



Приложение № 6
к Соглашению
по обслуживанию клиентов-юридических
лиц, индивидуальных предпринимателей и
физических лиц, занимающихся в
установленном законодательством РФ
порядке частной практикой, по системе
«Клиент-Банк»
№ _____ от _____ 20__ г.

ПАМЯТКА ПО БЕЗОПАСНОЙ РАБОТЕ В СИСТЕМЕ "КЛИЕНТ-БАНК"

Уважаемые Клиенты!

«Хакерские» атаки на системы "Клиент-Банк", приводящие к хищениям денежных средств клиентов банков в РФ фиксируются все чаще и чаще.

При этом "хакерами" взламываются не серверы банков, а похищаются клиентские ключи подписи и пароли доступа, как путем прямого доступа, так и с помощью вредоносных программ. Завладев ключами и паролями, злоумышленники осуществляют платежи от имени клиентов.

Поэтому очень важны меры безопасности при работе в системе «Клиент-Банк».

1. Выделите отдельный компьютер, подключаемый к сети Интернет только для работы с системой «Клиент-Банк».

Максимально ограничьте к нему доступ сотрудников. Запретите сотрудникам использовать на этом компьютере какие-либо съемные устройства, за исключением ключевых носителей.

Установленное программное обеспечение должно быть лицензированным и регулярно обновляться.

Установите на этот компьютер антивирусную программу и поддерживайте ее актуальность.

По возможности ограничьте (наши специалисты помогут вам в этом) количество ваших ip-адресов с которых разрешён доступ в систему "Клиент-Банк".

2. Необходимо обеспечить хранение ключей электронной подписи и пароля доступа к системе «Клиент-Банк» в тайне и только уполномоченными сотрудниками.

Ключ электронной подписи храните только на съёмном носителе.

Пароль доступа в систему желательно помнить и вводить вручную. Ни в коем случае не используйте функцию "запомнить пароль". Пароль, записанный на листе бумаги, обязательно храните отдельно от ключевого носителя.

Меняйте пароль доступа не реже одного раза в 3 месяца, и обязательно при компрометации или смене ключей подписи.

3. Не используйте для работы с системой "Клиент-Банк" общедоступные или чужие компьютеры.

4. Для хранения сгенерированных секретных ключей ЭЦП и формирования ЭЦП под документами используется USB-ключ «MS_key».

При использовании этого устройства секретный ключ электронно-цифровой подписи формируется в защищенной области памяти, встроенной в USB-ключ. В отличие от других носителей, с USB-ключа невозможно извлечь, считать или скопировать информацию ни при каких обстоятельствах. USB-ключ – неуязвим в отношении хакерских атак, которые нацелены на похищение секретных ключей не только со съемных носителей, но и из памяти компьютера. USB-ключ может содержать в себе до 64 секретных ключей! Соблюдение перечисленных мер позволяет Вам существенно снизить риски, связанные с использованием систем "Клиент-Банк" и предотвратить хищение денежных средств.

Если у Вас появились подозрения, что Ваши данные (электронные ключи, пароли) могли быть скомпрометированы, свяжитесь со службой тех. поддержки Банка - (495) 363-91-62, доб.153