УДК 004.056
DOI: 10.31673/2409-7292.2023.020006

**Волошко Д. С., Гамза Д. Є., Смолєв Є. С.**

# ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ПРОСТИХ ВІРУСІВ У ПРОГРАМНОМУ КОДІ

У даній статті розглянуто питання виявлення простих вірусів у програмному коді. Віруси можуть завдати значної шкоди програмному забезпеченню, тому важливо попередити їхнє поширення та виявляти їх вчасно. Для виявлення вірусів можна використовувати різні методики, такі як вірус сканери, статичний аналіз коду, аналіз поведінки програмного коду та інші. При виявленні вірусів в програмному коді важливо звертати увагу на контекст виявлення та досвід експерта з безпеки програмного забезпечення. Виявлення вірусів у програмному коді є важливим етапом в забезпеченні безпеки програмного забезпечення та може допомогти запобігти шкоді, яку можуть завдати віруси.

**Ключові слова:** віруси, програмний код, виявлення, безпека, методи виявлення, статичний аналіз, динамічний аналіз, машинне навчання.

## Вступ

Віруси у програмному коді можуть стати серйозною загрозою безпеці комп'ютерів та інших пристроїв. Програмний код, який містить віруси, може призвести до відключення систем, викрадення конфіденційної інформації або навіть знищення даних. Одним з найбільш поширених типів вірусів є прості віруси, які можуть швидко поширюватися та заражати інші програми. У цій статті ми розглянемо основні ознаки простих вірусів та інструменти їх виявлення в програмному коді. Також ми надамо рекомендації щодо захисту програмного коду від простих вірусів.

## Постановка проблеми

Віруси програмного коду – це зловмисні програми, які можуть відтворювати себе та вбудовуватися в інші програми. Ці програми зазвичай розповсюджуються шляхом копіювання та запуску від імені їх жертв. Якщо вірус вбудовується в програмний код, він може стати невидимим та почати діяти без знання користувача. Віруси у програмному коді можуть мати різноманітні наслідки, включаючи викрадення чутливої інформації, знищення даних та пошкодження програмного забезпечення. Віруси можуть працювати в тлі, невидимо для користувача, та поступово знищувати дані або збільшувати обсяг пам'яті, що використовується програмою, що призводить до відключення систем. Одним із основних типів вірусів у програмному коді є прості віруси. Далі ми розглянемо їх ознаки та механізм поширення.

## Аналіз дотичних робіт

Загальні напрямки дослідження у галузі виявлення вірусів у програмному коді включають:

*Аналіз синтаксису* та поведінки програмного коду: дослідження способів виявлення вірусів за допомогою аналізу синтаксису та структури програмного коду, а також аналізу його поведінки [1]. Цей метод базується на порівнянні двох версій програмного коду та виявленні змін, які можуть свідчити про наявність вірусу. Наприклад, можна порівняти оригінальний програмний код зі зміненим кодом та порівняти різницю між ними. Якщо виявлено зміни, які не пов'язані з оновленням або покращенням програмного коду, то це може свідчити про наявність вірусу. Цей метод є корисним для виявлення вірусів, які маскують свою присутність шляхом внесення незначних змін у програмний код.

*Машинне навчання*: застосування методів машинного навчання, зокрема нейронних мереж, для виявлення вірусів у програмному коді [2]. Машинне навчання стає все більш популярним методом виявлення вірусів у програмному коді. Цей метод базується на створенні моделей, які можуть відрізняти "здоровий" код від коду, що містить вірус. Ці моделі можуть бути навчені на великій кількості програмного коду та здатні виявляти навіть невеликі зміни, які можуть свідчити про наявність вірусу.

*Віртуалізація*: використання віртуальних машин для виявлення вірусів здійснюється шляхом пошуку та аналізу змін в програмному коді [3]. Використання віртуальної машини для

виконання програмного коду може допомогти виявити прості віруси, які використовують вразливості в операційній системі для запуску свого коду. Віртуальна машина забезпечує ізольоване середовище виконання програмного коду, що ускладнює можливість використання вразливостей операційної системи.

*Статистичні методи*: використання статистичних методів для виявлення аномалій у програмному коді, які можуть вказувати на наявність вірусів [4]. Цей метод полягає у спостереженні за виконанням програмного коду та виявленні незвичних дій, які можуть свідчити про наявність вірусу. Наприклад, можна аналізувати виклики до системних функцій, що можуть вказувати на спробу вірусу отримати доступ до системних ресурсів. Цей метод може виявляти навіть ті віруси, які змінюють свою сигнатуру.

*Сигнатурний аналіз*: використання баз даних підписів вірусів для виявлення знайомих вірусів у програмному коді [5]. Сигнатурний аналіз є одним з найпоширеніших методів виявлення вірусів у програмному коді. Цей метод базується на пошуку унікальних сигнатур або підписів, що характерні для певного вірусу. Ці сигнатури можуть бути ключовими словами, шаблонами байтів або послідовностями команд, які використовуються вірусом. Шукаючи ці сигнатури у програмному коді, можна виявити наявність вірусу. Однак, цей метод має деякі недоліки. По-перше, вірус може бути модифікованим, що змінює його сигнатуру та робить метод непридатним для виявлення. По-друге, більш складні віруси можуть містити декілька різних сигнатур, що робить метод менш ефективним.

Зазначені напрямки є лише декількома із можливих методів виявлення вірусів у програмному коді, але вони можуть бути використані дослідниками та фахівцями зі збереження безпеки інформації для покращення захисту комп'ютерних систем. Хоча методи виявлення вірусів у програмному коді постійно удосконалюються, вони не можуть гарантувати 100% виявлення всіх видів вірусів. Тому важливо дотримуватись правил безпеки при роботі з програмним кодом та використовувати антивірусне програмне забезпечення для захисту від можливих загроз.

