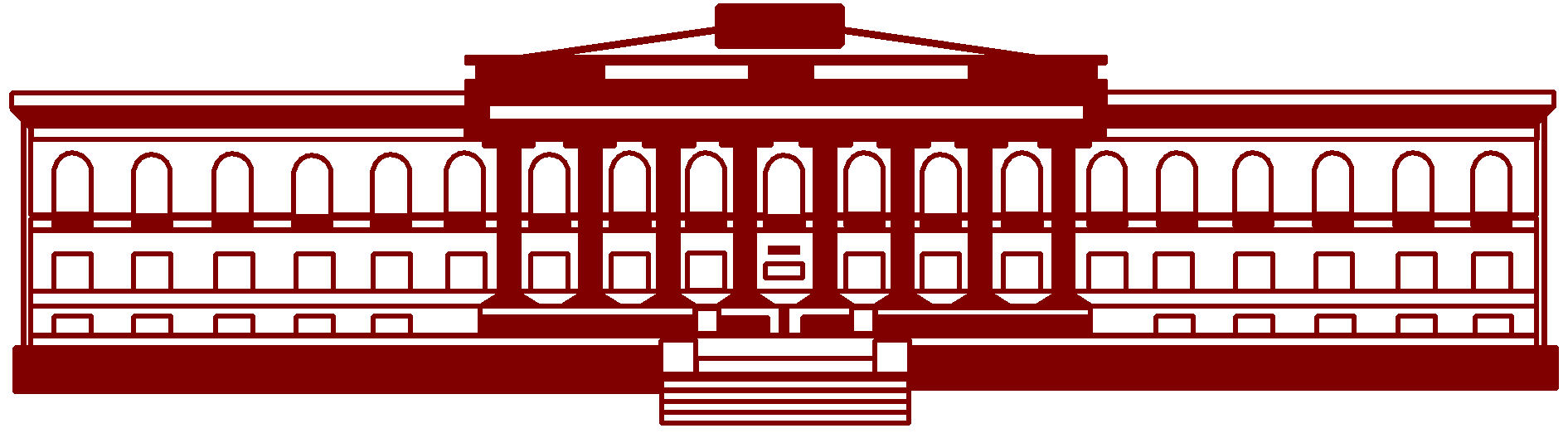
**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**імені ТАРАСА ШЕВЧЕНКА**

****

**ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**Кафедра прикладних інформаційних систем**

**Звіт до лабораторної роботи №2**

**З курсу**

**«Безпека мереж і комп’ютерних систем»**

*студента 2 курсу*

*групи ПП-22*

*спеціальності 122 «Комп'ютерні науки»*

*ОП «Прикладне програмування»*

Шевлюк Вікторії Віталіївни

*Перевірив:*

д.т.н, професор

Сайко В. Г.

**Київ 2022**

**Тема:** Профілактика проникнення «троянських програм»

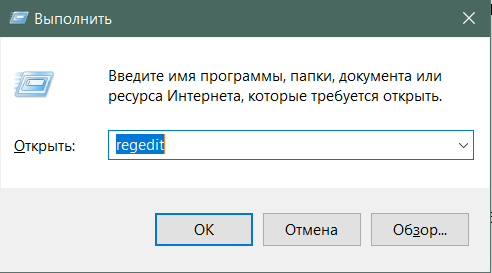
**Мета:** перевірити потенційні місця записів «троянських програм» у системному реєстрі операційної системи Windows

**Завдання:**

1. Перевірте вміст ключа HKEY\_LOCAL\_MACHINE\Software\ Microsoft\WindowsNT\CurrentVersion\Winlogon\System (REG\_SZ).
2. Зафіксуйте етапи роботи, використовуючи команду PrintScreen клавіатури.
3. Складіть звіт про результати перевірки.

