



ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
“САЙФЕР”

Адрес: 04107, Киев, ул. Нагорная, 25
Тел./Факс: (044) 246-99-00, 246-98-35
E-mail: sales@cipher.kiev.ua
<http://www.cipher.kiev.ua>

**Комплекс «Шифр-К»
Программные средства защиты для систем «Клиент-банк»**

Краткая характеристика

Комплекс предназначен для защиты от навязывания ложных сообщений, защиты электронных документов от преднамеренных и непреднамеренных искажений, скрывания смыслового содержания и авторизации (цифровой подписи) электронных документов, обрабатываемых в системах «Клиент-банк».

Комплекс средств защиты функционально состоит из следующих подсистем:

- подсистемы криптографической защиты;
- подсистемы управления средствами защиты информации;

Подсистема криптографической защиты предназначена для криптографического преобразования конфиденциальных электронных документов с целью скрывания их содержания, обеспечения проверки подлинности и целостности, обеспечения юридической ответственности за сформированные электронные документы, а также для шифрования ключевых данных при их автоматизированной доставке по открытым каналам связи участникам конфиденциального электронного документооборота.

Основными функциями подсистемы криптографической защиты информации являются:

аутентификация (установление подлинности) пользователей, технических средств, процессов и сообщений, участвующих в обмене электронными документами;

криптографическое преобразование информации, передаваемой по каналам и линиям связи или хранимой на запоминающих устройствах;

авторизация электронных документов (формирование цифровой подписи с целью обеспечения юридической ответственности за сформированные электронные документы, предотвращения их модификации и подделки, а также обеспечения возможности разрешения спорных ситуаций).

Программные средства подсистемы реализуют два уровня защиты конфиденциальной информации.

Основой первого уровня защиты является цифровая подпись электронного документа. Цифровая подпись реализована на основе криптографических алгоритмов преобразования данных, утвержденных ГОСТ 34310-95, ГОСТ 34311-95. Первый уровень защиты обеспечивает проверку целостности и подлинности электронного документа, строгую аутентификацию отправителя документа, обеспечивает персональную (юридическую) ответственность за сформированный электронный документ.

Второй уровень защиты предназначен для обеспечения целостности и скрывания смыслового содержания подписанного цифровой подписью электронного документа, а также ключевых

данных при их передаче по открытым каналам связи. Эта задача решается путем формирования и включения в состав передаваемого документа (ключевых данных) его кода аутентификации и последующего шифрования полученного таким образом сообщения. Формирование кода аутентификации (имитовставки) и шифрование выполняется по алгоритму, утвержденному ГОСТ 28147-89.

Средства банковской части подсистемы криптографической защиты обеспечивают ведение архивов подписанных электронных документов. Наличие таких архивов необходимо для обеспечения возможности разрешения третейских и/или арбитражных споров, которые могут возникнуть между участниками электронного документооборота.

Подсистема управления средствами защиты информации обеспечивает управление ключами цифровой подписи на первом уровне защиты, и симметричными шифрключами на втором. Кроме того, средства этой подсистемы позволяют конфигурировать средства защиты информации, обеспечивают защиту и контроль целостности ключевых данных, хранимых на носителях, обеспечивают работу с архивами отправленных и принятых электронных документов, протоколируют действия администратора по управлению криптографическими ключами.

Технически комплекс средств защиты информации для систем «Клиент-банк» реализованы в виде двух взаимосвязанных частей программных средств:

программные средства защиты информации для банковской части системы «Клиент-банк»;
программные средства защиты информации для АРМ «Клиент банка».

В каждой из перечисленных частей комплекса реализуются функции подсистемы криптографической защиты и подсистемы управления средствами защиты информации.

В программные средства защиты информации для банковской части системы «Клиент-банк» входят:

- библиотеки функций криптографических преобразований (программное изделие «Шифр»);
- библиотеки инициализации процедур постановки\проверки цифровой подписи исполнителей банка;
- библиотеки инициализации процедур постановки\проверки цифровой подписи банка и шифрования файлов;
- программное обеспечение АРМ администратора системы защиты информации;
- библиотеки поддержки работы с "Touch Memory".

В программные средства защиты информации для АРМ «Клиент банка» входят:

- библиотеки функций криптографических преобразований (программное изделие «Шифр»);
- библиотеки инициализации процедур постановки\проверки цифровой подписи должностных лиц клиента (директора, бухгалтера);
- библиотека инициализации процедур шифрования файлов;
- библиотеки инициализации процедур управления ключами;
- библиотеки интерактивных средств пользователя;
- библиотеки поддержки работы с "Touch Memory".

Сертификаты

Библиотеки функций криптографических преобразований (программное изделие «Шифр»), являющиеся основой подсистемы криптографической защиты комплекса, Сертифицированы Органом сертификации средств защиты информации ДСТСЗИ СБ Украины. **Сертификат № UA-1.112.14243-01, выдан 15.06.2001г. Государственным комитетом Украины по стандартизации, метрологии и сертификации.**

Технология функционирования комплекса средств защиты одобрена НБУ в процессе сертификации системы клиент-банк «Стиль», **сертификат SEPК № 0019 от 12.02.1997г.**