

Міністерство освіти і науки України  
Національний технічний університет «ХПІ»  
Навчально-науковий інститут комп'ютерних наук та інформаційних  
технологій  
Кафедра комп'ютерної інженерії та програмування

## **ЗВІТ**

з лабораторної роботи № 9  
з дисципліни «Сучасні технології безпечного програмування»  
**«ЗАХИСТ ВІД ЗМІНИ БІНАРНОГО ФАЙЛУ»**

Виконав:  
студент гр. КН-Н9226  
Кулик Д.І.

Перевірив:  
Бульба С. С.

Харків – 2022

**Мета роботи:** Навчитися підписувати виконувані файли.

### Індивідуальне завдання

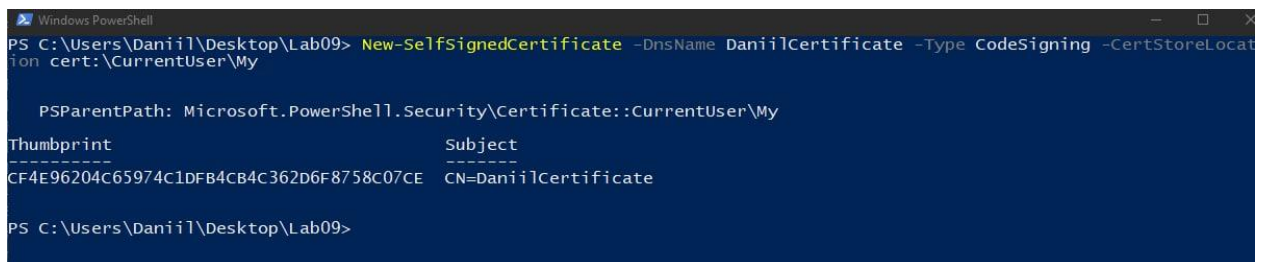
- створити сертифікат
- проінсталювати його в систему, щоб він був "довіреним"
- використовуючи проект будь-якої попередньої роботи, виконати підпис виконуваного файлу за допомогою утиліти SignTool (або JarSigner)
- виконати верифікацію підпису (бажано на рівні самого кода при завантаженні додатка):
  - чи є підписаний сертифікат валідним
  - чи не було (бінарної) зміни файлу та його код цілісний

### Хід роботи

В даній лабораторній роботі ми створимо сертифікат для цифрового підпису для цифрового підпису файлів за допомогою Windows PowerShell. Цифровий сертифікат зазвичай видається центром сертифікації (CA). Але ми збираємося створити самопідписаний сертифікат.

Файл підписується сертифікатом. Для перевірки автентичності можна використовувати криптографію. Це робиться за допомогою пари ключів закритого ключа та відкритого ключа. Файл має цифровий підпис за допомогою закритого ключа, а відкритий ключ використовується для перевірки його ідентичності. Відкритий ключ можна надати будь-кому. Приватний ключ тільки ваш. Це означає, що нашу особу можна перевірити.

### Створюємо сертифікат



```
Windows PowerShell
PS C:\Users\Danil\Desktop\Lab09> New-SelfSignedCertificate -DNSName DanilCertificate -Type CodeSigning -CertStoreLocation cert:\CurrentUser\My

PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                               Subject
-----
CF4E96204C65974C1DFB4CB4C362D6F8758C07CE  CN=DanilCertificate

PS C:\Users\Danil\Desktop\Lab09>
```

**Рисунок 1** – Створений сертифікат

### Експорт сертифікату без private ключа

Для експорту [0] змусить це працювати для випадків, коли є більше одного сертифіката. Очевидно, що індекс повинен відповідати сертифікату, який ми хочемо використовувати.

```
PS C:\Users\Danii\\Desktop\Lab09> Export-Certificate -Cert (Get-Childitem Cert:\CurrentUser\My -CodeSigningCert)[0] -FilePath code_signing.crt

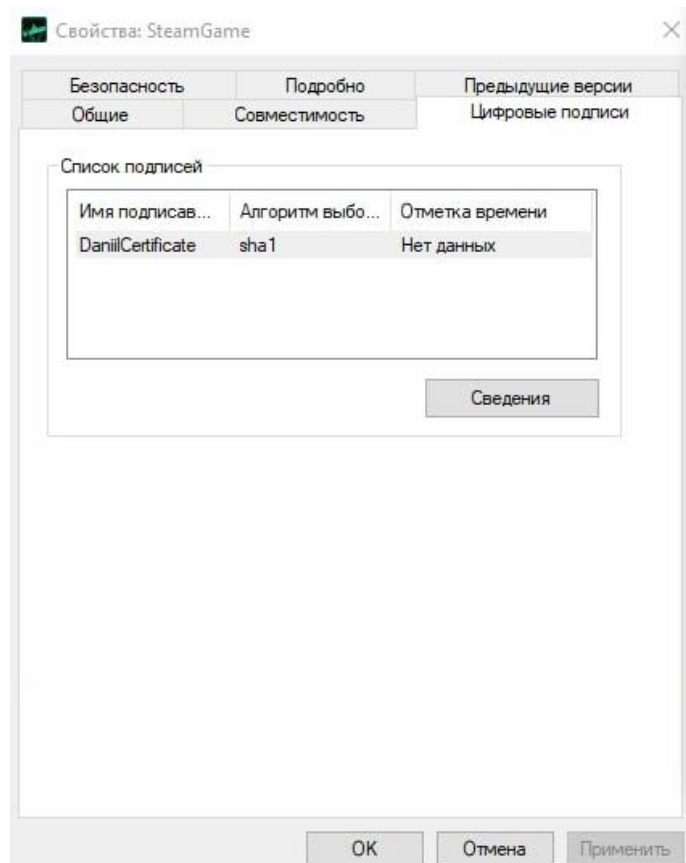
Каталог: C:\Users\Danii\Desktop\Lab09

Mode                LastWriteTime         Length Name
----                -
-a-----         27.11.2022    19:18           810 code_signing.crt

PS C:\Users\Danii\Desktop\Lab09> _
```