**Хід роботи:**

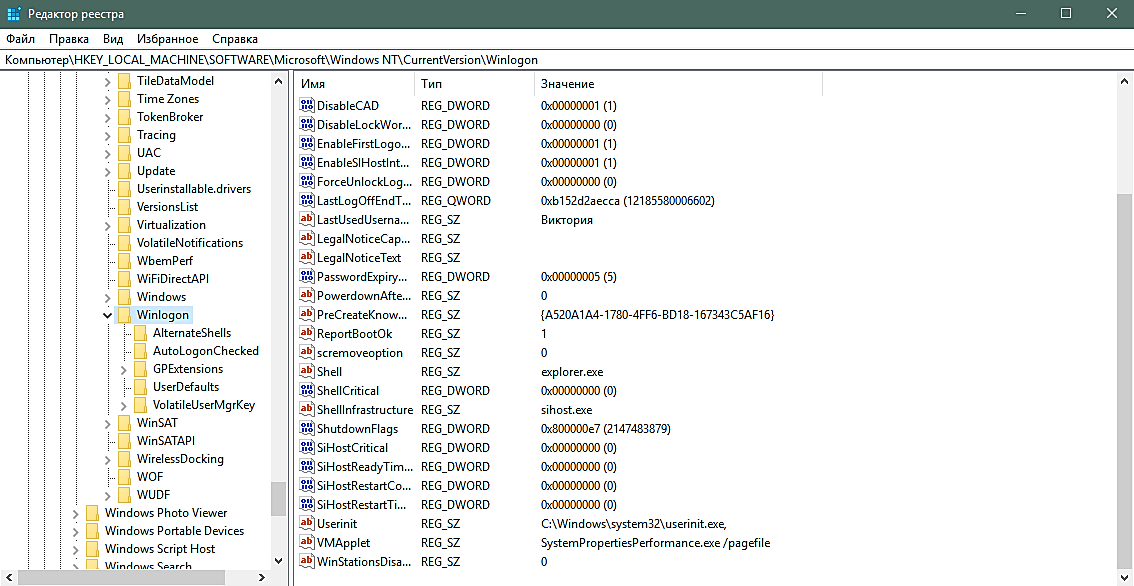
1. Запускаємо програму **regedit.exe** за домогою вікна «Виконати»



1. У вікні, що відкрилося, обираємо галузь HKEY\_LOCAL\_MACHINE і **далі Software\Microsoft\WindowsNT\CurrentVersion\**Winlogon.

У правій половині відкритого вікна програми **regedit.exe** з'явився список ключів.

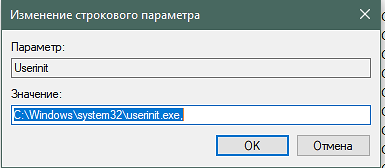
Нам потрібно знайти Userinit та перевірити його вміст.



1. За замовчуванням (вихідний стан) 151 цей ключ містить наступний запис **C:\WINDOWS\system32\userinit.exe**.

Якщо в зазначеному ключі втримуються додаткові записи, то це можуть бути «троянські програми».

Поглянемо на зміст мого ключа:

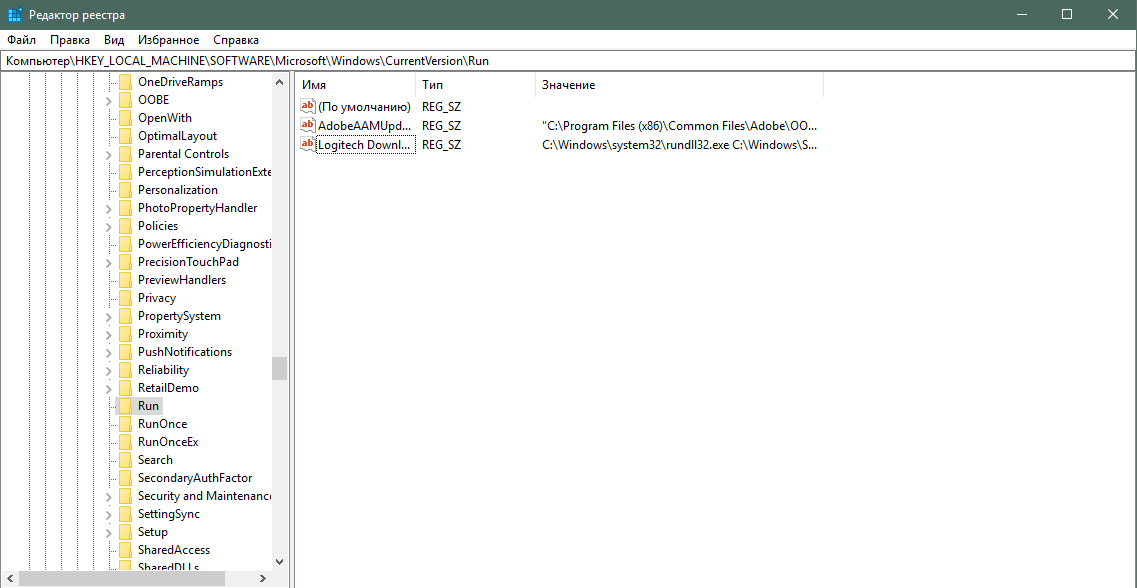


Як бачимо, ключ відповідає його нормальному змісту, а отже в цьому місці троянів не виявлено.

