



ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО  
“САЙФЕР”

Адрес: 04053, г.Киев, пер. Бехтеревский, д. 4-б  
Тел/Факс: (044) 246-99-00, 246-98-35  
E-mail: [tk@cipher.kiev.ua](mailto:tk@cipher.kiev.ua)  
<http://www.cipher.kiev.ua>

---

## Программное изделие «Шифр»

### Библиотеки функций криптографических преобразований

#### *Легитимность*

*Реализация программного изделия «Шифр» соответствует требованиям ГОСТ 28147-89, ГОСТ 34.310-95, ГОСТ 34.311-95, а также технического задания UA. 23154898.00001-01 90 01, согласованного с ДСТСЗИ СБ Украины, что подтверждается сертификатом соответствия № UA-1.112.14243-01 от 15.06.2001г., выданным Государственным комитетом Украины по стандартизации, метрологии и сертификации.*

#### *Краткое описание*

Программное изделие «Шифр» (библиотеки функций криптографических преобразований), является средством криптографической защиты информации и предназначено для использования в программных, программно-аппаратных средствах (комплексах) для:

- сокрытия смыслового содержания обрабатываемых данных,
- защиты от навязывания ложной информации,
- формирования и распределения (управления) ключевыми данными, которые используются в средствах КЗИ, независимо от вида носителя ключевой информации,
- защиты информации от несанкционированного доступа с использованием криптографических алгоритмов.

Функции, входящие в состав библиотек реализуют:

- зашифрование/расшифрование и выработку имитовставки по алгоритмам согласно ГОСТ 28147-89;
- выработку/проверку цифровой подписи по алгоритму согласно ГОСТ 34.310-95;
- генерацию параметров цифровой подписи по алгоритму согласно ГОСТ 34.310-95;
- генерацию секретных и открытых ключей цифровой подписи по алгоритму согласно ГОСТ 34.310-95;
- вычисление хэш-функции данных по алгоритму согласно ГОСТ 34.311-95;
- выработку ключей шифрования по методу Диффи-Хеллмана;
- генерацию параметров для распределения ключей по методу Диффи-Хеллмана;
- генерацию секретных и открытых ключей для формирования ключей шифрования по методу Диффи-Хеллмана;
- генерацию псевдослучайной последовательности;
- самоконтроль (при инициализации) криптографических функций на правильность функционирования;
- самоконтроль (при инициализации) генератора псевдослучайной последовательности – на удовлетворение генерируемой последовательности требованиям, описанным в стандарте FIPS 140-1.

### **Комплект поставки**

В комплект поставки программного изделия «Шифр» входят:

- динамическая библиотека функций криптографических преобразований (DLL для языка программирования C\C++);
- статическая библиотеки функций криптографических преобразований(LIB для языка программирования Visual C++ 6.0);
- библиотеки функций криптографических преобразований в виде пакета JAVA – классов;
- техническая документация (спецификация, описание, руководство программиста).

### **Технические характеристики**

Процедуры, которые входят в состав библиотек, обеспечивают при работе на компьютере IBM PC с процессором типа Intel Celeron 300A и тактовой частотой 450 МГц показатели не хуже, указанных ниже.

<b>Характеристика</b>	<b>Показатель</b>
Скорость формирования имитовставки и зашифрования данных, не менее	6,8 Мбит/сек
Скорость расшифрования данных и контроль их целостности на основе проверки имитовставки, не менее	6,8 Мбит/сек
Скорость выработки хеш-функции (ГОСТ 34311-95), не менее	0.98 Мбит/сек
Время выполнения процедуры формирования цифровой подписи (длина ключа 512 бит), не более	0.0052 сек.
Время выполнения процедуры проверки цифровой подписи (длина ключа 512 бит), не более	0.0081 сек.
Время выполнения процедуры генерации ключей (секретного и открытого) протокола Диффи-Хеллмана (длина ключа 512 бит), не более	0.098 сек.
Время формирования ключа шифрования (длина ключа 512 бит) по методу Диффи-Хеллмана на основе своего секретного ключа и открытого ключа корреспондента, не более	0.13 сек.

Библиотеки криптографических преобразований, входящие в состав программного изделия «Шифр», могут применяться в программных, программно-аппаратных средствах и комплексах, написанных на языках программирования C (C++) и Java.

### **Требования к программному и аппаратному обеспечению**

Библиотеки криптографических преобразований, входящие в состав программного изделия «Шифр» устойчиво функционируют на компьютерах с INTEL-PENTIUM совместимым процессором в операционных системах WINDOWS 95\98, NT, 2000, а также во всех операционных системах, которые поддерживают технологию JAVA.

### **Условия поставки, стоимость**

Программное изделие «Шифр» поставляется с **неограниченной по времени лицензией, предоставляющей покупателю право тиражирования библиотек** для использования без права или с правом передачи третьим лицам только в составе другого программного обеспечения.

Цена договорная и определяется исходя из потенциальных потребностей Заказчика по тиражированию.