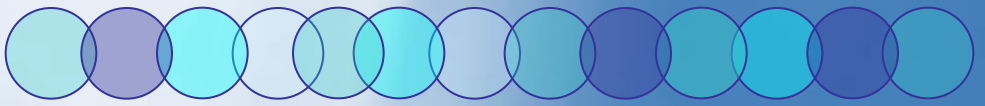
БЕЗОПАСНОСТЬ
ИНИСТ БАНК-КЛИЕНТ

ИНИСТ Банк-Клиент

Введение



- Основным назначением системы «ИНИСТ Банк-Клиент» является предоставление клиентам банков возможности удаленного управления своими счетами.
- Взаимодействие между клиентской и банковской частями осуществляется посредством каналов связи.
- Система гарантирует целостность доставляемых данных и безопасность их передачи.

ИНИСТ Банк-Клиент

Безопасность

- Клиент банка может использовать любой компьютер и соединяться с банком по модему через коммутируемый канал или выделенную линию. Также возможно прямое IP-соединение через сеть.
- Работа с программой **не зависит** от типа соединения.
- Безопасность передачи информации и целостность доставляемых данных обеспечивается использованием современных разработок:

  - Защищенное SSL-соединение
  - Электронный аналог собственной подписи
  - Генератор одноразовых паролей
  - Виртуальная клавиатура

ИНИСТ Банк-Клиент

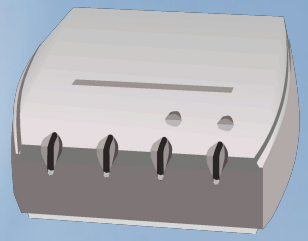
Электронный аналог собственной подписи

- Каждый раз при передаче данных между клиентом и банком в Системе осуществляется проверка электронных подписей (АСП).
- Криптосервер реализует функции подписания пакетов АСП банка и проверки подписей АСП клиентов. Проверка осуществляется на основании справочника открытых ключей клиентов.
- Проверке подвергаются все подписанные клиентскими ключами данные, а подписанию – все данные, отправляемые банком. Подписание данных осуществляется закрытым ключом банка.
- Такой подход гарантирует целостность и достоверность передаваемых в Системе данных.

ИНИСТ Банк-Клиент

Криптосервер

- Система предоставляет возможность использования как одного, там и нескольких криптосерверов, реализующих криптоалгоритмы и криптографические API, разработанные сторонними производителями.
- Криптосервер представляет собой сервер приложений, работающий в стандарте CORBA по протоколу TCP/IP.
- На сегодняшний день осуществлена поддержка следующих сертифицированных ФСБ криптосистем :
  - КриптоПро
  - СигналКом
  - Криптоком
  - СКЗИ Верба
  - Крипто-Си
  - ПКЗИ ММВБ
  - Агава



ИНИСТ Банк-Клиент

Ключевая регистрация

- Регистрация в Системе ИНИСТ Банк-Клиент происходит на основании электронного ключа клиента.
- В качестве носителей ключевой информации могут быть использованы оптические диски, жесткий диск, различные USB-накопители.
- Электронный ключ дополнительно защищен паролем и имеет ограниченный срок действия.
- Безопасность регистрации обеспечивается за счет того, что при каждом входе в Систему клиент должен ввести не только логин, но и электронный ключ, а также пароль для доступа к нему.
- Достоверность и целостность передаваемых данных гарантируется тем, что каждый пересылаемый документ подписывается электронным ключом, а каждый полученный – проверяется.

ИНИСТ Банк-Клиент

Одноразовые пароли

- В качестве альтернативы ключевой регистрации в Системе существует возможность использования одноразовых паролей.
- Это особенно удобно для клиентов – физических лиц, которые могут испытывать трудности с генерацией ключей.
- Безопасность подключения в этом случае гарантируется тем, что каждый раз при входе в Систему клиент вводит новый пароль, что исключает возможность использования его злоумышленниками.

ИНИСТ Банк-Клиент

Генератор одноразовых паролей

- Для генерации одноразовых паролей в Системе предлагается возможность использования специального программно-аппаратного обеспечения Vasko Didipass.
- В этом случае клиент освобождается от необходимости регулярных визитов в банк для получения очередной серии паролей. Все, что нужно для регистрации в Системе и подписания документов, предоставляет соответствующее устройство – генератор одноразовых паролей.
- Таким образом, компрометация ключевой информации становится еще более затруднительной.

ИНИСТ Банк-Клиент

Виртуальная клавиатура

- Помимо прочих систем защиты информации Системой ИНИСТ Банк-Клиент предоставляется возможность использования виртуальной клавиатуры для ввода данных вручную.
- Виртуальная клавиатура позволяет обеспечить еще более высокий уровень защиты конфиденциальной информации клиентов.
- Данная технология повышает степень защищенности пароля, а также любых других введенных клиентом данных от перехвата злоумышленниками.

ИНИСТ Банк-Клиент

Дополнительные средства обеспечения безопасности

- SMS-информирование клиента о каждом случае регистрации в Системе с его ключами.
- Возможность самостоятельного осуществления клиентом добровольной блокировки – запрета на использование электронного ключа.
- Ограничение списка IP-адресов, с которых разрешено осуществлять регистрацию в Системе.
- Использование для хранения ключей USB-устройства eToken - персонального средства аутентификации и хранения данных. Для доступа к ключу клиент должен дополнительно вводить пин-код.