

127 018, Москва, Сущевский вал, д.16/5  
Телефон: (495) 780 4820  
Факс: 4095) 780 4820  
<http://www.CryptoPro.ru>  
E-mail: [info@CryptoPro.ru](mailto:info@CryptoPro.ru)



Средство Криптографической Защиты Информации	КриптоПро CSP Версия 3.6 АРМ выработки внешней гаммы
---	---

ЖТЯИ.00050-02 90 04  
Листов 5

## Аннотация

Настоящий документ определяет требования к АРМ и порядок изготовления внешней гаммы, используемой в качестве исходного материала для инициализации программного датчика случайных чисел в СКЗИ "КриптоПро CSP" версии 3.6 (СКЗИ ЖТЯИ.00050-2) в составе серверов на аппаратно-программных платформах, для которых в настоящее время не существует ПАК защиты от НСД или электронного замка с физическим датчиком случайных чисел.

## Содержание

1. Требования к внешней гамме .....	4
2. Требования к АРМ выработки внешней гаммы .....	4
3. Порядок изготовления носителей с внешней гаммой .....	5
4. Использование внешней гаммы в СКЗИ .....	5
5. Требование по безопасности .....	5

## 1. Требования к внешней гамме

К внешней гамме, используемой в качестве исходного материала для инициализации программного датчика случайных чисел (ПДСЧ) в СКЗИ ЖТЯИ.00050-02, предъявляются следующие требования:

1. Внешняя гамма является **конфиденциальной**.
2. Гамма представляется отрезками равновероятной случайной бинарной последовательности размера 256 бит (32 байта).
3. Гамма на носителях (отчуждаемый носитель, ЖМД ПЭВМ) представляется в формате файла, содержащего заданное количество отрезков с защитным кодом CRC (4 байта) каждого отрезка.
4. Для повышения надежности записи/считывания гаммы с носителя файл с гаммой дублируется на носителе в двух директориях.
5. Носитель гаммы должен допускать последовательное считывание очередного отрезка с его защитным кодом с конца файла и перемещением конца файла (EOF) на 36 байтов.

## 2. Требования к АРМ выработки внешней гаммы

Выработка внешней гаммы и запись ее на отчуждаемые носители производится на автономном АРМ, функционирующем в программно-аппаратной среде Windows XP (платформа IA32).

На АРМ устанавливаются:

1. СКЗИ ЖТЯИ.00050-02 в исполнениях 2 (уровень защиты КС2), 3-5 (уровень защиты КС2 с электронным замком "Соболь". В настройке СКЗИ "**Свойства КриптоПро CSP/оборудование/датчики случайных чисел**" должен быть оставлен только "Соболь".
2. Утилита **genkpm** выработки внешней гаммы;
3. Устройства вывода внешней гаммы на требуемые типы отчуждаемых носителей, разрешенных к использованию в СКЗИ ЖТЯИ.00050-02.

АРМ функционирует по схеме:



### 3. Порядок изготовления носителей с внешней гаммой

Изготовление внешней гаммы на АРМ обеспечивается утилитой **genkpm**.

Для изготовления внешней гаммы с командной строки производится запуск утилиты **genkpm**:

**genkpm.exe y n <p>**

Здесь **y** - необходимое количество случайных отрезков гаммы для записи на носитель, **p** - путь, по которому записаны директории DB1 и DB2 (если путь не указан, то по умолчанию идет обращение к диску а:), **n** - номер комплекта внешней гаммы (8 символов в 16-ричном коде).

В результате выполнения команды генерируется заданный объем материала внешней гаммы и формируется файл **kis\_1**, содержащий **y** отрезков гаммы по 36 байтов (32 байта -отрезок гаммы, 4 байта - код CRC отрезка гаммы).

Файл **kis\_1** по пути **p** дублированием в две директории: DB1 и DB2 записывается на носитель внешней гаммы.

### 4. Использование внешней гаммы в СКЗИ

Внешняя гамма используется в качестве исходного материала для инициализации ПДСЧ в СКЗИ в составе серверов на аппаратно-программных платформах, для которых в настоящее время не существует ПАК защиты от НСД или электронного замка с физическим ДСЧ.

Для использования внешней гаммы в СКЗИ директории DB1 и DB2 с файлом **kis\_1** записываются с отчуждаемого носителя внешней гаммы на жесткий диск сервера.

Для переинициализации состояния ПДСЧ, производимой при каждом создании ключевого контейнера и при генерации каждого закрытого пользовательского ключа, используется очередной отрезок гаммы от конца файлов **kis\_1** в директориях DB1 и DB2 на жестком диске.

Бесповторное использование отрезков гаммы и их отбраковка проверкой кода CRC в процессе функционирования сервера обеспечивается средствами СКЗИ. Дублируемые в директориях DB1 и DB2 отрезки гаммы в случае их несовпадения игнорируются.

### 5. Требование по безопасности

При эксплуатации АРМ выработки внешней гаммы и использовании отчуждаемых носителей внешней гаммы должны выполняться требования:

1. АРМ выработки внешней гаммы размещается в одной контролируемой зоне с сервером, в котором внешняя гамма используется.

2. Изготовление носителей с внешней гаммой осуществляется только администратором сервера или заменяющим его лицом, допущенным к ключам сервера.

3. На носители с записанной на них внешней гаммой распространяются требования по обращению с ними как с ключевыми документами.

4. После записи внешней гаммы с отчуждаемого носителя на жесткий диск сервера отчуждаемый носитель должен быть переформатирован с физическим уничтожением всех данных.

5. Должны соблюдаться требования эксплуатационной документации на СКЗИ, Формуляр ЖТЯИ.00050-02 30 01.