ООО Фирма «ИнфоКрипт»

АРМ управления бэкапированием
Инструкция по установке и эксплуатации

11485466.72.21.12.132 91

2025

Содержание

Введение

Настоящий документ содержит инструкцию по эксплуатации программы удалённого копирования ключей версии 2.0 (далее «АРМ управления бэкапированием»). Руководство включает в себя справочную информацию о программе и описывает конкретные действия, которые можно выполнять с помощью программы.

1 Назначение и условия применения

1.1 Назначение программы

Программа «АРМ управления бэкапированием» предназначена для безопасной передачи конфигурации секретных ключей (набора всех ключей) от программного изделия «Сервер бэкапирования. Источник» (далее сервер-источник) программному изделию «Сервер бэкапирования. Получатель» (далее «сервер-получатель»). Сервер-источник и сервер-получатель имеют созданный заранее «общий секрет» – ключевую пару. Закрытый ключ из «общего секрета» называется мастер-ключ.

«АРМ управления бэкапированием» используется преимущественно в пакетном режиме. Для реализации процедуры передачи конфигурации секретных ключей пользователю необходимо подготовить BAT-файл с набором команд.

Процедура передачи конфигурации секретных ключей состоит из следующих этапов:

1. АРМ управления посылает на сервер-источник запрос информации об установленных на нём ключах.
2. Сервер-источник отправляет список ключей программе АРМ управления.
3. АРМ управления посылает на сервер-получатель запрос на создание ключевой пары и получение открытого ключа из этой пары.
4. Сервер-получатель создает ключевую пару и отправляет открытый ключ программе АРМ управления.
5. АРМ управления посылает на сервер-источник запрос на шифрование, содержащий полученный от сервера-получателя открытый ключ, подписанный при помощи открытого ключа из «общего секрета», и имя файла, который требуется зашифровать.
6. Сервер-источник проверяет подпись полученного открытого ключа при помощи мастер-ключа.
7. Сервер-источник шифрует указанный файл при помощи полученного открытого ключа.
8. АРМ управления посылает на сервер-источник запрос на получение зашифрованного файла.
9. Сервер-источник отправляет программе АРМ управления зашифрованный файл.
10. АРМ управления посылает полученный от сервера-источника зашифрованный файл на сервер-получатель.
11. АРМ управления посылает на сервер-получатель запрос на установку ключа (или всех ключей) из отправленного файла.
12. Сервер-получатель расшифровывает файл и устанавливает полученный ключ (или все ключи).

Основные возможности программы:

- Получение информации о ключах на сервере-источнике.
- Получение открытого ключа от сервера-получателя.
- Отправка открытого ключа и запроса на шифрование файла с помощью данного ключа на сервере-получателе.
- Шифрование файла при помощи указываемого ключа локально.
- Шифрование ключа RSA при помощи указываемого ключа локально.
- Получение файла от сервера-источника.
- Загрузка файла на сервер-получатель.
- Отправка запроса на установку всех ключей из файла на сервер-получатель.

1.2 Условия применения программы

Программа «АРМ управления бэкапированием» устанавливается на компьютер, удовлетворяющий следующим аппаратным требованиям:

- процессор не ниже Pentium II;
- НЖМД ёмкостью не менее 1 Гб;
- ОЗУ ёмкостью не менее 1 Гб.

Компьютер должен работать под управлением 32-х или 64-х битной операционной системы из семейства Windows.

На компьютере должно быть установлено СКЗИ «Бикрипт 5.0».

2 Установка программного изделия «АРМ управления бэкапированием»

Для того чтобы установить программное изделие «АРМ управления бэкапированием», следует скопировать содержимое дистрибутива «АРМ управления бэкапированием» на жёсткий диск компьютера.

3 Удаление программного изделия «АРМ управления бэкапированием»

Для того чтобы удалить программное изделие «АРМ управления бэкапированием», необходимо удалить с жёсткого диска компьютера ранее установленные файлы дистрибутива «АРМ управления бэкапированием».

4 Описание операций

4.1 Начало работы с программой «АРМ управления бэкапированием»

Для начала работы с программой «АРМ управления бэкапированием» следует в режиме командной строки (cmd) перейти в каталог, где расположен файл upc.exe, набрать строку

upc *command ip* [*port*] [*timeout*] *filelist*

и нажать клавишу Enter.

Здесь **command** – команда, которую следует выполнить:

Команда	Пояснение
info	Получить информацию о файлах на сервере-источнике
pub	Создать ключевую пару на сервере-получателе и получить открытый ключ
crypt	Зашифровать файл на сервере-источнике при помощи передаваемого ключа
local	Зашифровать файл при помощи указываемого ключа локально
rsa	Зашифровать ключ RSA при помощи указываемого ключа локально
get=xx	Получить файл от сервера-источника, где xx – размер блока обмена (от 100 до 10000 байтов)
put=xx	Загрузить файл на сервер-получатель, где xx – размер блока обмена (от 100 до 10000 байтов)
inst	Установить файл на сервер-получатель
onekey	Установить на сервер-получатель ровно один ключ из файла. (После выполнения команды необходимо перезагрузить сервер-получатель, чтобы ключ с диска стал доступен)

Параметр ***ip*** указывает ip-адрес сервера, на который отправляется команда.