**Рисунок 2 – Экспорт сертификату**

Виконаємо перевірку на ОС Windows:



**Рисунок 2 – Підписаний .exe файл**

Імпортуємо сертифікат щоб зробити його Trusted

```
PS C:\Users\Danii\Desktop\Lab09> Import-Certificate -FilePath .\code_signing.crt -Cert Cert:\CurrentUser\TrustedPublisher

PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\TrustedPublisher

Thumbprint                               Subject
-----
CF4E96204C65974C1DFB4CB4C362D6F8758C07CE CN=DaniiCertificate
```

**Рисунок 3 – Імпорт сертификату**

Імпортуємо сертифікат як кореневий центр сертифікації

```
PS C:\Users\Daniil\Desktop\Lab09> Import-Certificate -FilePath .\code_signing.crt -Cert Cert:\CurrentUser\Root

PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\Root
Thumbprint           Subject
-----
CF4E96204C65974C1DFB4CB4C362D6F8758C07CE CN=DaniilCertificate

PS C:\Users\Daniil\Desktop\Lab09>
```

**Рисунок 4 – Імпорт сертифікату**

Підпис .exe файлу

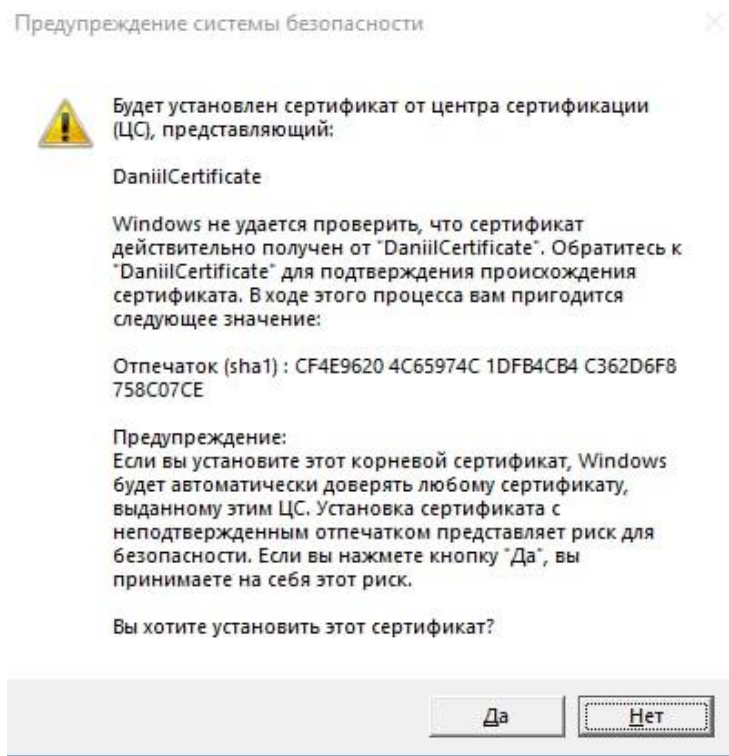
```
PS C:\Users\Daniil\Desktop\Lab09> Set-AuthenticodeSignature .\SteamGame.exe -Certificate (Get-Childitem Cert:\CurrentUser\My -CodeSigningCert)

Каталог: C:\Users\Daniil\Desktop\Lab09

SignerCertificate           Status           Path
-----
CF4E96204C65974C1DFB4CB4C362D6F8758C07CE Valid           SteamGame.exe

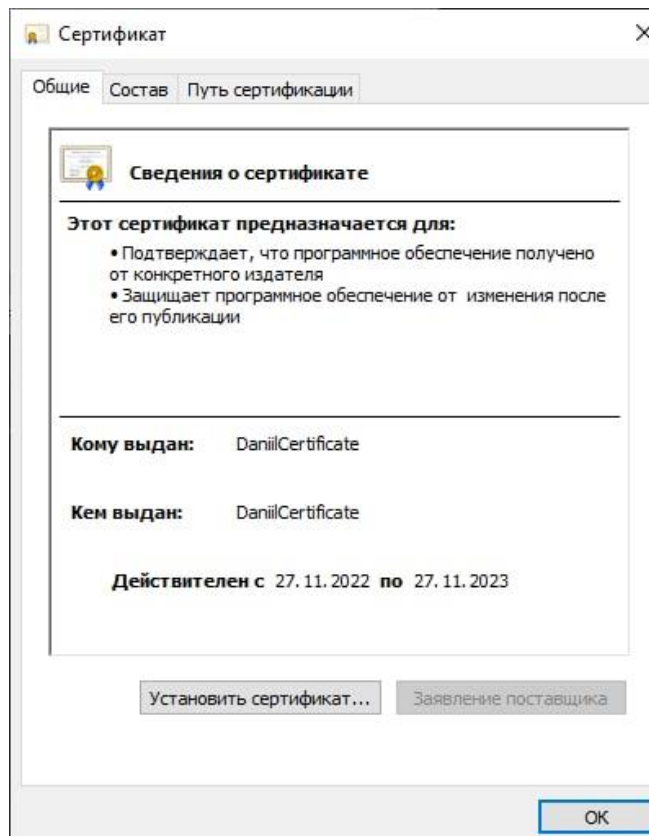
PS C:\Users\Daniil\Desktop\Lab09>
```

