

Памятка по информационной безопасности при работе с системой "Клиент-Банк" и хранении ключей на отчуждаемом (съемном) носителе.

Уважаемые клиенты.

В целях повышения безопасности работы с системой "Клиент-Банк" и для снижения угроз компрометации секретного ключа ЭЦП, хранящегося на съемном носителе, необходимо соблюдать следующие меры предосторожности:

Храните клиентский модуль (программу) и ключи на разных носителях. Программу можно скопировать и запускать с жесткого диска компьютера, но мы рекомендуем программу хранить и запускать на отключаемом носителе, отдельном от ключевого носителя.

НЕМЕДЛЕННО ИЗВЛЕКАЙТЕ носитель с ключами ЭЦП из персонального компьютера после завершения сеанса работы с системой.

Используйте и регулярно обновляйте антивирусное ПО, персональные файрволлы, средства защиты от несанкционированного доступа и т.п. Проводите полное сканирование компьютера на наличие вирусов на регулярной основе и при смене персонала, имевшего доступ к нему.

Не устанавливайте на компьютере, используемом для работы в системе, средства удаленного управления компьютером.

Соблюдайте правила информационной безопасности при работе в Интернете – не посещайте подозрительные сайты, не устанавливайте программы из недоверенных источников, не открывайте файлы от неизвестных отправителей и пр.

Используйте системное и прикладное ПО, полученное из источников, гарантирующих отсутствие вредоносных программ.

Ограничьте физический доступ к компьютерам, используемым для работы с системой "Клиент-Банк".

Не передавайте носитель с секретными ключами сотрудникам или иным лицам, не имеющим доступ к работе с системой. Храните в тайне пароли ЭЦП.

При увольнении ответственного сотрудника, имевшего доступ к секретному ключу ЭЦП, обязательно позвоните в Банк для временной блокировки системы и перевыпуска ключей.

Если у Вас возникли подозрения, что доступ к компьютеру или носителю с ключом могли получить неуполномоченные лица, а также при возникновении нештатных ситуаций, таких как зависание операционной системы, выход из строя жесткого диска или различные другие нарушения работоспособности компьютера, немедленно позвоните в Банк для блокировки доступа в систему.