Шифрование паролей и секретов

Для дополнительной защиты системы рекомендуется зашифровать файлы конфигурации после окончательных правок.

В составе дистрибутива доступна утилита Configuration protector - расположена в папке `\MISC\Core.IdP.Encryptor\`

Шифрованию подлежат конфигурационные файлы компонентов Core, IdP, ProxyApp и SSHProxy.

- Для шифрования конфигурации **core** выполните команду:

  ```
  Pam.Tools.Configuration.Protector protect --component Core --file C:\inetpub\wwwroot\pam\core\appsettings.json
  ```

- Для шифрования конфигурации **idp** выполните команду:

  ```
  Pam.Tools.Configuration.Protector protect --component Idp --file C:\inetpub\wwwroot\pam\idp\appsettings.json
  ```

- Для шифрования конфигурации **proxyapp** выполните команду:

  ```
  Pam.Tools.Configuration.Protector protect --component ProxyApp --file "C:\Program Files\IndeedPAM\Gateway\ProxyApp\appsettings.json"
  ```

- Для шифрования конфигурации **sshproxy** выполните команду

  ```
  Pam.Tools.Configuration.Protector protect --component SshProxy --file "C:\Program Files\IndeedPAM\SSH Proxy\SshProxy\appsettings.json"
  ```

Для расшифровки конфигурации выполните команду:

```
Pam.Tools.Configuration.Protector unprotect --file "c:\путь\к\файлу\конфигурации"
```

О механизме шифрования

Шифрование выполняется алгоритмом AES-256 с помощью набора ключей, который генерируется с использованием Data Protection API. Хранятся ключи в `%ProgramData%\Indeed\Pam\Keys`.

Ключи зашифрованы с использованием Windows Data Protection API с завязкой на ЭВМ (любой пользователь в рамках ЭВМ может зашифровать или расшифровать). Если ключи шифрования Data Protection API не синхронизированы между инстансами балансировщика, то необходимо перешифровать конфигурацию заново, так как у инстансов будут разные ключи.