**Метою** цієї статті є розглянути, що таке прості віруси у програмному коді та як вони можуть стати загрозою безпеці комп'ютерів та інших пристроїв. У статті будуть описані основні ознаки простих вірусів та розглянуті інструменти їх виявлення в програмному коді. Також, стаття надасть рекомендації щодо захисту програмного коду від простих вірусів. Кінцевою метою статті є допомога читачам у попередженні зараження програмного коду вірусами та збереженні безпеки їх комп'ютерів та інших пристроїв.

**Приклади простих комп’ютерних вірусів**

У соціальних мережах та на популярних Веб-ресурсах можна знайти сотні публікацій про методи, за допомогою яких можна створити комп’ютерний вірус за лічені секунди. Разом з тим, не слід забувати, що такий вид діяльності є небезпечним і протизаконним та може нанести шкоду як комп’ютерам у мережі, так і самому розробнику вірусу. Ось декілька прикладів, знайдених в Інтернеті, щодо створення вірусів [6].

**Відносно безпечні віруси:**

**1. Заборона доступу до Інтернету**

Цей вірус зовсім не шкідливий і не може зашкодити роботі комп’ютера. Ним можна здивувати своїх друзів чи знайомих, закривши їм доступ до Інтернету.

1. У Блокноті необхідно написати код (рис. 1).

2. Тепер потрібно зберегти цей файл під будь-якою назвою але з розширенням «.bat». Наприклад, notepad.bat.

3. Далі, надіслати цей файл друзям.

4. Коли вони відкриють цей файл, їх IP-адреса буде втрачена.

5. Щоб вирішити цю проблему, просто потрібно ввести renew або IPconfig у cmd, і проблему буде вирішено.

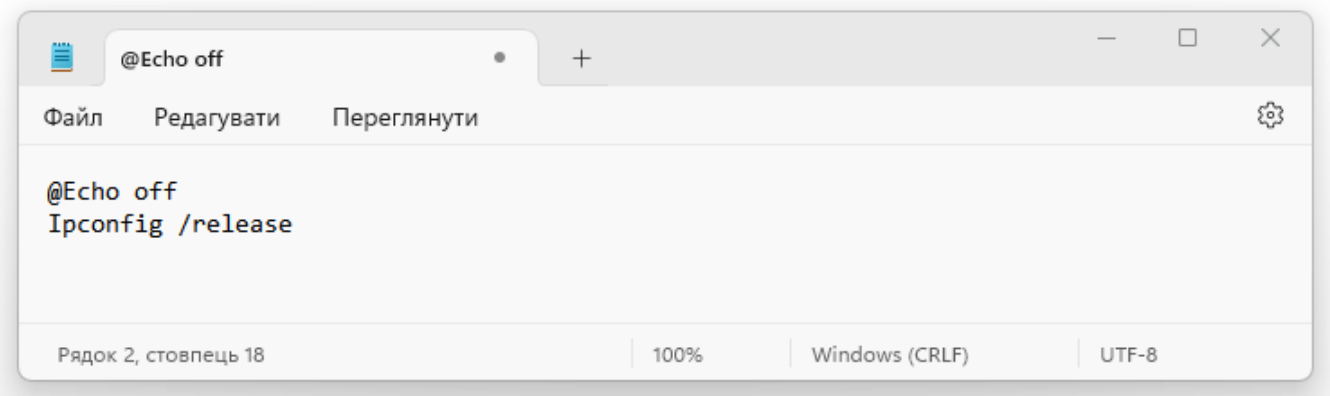


Рис. 1. Код вірусу заборони доступу до Інтернету

**2. Матричний екран**

Це також не справжній вірус і є достатньо безпечним. Використовуючи цей метод, можна побачити екран матричного типу з зеленими лініями, які раптово з'являться на екрані. Коли ваші друзі побачать це, вони подумають, що на їх комп'ютері є вірус, оскільки зелений екран виглядає саме так.

1. У Блокноті треба набрати код (рис. 2).
2. Зберегти файл під назвою «Matrix.bat».
3. Відкрити файл і побачити шоу.

