа;
- в случае компрометации или подозрения на компрометацию следует немедленно произвести замену (перегенерацию) ключа ЭЦП и связаться со специалистами ЗАО КБ "Мираф-Банк". В качестве события, рассматриваемого как компрометация ключа, может выступать как потеря ключевого носителя (даже с последующим обнаружением), так и увольнение или смена лиц, допущенных к этим ключам;
- рекомендуется использовать для хранения ключей ЭЦП внешние носители (дискеты или флеш-накопители), а не жёсткие/сетевые диски компьютера. При этом необходимо хранить данный носитель в условиях, исключающих доступ к нему третьих лиц (например, использовать для хранения личный сейф);
- не используйте носители с ключами ЭЦП для каких-либо других целей (в частности, не храните на них любую другую информацию);
- извлекайте носители с ключами ЭЦП из компьютера каждый раз после завершения их использования (т.е. носители с ключами ЭЦП должны находиться в компьютере только в момент подписания) - даже если работа в системе "Клиент-Банк" продолжается, носители должны быть извлечены из компьютера сразу после окончания подписания документов;
- не оставляйте без присмотра работников сторонних организаций, которые производят сервисные работы на компьютере с установленной системой "Клиент-Банк".