**Рисунок 5 – Підпис файлу**

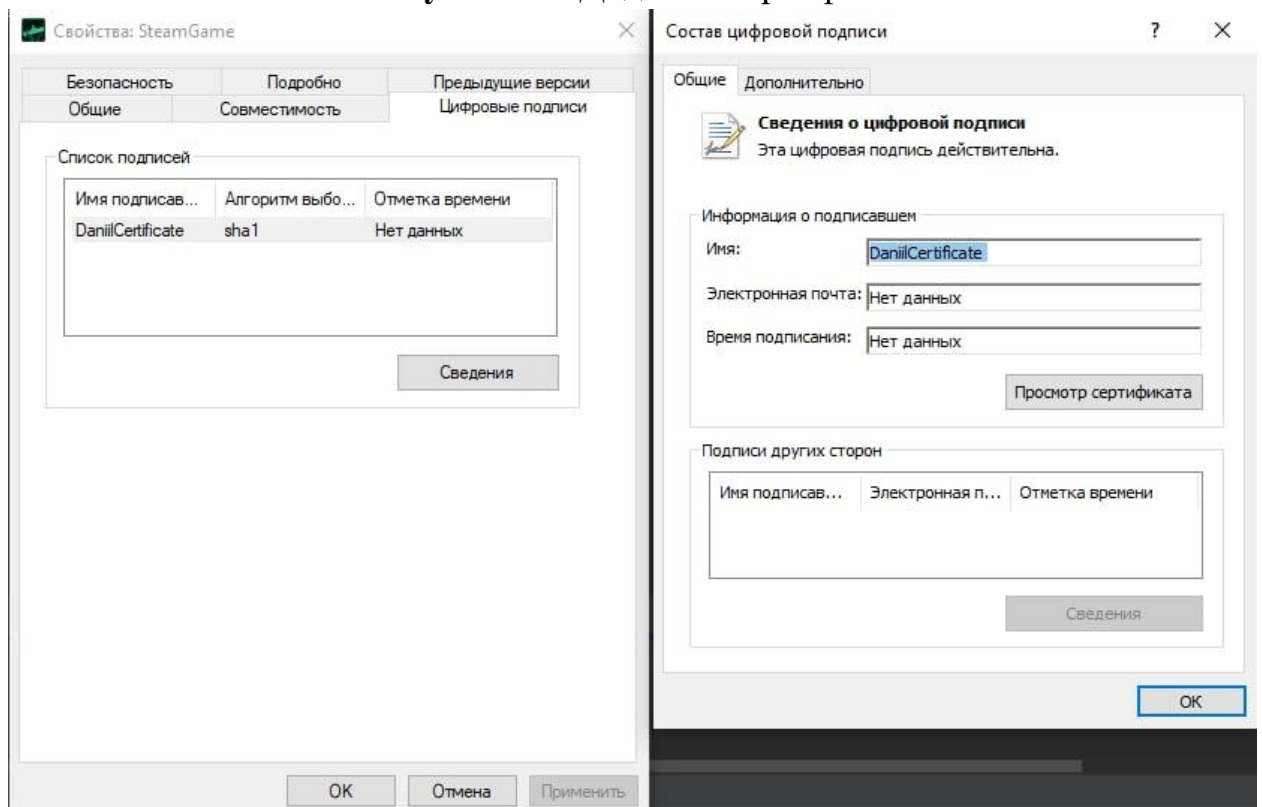


**Рисунок 6 – Підтвердження додавання сертифікату в trusted**

Тепер доданий сертифікат не відображається як Untrusted



**Рисунок 7 – Доданий сертифікат**



**Рисунок 8 – Перевірка підпису**

**Висновки:** в результаті виконання лабораторної роботи навчилися підписувати виконувані файли.