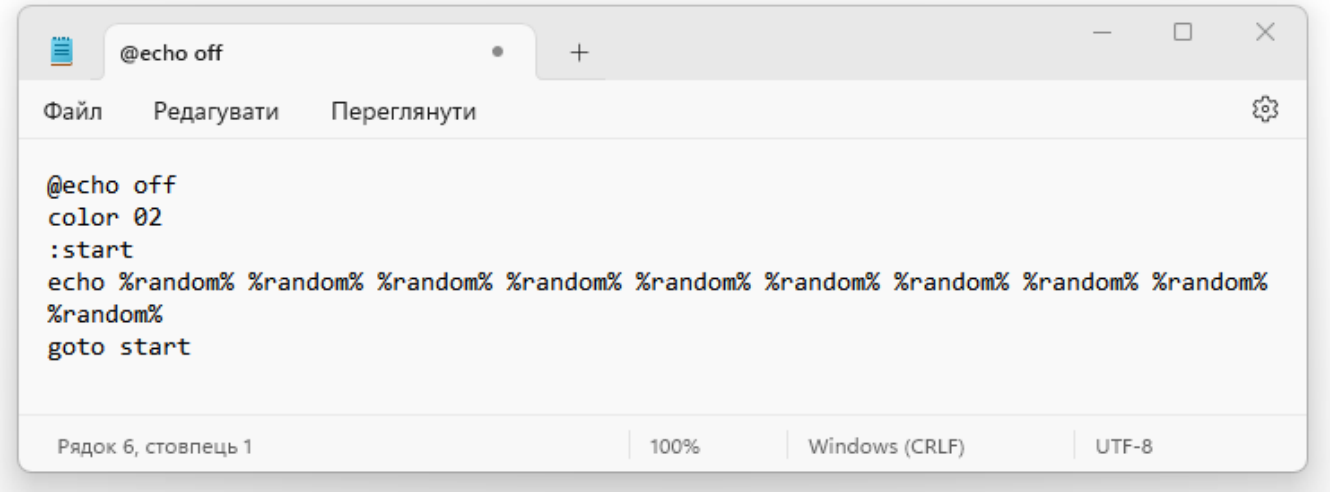


Рис. 2. Код вірусу Матричний екран

**3. Вимкнення комп'ютера**

Використовуючи цей метод, можна легко вимкнути комп'ютер за допомогою нешкідливого вірусу.

1. На першому кроці потрібно клацнути правою кнопкою миші на робочому столі та вибрати опцію «Створити ярлик».

2. В полі «Укажіть розташування об'єкта» потрібно ввести наступне (рис. 3). Можна ввести будь-яке число замість 50. Це число використовується для встановлення часу в секундах.

3. Тепер потрібно натиснути «Далі».

4. Потім можна ввести назву будь-якої програми. Наприклад, Google Chrome.

5. В цьому вікні (рис. 4) необхідно обрати піктограму для вірусу, як у нашому прикладі – Google Chrome, чим буде легко когось заплутати. Наш вірус матиме піктограму, як Google Chrome і при натисканні на неї, комп'ютер вимкнеться.

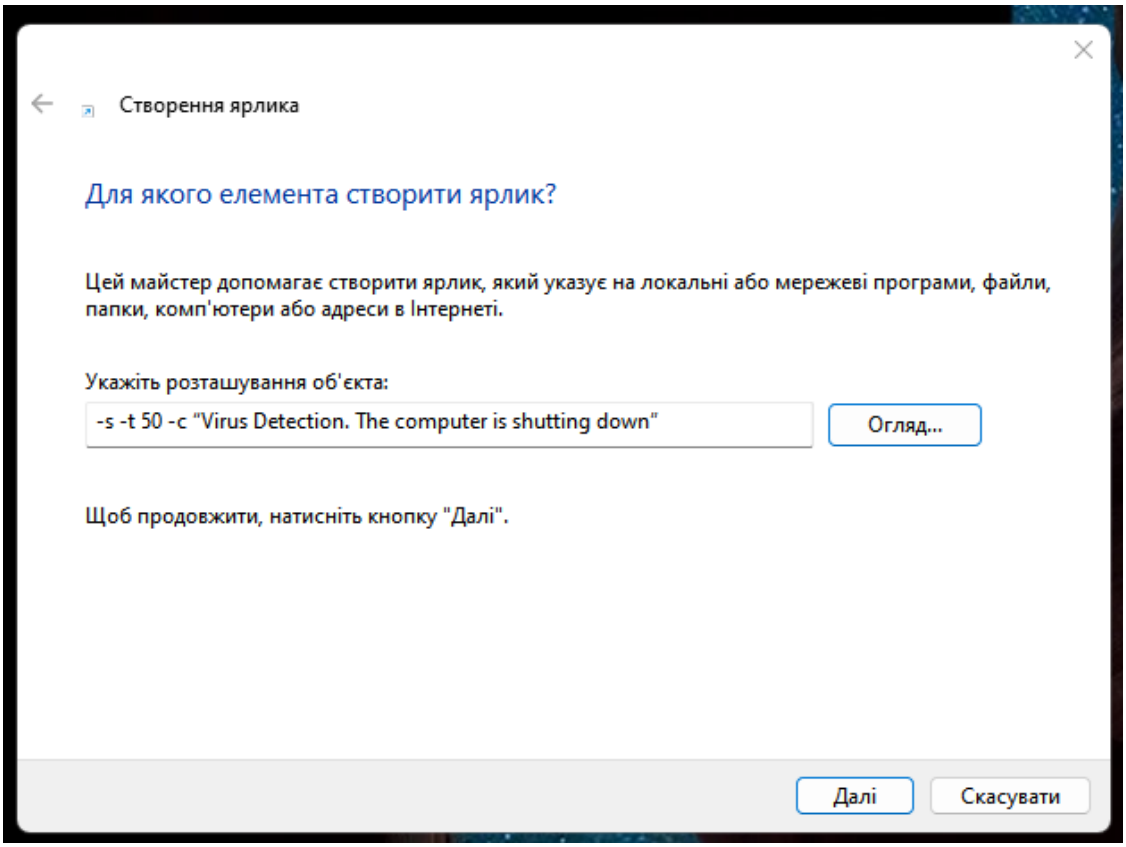


Рис. 3. Заповнення поля «Укажіть розташування об’єкта»

