# Міністерство освіти і науки України Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" НН Фізико-технічний інститут Дисципліна: "Методи реалізації криптографічних механізмів"

### ЛАБОРАТОРНА РОБОТА №4

Виконали:

Студенти групи ФБ-21мн

ЩЕРБАКОВ О.К. КАЗМІДІ І.Д.

## Завдання

1. Розробка реалізацій ІТ-систем (Реалізація Web-сервісу електронного цифрового підпису).

## Web-застосунок

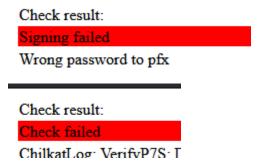
| DESZ          | 05       | *-*             | DEX1          |  |
|---------------|----------|-----------------|---------------|--|
| PFX:          | Оозор    | Файл не выбран. | PFX password: |  |
| File to sign: | Обзор    | Файл не выбран. |               |  |
| Sign          |          |                 |               |  |
|               |          |                 |               |  |
| Signature:    | Обзор    | Файл не выбран. |               |  |
| File to check | с: Обзор | Файл не выбран. |               |  |
| Check         |          |                 |               |  |

Веб-сторінка підпису для накладання підпису приймає PFX-контейнер з ключами користувача, пароль до контейнеру та файл, що треба підписати.

У відповідь користувачу у браузері завантажується відокремлений підпис у вигляді файлу формату .p7s.

Для перевірки підпису необхідно обрати файл та підпис у форматі р7s.

У випадку неправильно паролю до pfx-контейнера, неспівпадіння підпису або інших помилок - видається відповідне повідомлення.



Застосунок працює на веб-сервері Django. Криптографічні функції забезпечуються бібліотекою CkPython (Chilkat).

#### Висновки

Генератор ПВЧ модуля РуСтурtоDome має достатній рівень захищеності для використання у криптографічних системах ОС Linux. У критичних криптографічних системах (наприклад у державних установах) рекомендується користуватися апаратними джерелами ентропії для генераторів ПВЧ.