Шифрование ini-файлов

- Режим 1 (RSA Only)
- Режим 2 (RSA + AES)

В кассовом ПО Artix реализовано шифрование ini-файлов. Данный функционал позволяет обеспечить хранение и передачу данных в зашифрованном виде.

Считывание и расшифровка конфигурационных файлов происходит из основных директорий:

- /linuxcash/cash/conf/ncash.ini.d/,
- /linuxcash/cash/conf/ncash.ini.d/puppet/,
- /linuxcash/cash/conf/drivers/,
- /linuxcash/cash/queue/config/,
- /linuxcash/cash/view/config/.

Шифрование реализовано в двух режимах:

- **Режим 1:** Применяется для файлов размером не более 470 байт. Шифрование происходит с использованием открытого ключа алгоритма RSA.
- **Режим 2:** Применяется для файлов любого размера. В данном режиме применяется симметричный алгоритм AES-256 в режиме CBC. Ключ шифрования передается на кассу в защищенном виде с помощью шифрования открытым ключом алгоритма RSA.

После шифрования в директории будет создан файл <название_файла>.ini.enc. В записях логов и в консоли длина исходного значения не учитывается и маскируется тремя символами "*******".

Пример отображения при вызове /linuxcash/cash/bin/currentsettings

```
[gui]
   interface = ***
...
[theme]
   name = ***
```

Режим 1 (RSA Only)

Для шифрования ini-файла необходимо:

1. Добавить публичный ключ конфигурации public_key.pem в директорию, где находится конфигурационный файл.
2. Выполнить шифрование файла командой:

Пример шифрования gui.ini

openssl pkeyutl -encrypt -pubin -inkey public_key.pem -in **gui.ini** -out **gui.ini.enc**

Режим 2 (RSA + AES)

Для шифрования ini-файла необходимо:

1. Добавить публичный ключ конфигурации public_key.pem в директорию, где находится конфигурационный файл.
2. Выполнить шифрование файла командой:

Пример шифрования gui.ini

echo -n "password" | openssl pkeyutl -encrypt -pubin -inkey public_key.pem > **gui.ini.enc**

openssl enc -aes-256-cbc -k "password" -pbkdf2 -iter 100000 -in **gui.ini** -out data

cat data >> **gui.ini.enc**