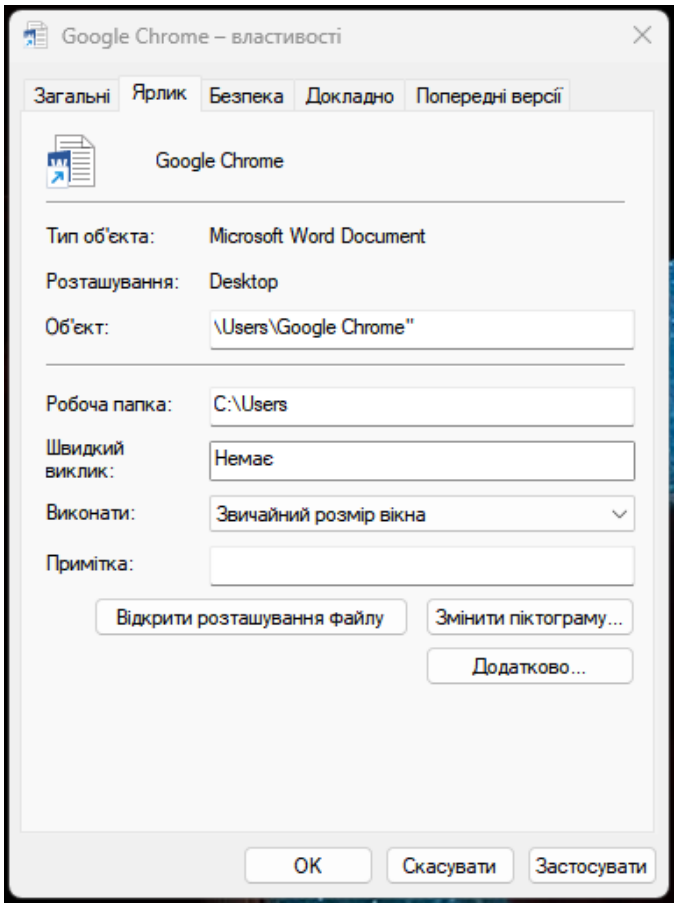


Рис. 4. Вікно для зміни піктограми для вірусу

**4. Видалення Cdrom**

Нижче наведено кроки для створення вірусу Cdrom, який відключає DVD чи CD-приводи:

1. У Блокнот необхідно вставити код (рис. 5).
2. Далі потрібно зберегти цей файл з розширенням “.vbs”. Наприклад, notepad.vbs
3. Якщо двічі клацнути на цьому файлі, DVD і CD-приводи будуть повністю вимкнуті.
4. Щоб зупинити цей вірус, доведеться відкрити диспетчер завдань, вибрати вкладку процесу, а потім натиснути «завершити файл wscript.exe».

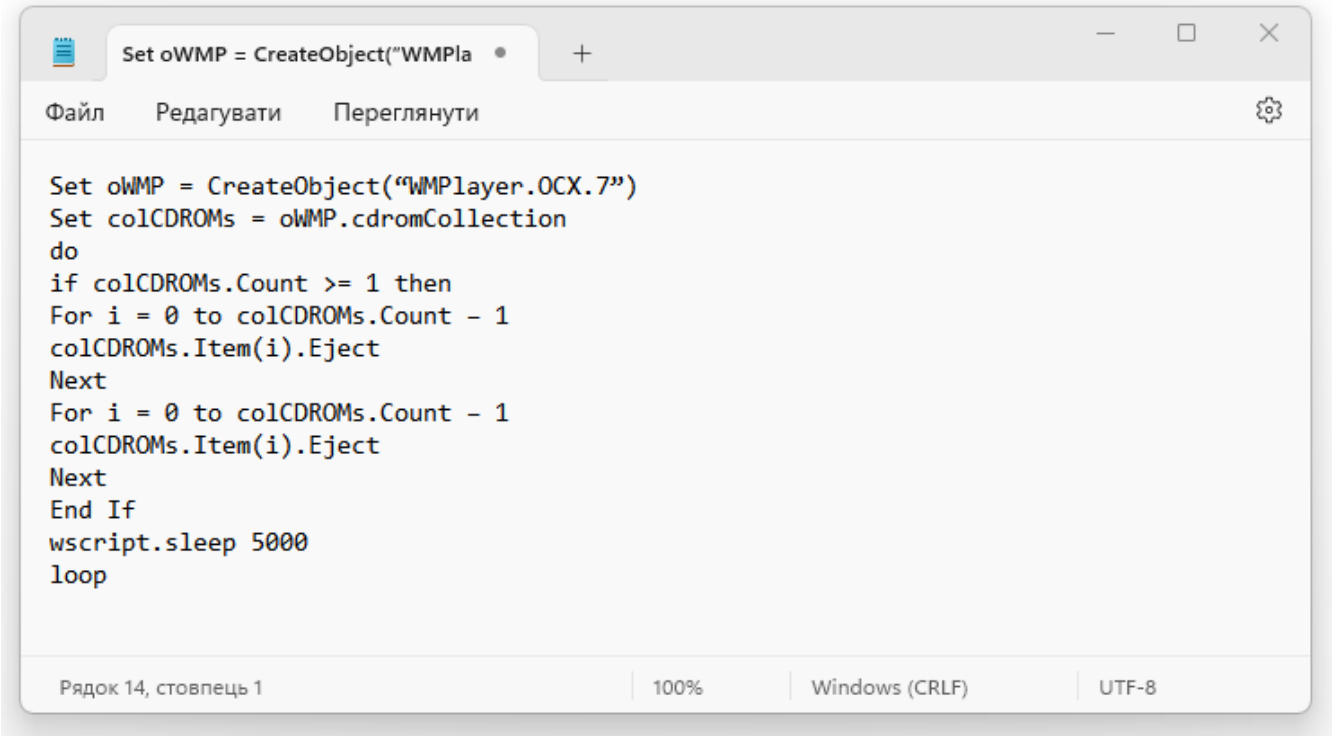


Рис. 5. Код вірусу Cdrom

**5. Перевірка антивірусу**

Нижче наведено кроки для створення вірусу, за допомогою якого можна протестувати свій антивірус:

1. У Блокноті необхідно ввести код (рис. 6).
2. Тепер потрібно зберегти цей файл під назвою «EICAR.COM».
3. Якщо на комп’ютері є активний антивірус, файл буде негайно видалено. Цей вірус абсолютно не шкідливий для комп'ютера і його можна використовувати для перевірки рівня безпеки антивірусних програм.

