

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



Средство

Криптографической

Защиты

Информации

КриптоПро CSP

Версия 5.0 R3 KC1

(исполнение 1-Base)

APM выработки внешней гаммы

ЖТЯИ.00101-03 94 01
Листов 6

© ООО «КРИПТО-ПРО», 2000-2024. 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 R3 KC1; 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 Технические требования к АРМ 4

3 Порядок изготовления носителей с внешней гаммой 5

4 Использование внешней гаммы в СКЗИ 6

5 Требования по обеспечению безопасности 6

Аннотация

Настоящий документ определяет требования к АРМ выработки внешней гаммы (далее — АРМ) и порядок изготовления внешней гаммы (далее — гаммы), используемой в качестве исходного материала для инициализации программного датчика случайных чисел (далее — ПДСЧ) в СКЗИ КриптоПро CSP в составе серверов.

1 Требования к внешней гамме

Внешняя гамма, используемая в качестве исходного материала для инициализации ПДСЧ в СКЗИ КриптоПро CSP, и носитель гаммы должны удовлетворять следующим требованиям:

- 1) Внешняя гамма является **конфиденциальной**.
- 2) Гамма представляется отрезками равновероятной случайной бинарной последовательности размера 256 бит (32 байта).
- 3) Гамма на ключевых носителях (съёмные носители, раздел HDD/SSD 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 Технические требования к АРМ

Выработка внешней гаммы и запись ее на отчуждаемые носители производится на автономном АРМ, функционирующем в программно-аппаратных средах, перечисленных в п. 3.2 документа ЖТЯИ.00101-03 30 01. Формуляр (за исключением мобильных ОС).

На АРМ должны быть установлены:

- 1) СКЗИ КриптоПро CSP с установленным ДСЧ.



Примечание. Класс защиты СКЗИ КриптоПро CSP, установленного на АРМ, должен быть не ниже класса защиты СКЗИ, используемого на сервере, для которого генерируется внешняя гамма.



Примечание. Для просмотра списка настроенных ДСЧ и их приоритета:

- ОС Windows — откройте Панель управления КриптоПро CSP, вкладка **Оборудование**, кнопка «Настроить ДСЧ»;
- ОС Linux/Unix, Mac OS — выполните команду: `# ./cpconfig -hardware rndm -view`

- 2) Утилита командной строки `genkprim`;

- 3) Устройства вывода внешней гаммы на требуемые типы съёмных носителей, разрешенных к использованию в СКЗИ КриптоПро CSP.

3 Порядок изготовления носителей с внешней гаммой

Изготовление внешней гаммы на АРМ обеспечивается утилитой командной строки **genkpim**.

Утилита входит в состав дистрибутива СКЗИ КриптоПро CSP и после установки расположена в папке:

- ОС Windows — C:\Program Files (x86)\Crypto Pro\CSP
- ОС Linux/Unix — /opt/cproscsp/bin/<название_архитектуры>
- ОС Mac OS — /opt/cproscsp/bin

```
genkpim <number> <id_hex> [<path>]
```

number необходимое количество отрезков гаммы для записи на носитель

path путь, по которому будут созданы папки db1 и db2 (по умолчанию a:/)

id_hex номер комплекта внешней гаммы (8 hex-символов)

В результате выполнения команды генерируется заданный объем материала внешней гаммы и формируется файл **kis_1**, содержащий <number> отрезков гаммы по 36 байтов (32 байта — отрезок гаммы, 4 байта — контрольная сумма отрезка гаммы).

Файл **kis_1** записывается на носитель внешней гаммы в два каталога: <path>\db1 и <path>\db2.

Схема функционирования АРМ представлена на [Рисунок 1](#):

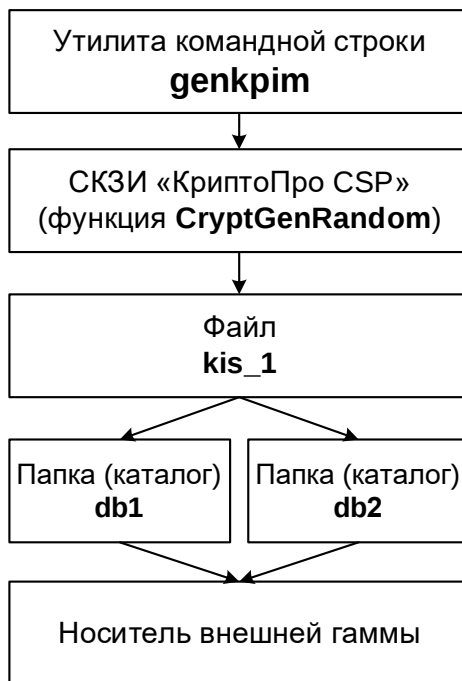


Рисунок 1. Схема функционирования АРМ выработки внешней гаммы

4 Использование внешней гаммы в СКЗИ

Внешняя гамма используется в качестве исходного материала для инициализации ПДСЧ в СКЗИ.

Для использования внешней гаммы в СКЗИ каталоги db1 и db2 с файлом kis_1 записываются с отчуждаемого носителя внешней гаммы на HDD/SSD сервера.

Для переинициализации состояния ПДСЧ, производимой при каждом создании ключевого контейнера и при генерации каждого закрытого пользовательского ключа, используются два очередных отрезка гаммы от конца файлов kis_1 в каталогах db1 и db2 на HDD/SSD сервера.

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 обеспечению безопасности

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

1) АРМ выработки внешней гаммы размещается в контролируемой зоне. Передачу гаммы между АРМ и сервером, размещенных в разных контролируемых зонах, необходимо обеспечить либо по криптографически защищенному каналу связи (в случае передачи по сети), либо доверенным образом (в случае передачи ключевого носителя с записанной на нем внешней гаммой).

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. 3.7 документа ЖТЯИ.00101-03 95 01. Правила пользования).

4) После записи внешней гаммы со съемного носителя на жесткий диск сервера носитель должен быть переформатирован с физическим уничтожением всех данных или уничтожен.