1. Ще одним потенційним місцем записів на запуск «троянських програм» є розділ автопуску **Run**.

Щоб перевірити його, обираємо галузь HKEY\_LOCAL\_MACHINE **і далі**

**Softtware\Microsoft\Windows\CurrentVersion\Run\...** (**REG\_SZ**).



Підозрілих записів у цьому розділі я не бачу, тому можу зробити висновок, що на моєму пристрої троянів у реєстрі не виявлено.

**Висновок:**

Виявити такі шкідливі програми як «троянські програми» на комп’ютері можна за допомогою перевірки ключа у реєстрі.

Щоб перевірити реєстр, потрібно запустити програму **regedit.exe** за допомогою вікна «Виконати» і перевірити два місця: Userinit та Run.

Якщо в ключі Userinit виявлено розбіжності з нормальним його станом, потрібно проаналізувати місце розташування програми, звернути увагу на час створення файлу й зіставити з моїми діями в цей час.

Якщо час створення файлу збігається з часом моєї роботи в Інтернеті, то можливо, що в цей час мій комп'ютер був заражений «троянською програмою».

Для видалення цього запису необхідно двічі клацнути по назві ключа

(або при виділеному ключі вибрати команду **Змінити** з меню **Виправлення** програми **regedit.exe**).

У вікні, що відкрилося, у поле Значення видалити посилання на підозрілий файл та закрити програму **rеgedit.exe**.

Далі переходимо у папку з підозрілим файлом і видаляємо його.

Перезавантажуємо операційну систему і знову перевіряємо вміст цього ключа.

Якщо вміст розглянутого ключа не змінився, то передбачуваний троян успішно вилучений з системи.

У разі виявлення підозрілих записів у розділі Run, слід повторити той самий алгоритм дій.

Таким чином можна час від часу перевіряти наш пристрій на наявність шкідливих програм – а саме «троянських програм».

**Контрольні запитання:**

1. ***Що таке реєстр?***

**Реєстр операційної системи Windows** — це велика база даних, де зберігається інформація про конфігурації системи. Цією інформацією користуються як операційна система Windows, так й інші програми.

1. ***Поясніть особливості «троянських програм»***

Головною особливістю «троянських програм» є те, що вони НЕ здатні поширюватись самостійно – тобто відтворювати самі себе, саме тому вони розповсюджуються безпосередньо людьми.

В основному вони потрапляють на пристрій шляхом встановлення як додаток (програми видаються за безпечне програмне забезпечення і жертви можуть, не знаючи цього, завантажити їх на комп’ютер), або через ел. пошту.

Такі програми можуть повністю імітувати діяльність програми, під яку вони маскуються.

Також розробники таких програм можуть спершу видати жертві продукт без шкідливого коду, а потім перекомпілювати програму, додавши до неї шкідника.

Використовуються троянські програми для шпигування, заважання роботі користувача, використання ресурсів комп’ютера-жертви для незаконної діяльності.

1. ***Чому профілактика «троянських програм» пов’язана із системним реєстром?***

Оскільки в системному реєстрі можна знайти сліди троянських програм та визначити їх розташування – профілактика таких вірусів і пов’язана реєстром.

1. ***Які розділи й ключі є потенційними місцями записів «троянських програм»?***

► галузь HKEY\_LOCAL\_MACHINE і **далі Software\Microsoft\WindowsNT\CurrentVersion\**Winlogon – ключ Userinit (pа замовчуванням (вихідний стан) 151 цей ключ містить наступний запис **C:\WINDOWS\system32\userinit.exe**. )

► галузь HKEY\_LOCAL\_MACHINE **і далі**

**Softtware\Microsoft\Windows\CurrentVersion\Run\...** (**REG\_SZ**).

**(**не має бути підозрілих записів**)**