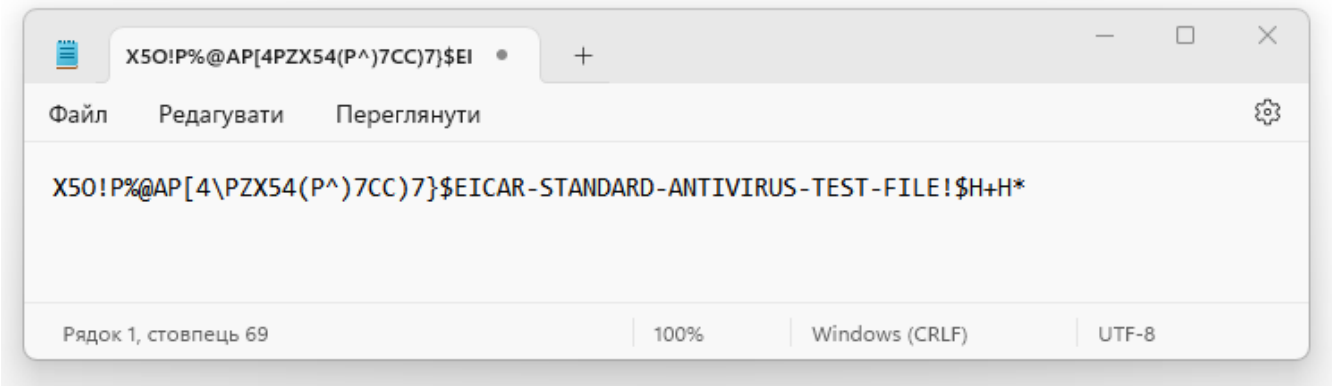


Рис. 6. Код вірусу для перевірки Антивірусної програми

**Прості, але небезпечні віруси**

Поряд з простими нешкідливими вірусами у мережі є багато прикладів коду шкідливих вірусів, що здатні нанести шкоду комп'ютерам. Відтворення таких вірусів є небезпечним та протизаконним, і тому не рекомендується. У даній публікації зразки коду використовуються виключно з дослідницькою метою.

**1. Небезпечний вірус для ПК**

1. У Блокноті потрібно вставити код (рис. 6).
2. Далі, потрібно зберегти цей файл з розширенням ".bat". Наприклад, notepad.bat
3. Тепер, при запуску цього файлу, диск С комп'ютера **буде видалено**. Також буде **знищено операційну систему** комп'ютера. Важливо пам'ятати, що не варто випробувати це на своєму комп'ютері чи з будь-якою незаконною метою.

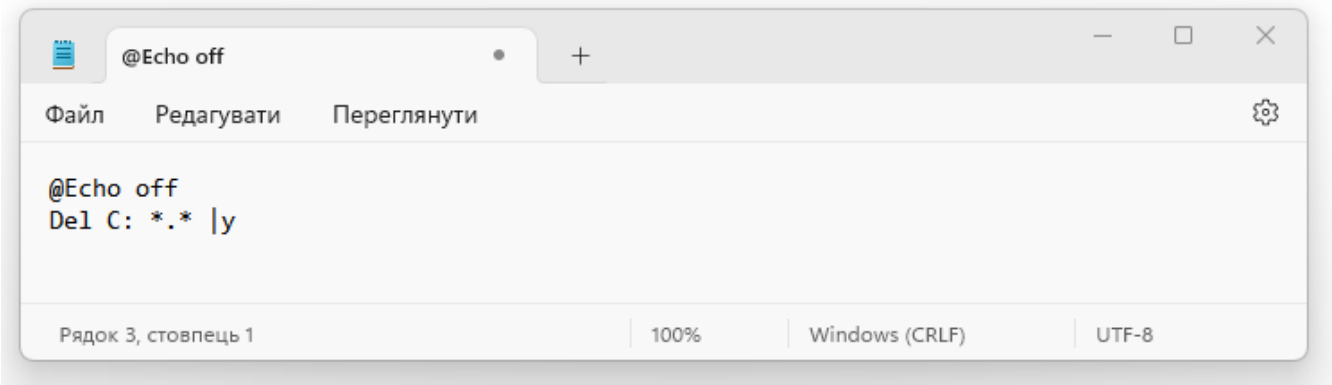


Рис. 6. Код вірусу для знищення операційної системи

Нижче наведено деякі інші коди для створення вірусів. Всі ці віруси дуже небезпечні, оскільки шкоду, спричинену такими вірусами, неможливо відновити або виправити.

**2. Відключення Інтернету назавжди**

Код, наведений на рис. 7, назавжди вимкне підключення до Інтернету. Отже, необхідно бути обережним, перш ніж використовувати цей вірус.

