

127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
<https://CryptoPro.ru>
E-mail: info@CryptoPro.ru



Средство

Криптографической

Защиты

Информации

КриптоПро CSP

Версия 5.0 KC1

1-Base

APM выработки внешней гаммы

ЖТЯИ.00101-01 94 01
Листов 6

© ООО «КРИПТО-ПРО», 2000-2019. Все права защищены.

Авторские права на средство криптографической защиты информации КриптоПро CSP и эксплуатационную документацию к нему зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент).

Документ входит в комплект поставки программного обеспечения СКЗИ КриптоПро CSP версии 5.0 КС1; на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО «КРИПТО-ПРО» документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

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 Требования по безопасности 6

Аннотация

Настоящий документ определяет требования к АРМ и порядок изготовления внешней гаммы, используемой в качестве исходного материала для инициализации программного датчика случайных чисел (ДСЧ) в СКЗИ КриптоПро CSP версия 5.0 KC1 Исполнения 1-Base в составе серверов на аппаратно-программных платформах, для которых в настоящее время не существует поддерживаемых физических ДСЧ.

1 Требования к внешней гамме

К внешней гамме, используемой в качестве исходного материала для инициализации программного датчика случайных чисел (ПДСЧ) в СКЗИ КриптоПро CSP, 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 контрольной суммой (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 следующих программно-аппаратных средах:

- Windows 7/8.1/10/Server 2003/2008 (x86, x64);
- Windows Server 2008 R2/2012/2012 R2/2016 (x64).

На АРМ устанавливаются:

- 1) СКЗИ «КриптоПро CSP» с электронным замком «Соболь». В настройке СКЗИ «Свойства КриптоПро CSP/оборудование/датчики случайных чисел» должен быть оставлен только «Соболь».
- 2) Утилита genkrip выработки внешней гаммы;
- 3) Устройства вывода внешней гаммы на требуемые типы отчуждаемых носителей, разрешенных к использованию в СКЗИ «КриптоПро CSP».

АРМ функционирует по схеме (см. [Рисунок 1](#)):

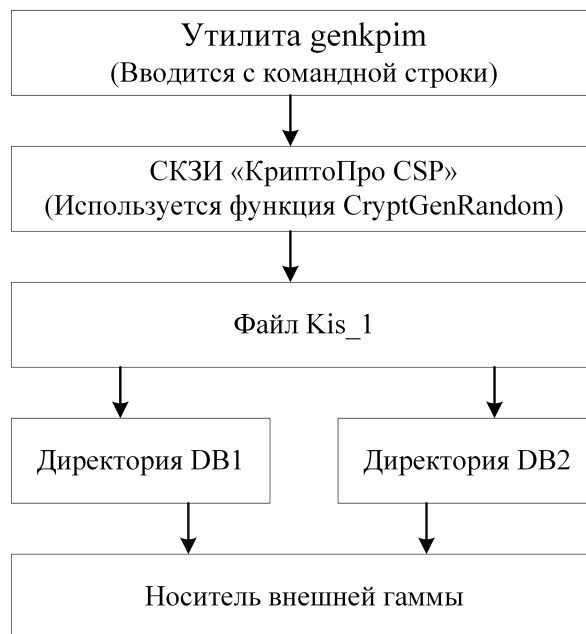


Рисунок 1. Схема функционирования АРМ выработки внешней гаммы

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 `a:`),
`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 — контрольная сумма 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 два очередных отрезка гаммы от конца файлов `kis_1` в директориях `DB1` и `DB2` на жестком диске.

Бесповторное использование отрезков гаммы и их отбраковка проверкой контрольной суммы в процессе функционирования сервера обеспечивается средствами СКЗИ. Дублируемые в директориях `DB1` и `DB2` отрезки гаммы

в случае их несовпадения игнорируются.

5 Требования 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 (п.6.7 ЖТЯИ.00101-01 91 01. Руководство администратора безопасности. Общая часть).
- 4) После записи внешней гаммы с отчуждаемого носителя на жесткий диск сервера отчуждаемый носитель должен быть переформатирован с физическим уничтожением всех данных или уничтожен.
- 5) Должны соблюдаться требования эксплуатационной документации на СКЗИ, в частности, требования формуляра ЖТЯИ.00101-01 30 01.