Параметр **[*port*]** позволяет задать номер порта на сервере. Значение по умолчанию 850.

Параметр **[*timeout*]** позволяет задать значение допустимой задержки в миллисекундах. Значение по умолчанию 2000.

Параметр ***filelist*** позволяет задать имена файлов для чтения или записи информации в зависимости от команды.

4.2 Получение информации о файлах на сервере-источнике

Для того чтобы получить информацию о файлах на сервере-источнике, следует выполнить команду **info**.

Пример:

```
upc.exe info ip [port] [timeout] dir.txt
```

Здесь **dir.txt** – имя файла, в который будет записана информация о файлах на сервере-источнике.

4.3 Создание ключевой пары на сервере-получателе и получение открытого ключа

Для того чтобы создать ключевую пару на сервере-получателе и получить открытый ключ, следует выполнить команду **pub**.

Пример:

```
upc.exe pub ip [port] [timeout] fpsu.sgn
```

Здесь **fpsu.sgn** – имя файла, в который будет записан созданный открытый ключ.

4.4 Шифрование файла на сервере-источнике при помощи указываемого ключа

Для того чтобы зашифровать файл на сервере-источнике при помощи указываемого ключа, следует выполнить команду **crypt**.

Пример:

```
upc.exe cryp ip [port] [timeout] fpsu.sgn ini_file_from_list
```

Здесь **fpsu.sgn** – имя файла, содержащего ключ шифрования, а **ini_file_from_list** – имя файла для шифрования.

4.5 Шифрование файла при помощи указываемого ключа локально

Для того чтобы зашифровать файл при помощи указываемого ключа локально, следует выполнить команду **`local`**.

Пример:

```
upc.exe local fpsu.sgn input_my_file.raw output_my_file.enc key_file_from_list
```

Здесь **`fpsu.sgn`** – имя файла, содержащего ключ шифрования, **`input_my_file.raw`** – имя файла для шифрования, **`output_my_file.enc`** – имя файла, в который будет записан результат шифрования, а **`key_file_from_list –`** имя файла на сервере-источнике, в который впоследствии будет записан результат шифрования.

4.6 Шифрование ключа RSA при помощи указываемого ключа локально

Для того чтобы зашифровать ключ RSA при помощи указываемого ключа локально, следует выполнить команду **`rsa`**.

Пример:

```
upc.exe rsa fpsu.sgn rsa_raw_key.pem output_rsa_file.enc key_number [id]
```

Здесь **`fpsu.sgn`** – имя файла, содержащего ключ шифрования, **`rsa_raw_key.pem`** – имя файла с ключом RSA в формате PEM (mime64, base64), **`output_rsa_file.enc`** – имя файла, в который будет записан результат шифрования, **`key_number –`** номер ячейки ФПСУ (число от 1 до 9999), в которую следует поместить ключ RSA, а **`id –`** идентификатор Бикрипт ключа (не обязательно).

4.7 Получение файла от сервера-источника

Для того чтобы получить файл от сервера-источника, следует выполнить команду **`get=xx`**, где xx – размер блока обмена (от 100 до 10000 байтов).

```
upc.exe get=xx ip [port=850] [timeout=2000] my_file.enc
```

Здесь **`my_file.enc`** – имя файла, запрашиваемого с сервера-источника.

4.8 Загрузка файла на сервер-получатель

Для того чтобы загрузить файл на сервер-получатель, следует выполнить команду **put=xx**, где xx – размер блока обмена (от 100 до 10000 байтов).

Пример:

```
upc.exe put=xx ip [port=850] [timeout=2000] my_file.enc
```

Здесь **my_file.enc** – имя файла, загружаемого на сервер-получатель.

4.9 Установка всех ключей из файла на сервер-получатель

Для того чтобы установить все ключи из файла на сервер-получатель, следует выполнить команду **inst**.

Пример:

```
upc.exe inst ip [port=850] [timeout=2000]
```

4.10 Установка одного ключа из файла на сервер-получатель

Для того чтобы установить на сервер-получатель ровно один ключ из файла, следует выполнить команду **onekey**. После выполнения команды **onekey** необходимо перезагрузить сервер-получатель, для того чтобы установленный ключ стал доступен.

Пример:

```
upc.exe onekey ip [port=850] [timeout=2000] src_key dst_key
```

Здесь **src_key** – номер ячейки в файле, в которой был установлен ключ на сервере-источнике, а **dst_key** – номер ячейки, в которую следует установить ключ.

Лист регистрации изменений

№№ п/п	Дата	Описание изменения, основание для внесения изменения	Автор
1			
2			
3			