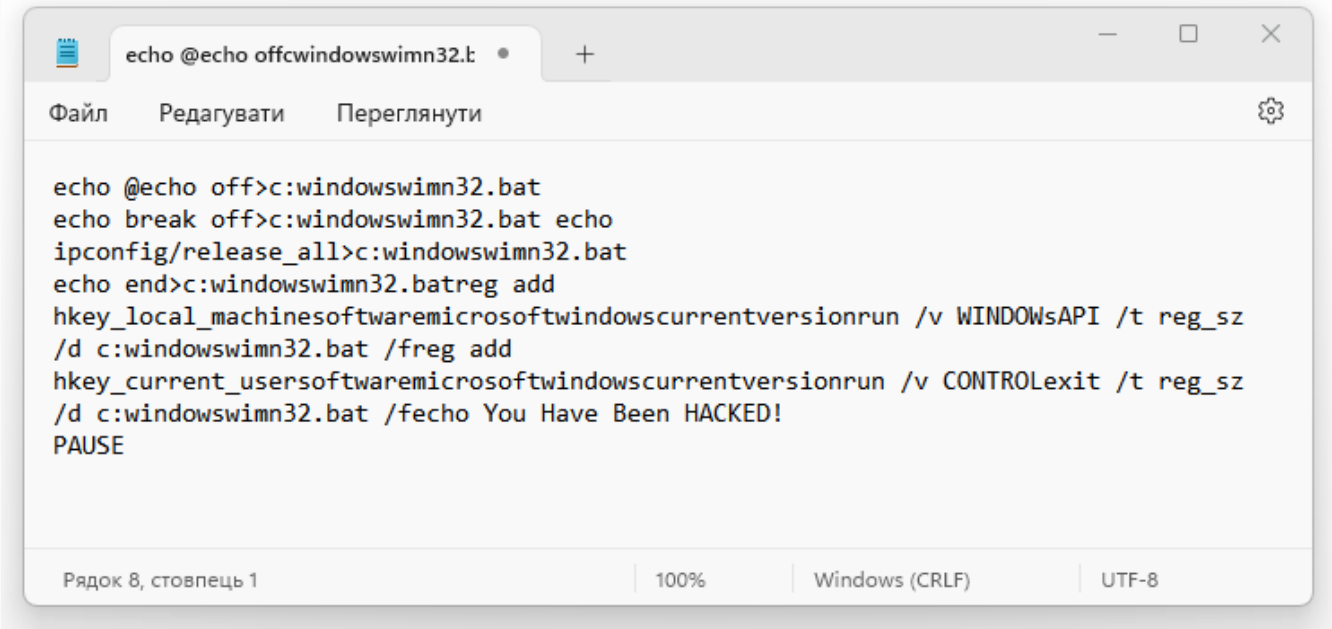


Рис. 7. Код вірусу для відключення Інтернету назавжди

**3. Нескінченні Блокноти**

Збій або зависання комп'ютера можна спричинити за допомогою коду (рис. 8), який створює нескінченні блокноти на комп'ютері, що призведе до його зависання.

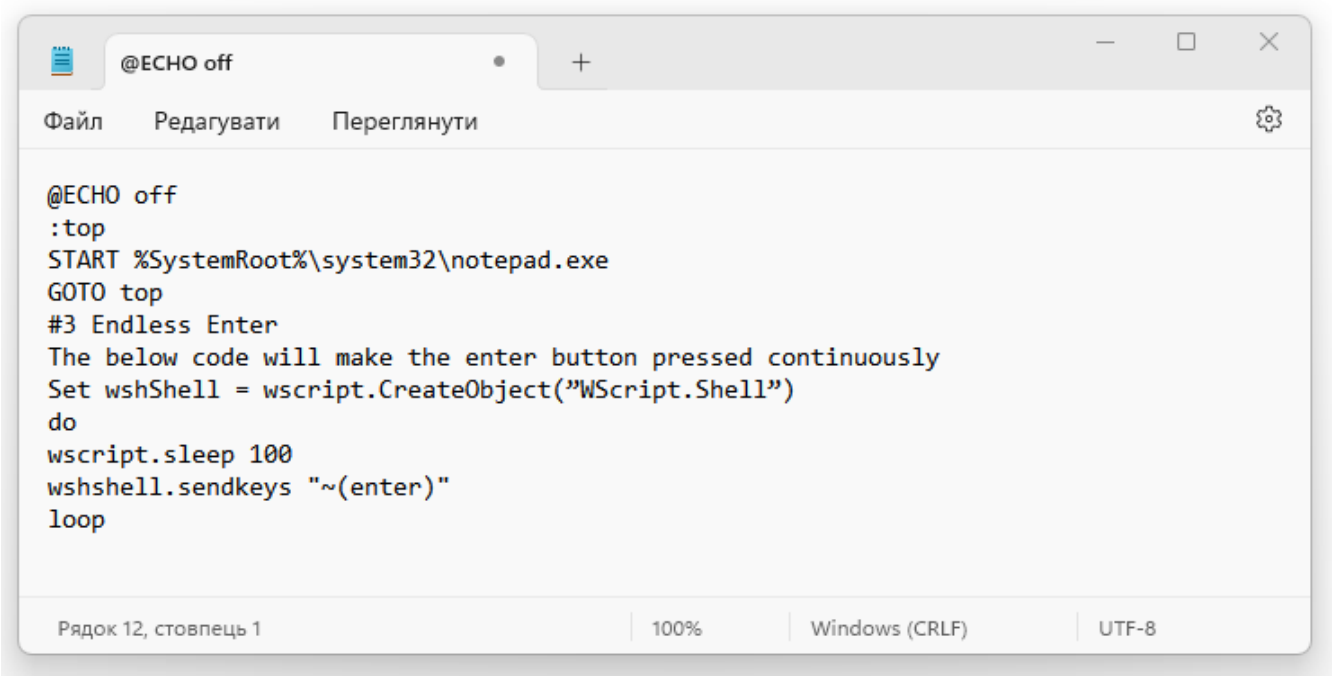


Рис. 8. Код вірусу для створення нескінченних Блокнотів

**4. Видалення ключових файлів Реєстру**

Це дуже небезпечний вірус, тому треба бути обережним перед його використанням. Цей вірус (рис. 8) не можна скасувати. Єдиний спосіб виправити вірус – знову перевстановити Windows.

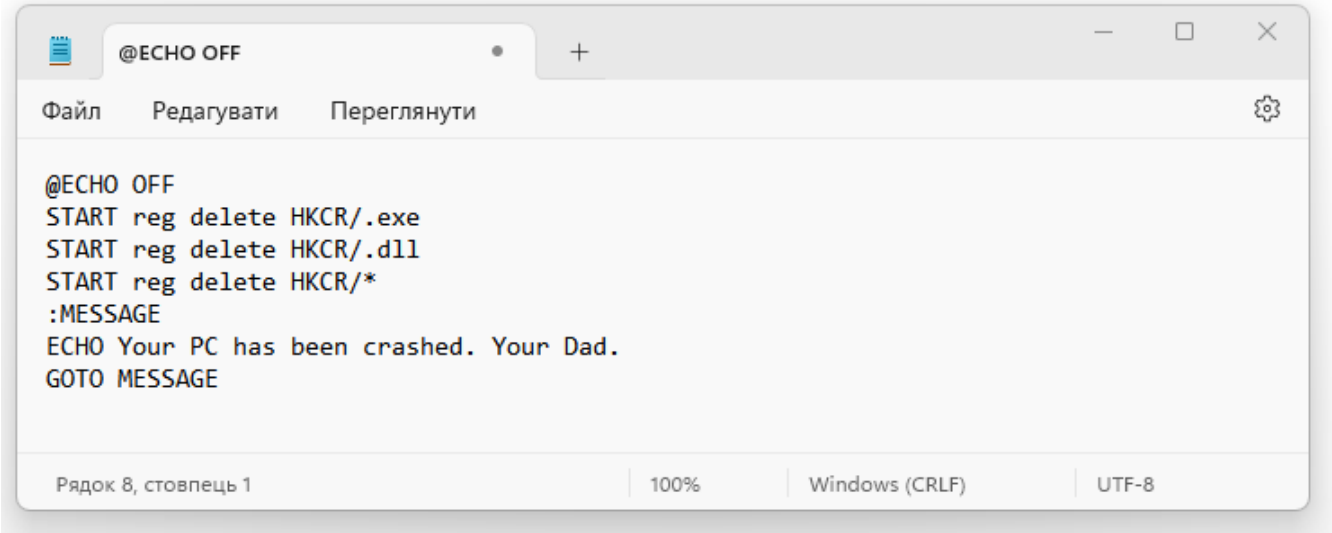


Рис. 9. Код вірусу для видалення ключових файлів Реєстру

**4. App Bomber** – вірус для створення нескінченної кількості програм.

Цей вірус (рис. 9) також дуже небезпечний. Він негайно заморозить комп’ютер, оскільки на екран буде з’являтися нескінченна кількість програм, що призведе до зависання або збою комп’ютера.

Таким чином, як бачимо, створення вірусів не потребує надто багато часу. Разом з тим шкода, заподіяна роботою таких вірусів є достатньо суттєвою.

**Виявлення простих вірусів у програмному коді**

Для виявлення простих вірусів у програмному коді можна використовувати різні методики та інструменти. Нижче наведено деякі з них [7–8]:

*Вірус сканери*: це спеціальні програми, які аналізують програмний код на наявність відомих вірусів. Деякі вірус сканери можуть також виявляти невідому шкідливе програмне забезпечення.

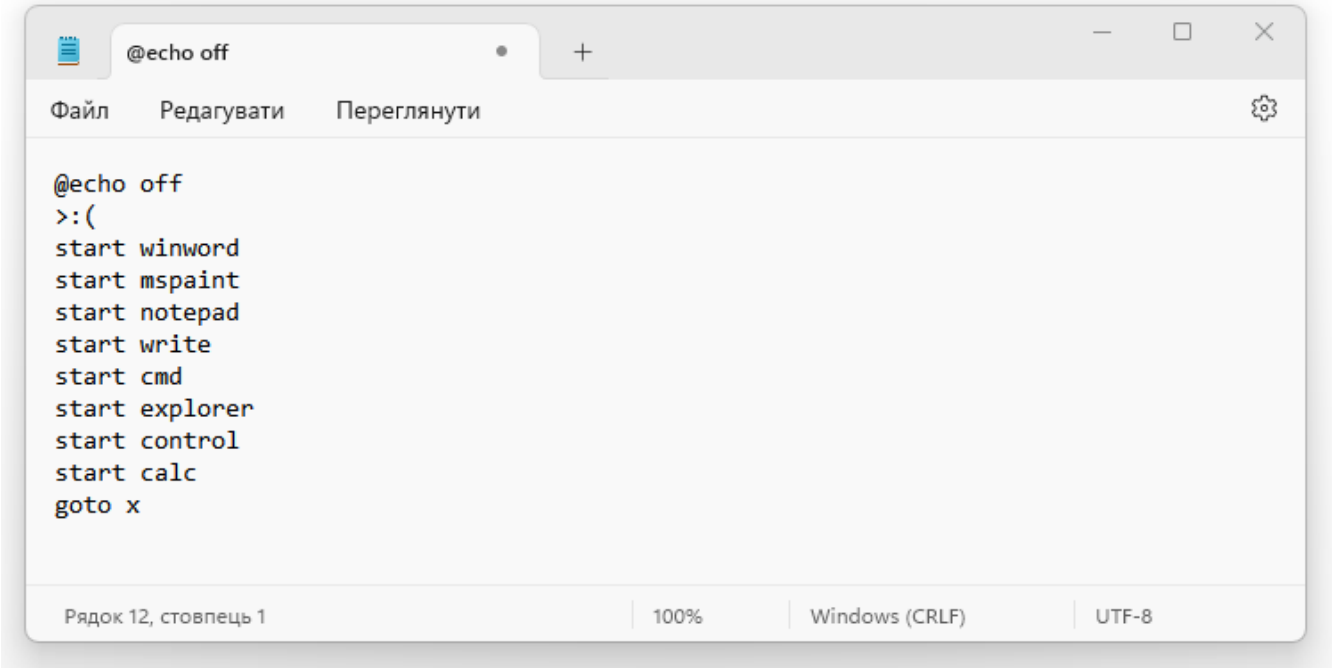


Рис. 9. Код вірусу для створення нескінченної кількості програм

*Проведення код-ревю*: це процес перегляду програмного коду з метою виявлення можливих вразливостей та шкідливого програмного коду. Цей процес може бути виконаний експертами з безпеки програмного забезпечення або використовувати автоматизовані інструменти для аналізу коду.

*Використання хеш-функцій*: хеш-функції можуть використовуватися для виявлення змін в програмному коді. Це може допомогти виявити шкідливі зміни, які можуть бути внесені в програмний код вірусом.

*Аналіз поведінки*: деякі програми можуть аналізувати поведінку програмного коду в реальному часі. Це може допомогти виявити шкідливу поведінку, таку як введення шкідливих команд або виконання небезпечних операцій.

*Використання евристичних методів*: евристичні методи можуть використовуватися для виявлення нових вірусів або змінених версій відомих вірусів. Ці методи можуть використовувати емпіричні правила та аналіз зразків вірусів для виявлення нових загроз.

Ці методи можуть бути використані для виявлення простих вірусів у програмному коді. Проте, важливо пам'ятати, що немає однієї універсальної методики, яка може виявити всі віруси у програмному коді. Тому, для надійного виявлення вірусів в програмному коді, можна використовувати комбінацію цих методів. Наприклад, можна поєднувати використання вірус сканерів з проведенням код-ревю та аналізом поведінки програмного коду.

Також варто зазначити, що при виявленні вірусів в програмному коді необхідно звертати увагу на контекст виявлення. Наприклад, можуть бути випадки, коли програмний код містить фрагменти, які мають вигляд вірусу, але насправді є безпечними. Тому, для визначення наявності вірусів в програмному коді, потрібно враховувати контекст виявлення та досвід експерта з безпеки програмного забезпечення.

В цілому, виявлення простих вірусів у програмному коді є важливим етапом в забезпеченні безпеки програмного забезпечення. Для ефективного виявлення вірусів можна використовувати різні методики та інструменти, а також комбінувати їх для досягнення кращих результатів.

## Висновки

У даній статті було розглянуто питання виявлення простих вірусів у програмному коді. Було зазначено, що віруси можуть завдати значної шкоди програмному забезпеченню та важливо попередити їхнє поширення. Для виявлення вірусів у програмному коді можна використовувати різні методики, такі як вірус сканери, статичний аналіз коду, аналіз поведінки програмного коду, та інші. Також було зазначено, що при виявленні вірусів в програмному коді важливо звертати увагу на контекст виявлення та досвід експерта з безпеки програмного забезпечення.

У цілому, виявлення вірусів у програмному коді є важливим етапом в забезпеченні безпеки програмного забезпечення та може допомогти запобігти шкоді, яку можуть завдати віруси.

## Перелік посилань

1. Сугоняк І.І., Марчук Г.В., Бобровнік С.О. Синтаксичний аналіз коду для системи дистанційного навчання програмування на мові C#. Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. Том 29 (68), Ч. 2, № 5, 2018. 65-71.

2. Muhammet Sahin and Serif Bahtiyar. 2021. A Survey on Malware Detection with Deep Learning. In 13th International Conference on Security of Information and Networks (SIN 2020). Association for Computing Machinery, New York, NY, USA, Article 34, 1–6. https://doi.org/10.1145/3433174.3433609

3. Sen, Sevil. (2015). A Survey of Intrusion Detection Systems Using Evolutionary Computation. 10.1016/B978-0-12-801538-4.00004-5.

4. С.Г. Семенов, С.Ю. Гавриленко, С.М. Глоба, О.С. Бабенко. Розробка системи виявлення комп'ютерних вірусів на основі нейронної мережі АРТ-1. Системи обробки інформації, 2015, випуск 10 (135). 126-129.

5. Albishry N, AlGhamdi R, Almalawi A, Khan AI, Kshirsagar PR, BaruDebtera. An Attribute Extraction for Automated Malware Attack Classification and Detection Using Soft Computing Techniques. Comput Intell Neurosci. 2022. Apr 25;2022:5061059. doi: 10.1155/2022/5061059. PMID: 35510059; PMCID: PMC9061036.

6. Six Ways To Create A Computer Virus (Using Notepad). By Pete Mitchell / October 16, 2022. https://techcult.com/create-a-computer-virus/

7. Войтович О. П. Особливості дослідження ознак шкідливого програмного забезпечення без наявності вихідних кодів / О. П. Войтович, В. О. Вітюк, В. А. Каплун // Інформаційні технології та комп'ютерна інженерія. - 2013. - № 3. - С. 4-9. - Режим доступу: http://nbuv.gov.ua/UJRN/Itki_2013_3_3.

8. С.М. Лисенко, Р.В. Щука. Аналіз методів виявлення шкідливого програмного забезпечення в комп'ютерних системах. Вісник Хмельницького національного університету, №2, 2020 (283). 101-107.

Надійшла: 03.03.2023 Рецензент: д.т.н., професор Вишнівський В.В.