НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА

ЗБІРНИК МАТЕРІАЛІВ

76-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ, АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ

ТОМ 1

14 травня – 23 травня 2024 р.

УДК 519.83

Г.В. Головко, к.т.н.,доцент
Студент групи 502-ТН С.І. Кутенний
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАХИСТУ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

В сучасному світі настає епоха цифрової трансформації і комп'ютерні інформаційні системи стають необхідною складовою успішної діяльності підприємств, технологічних розробок та розвитку кібербезпеки як науки. У цьому контексті безпека інформації стає одним з основних пріоритетів для організацій на всіх рівнях. Кібератаки, віруси та інші злочинні дії можуть призвести до серйозних фінансових збитків, погіршення репутації, викрадення інформації. Тому важко недооцінити важливість дослідження та розробки методів захисту комп'ютерних інформаційних систем від кібератак. [1]

Мета: Дослідження методів забезпечення захисту комп'ютерних інформаційних систем та розробка програмного засобу, для запобігання та усунення шкідливих вірусів, які можуть пошкодити чи зруйнувати роботу операційної системи.

Об'єкт дослідження: Джерела та види загроз комп'ютерних інформаційних систем.

Предмет дослідження Всі етапи розробки програмного засобу для протидії вірусам.

Розробка програмного забезпечення, яке буде складатись із зручного інтерфейсу, але включатиме ефективні функції для виявлення та усунення вірусного носія.

Для розробки продукту необхідно базуватись на операційній системі Windows, та VSCode, атакож мови Python. При проведені аналізу існуючої комп'ютерної інформаційної системи використати шкідливий файл, завантажений з VirusShare.com.

Призначення розробки - програмне забезпечення призначене для захисту операційної системи, а також пошуку шкідливих ПЗ в файлах та програмах.

Для реалізації поставленої мети сформульовані наступні завдання:

- дослідити класифікацію загроз;
- проаналізувати джерела загроз та їх способи втілення;
- створити програмний продукт на основі одного із засобів захисту;
- провести тестування пз.

Для системи безпеки необхідно орієнтувати заходи на:

- захист операційної системи від недозволеного доступу;
- контроль доступу для неповноважних користувачів;
- захист від вірусів та інших шкідливих програм;

- розуміння системи роботи вірусів та інших шкідливих атак.

Необхідно розглянути та проаналізовати види загроз комп'ютерних інформаційних систем, їх джерела, класифікацію та методи використання, а також буде створено таблицю з порівняльними характеристиками. До того ж, буде обрано окремий вид загроз – комп'ютерні віруси, і детальний опис кількох їхніх типів та порівняльний аналіз існуючих антивірусів. Для забезпечення безпеки буде написаний опис алгоритмів розпізнавання шкідливих ПЗ. Буде досліджено один із редакторів коду VS Code, його переваги та недоліки при написанні програмного забезпечення, а також функціональність та порівняння його зі ще одним інтегрованим середовищем розробки.

Важливу необхідно приділити процесу створення, налагодження та тестування антивірусного програмного засобу на базі існуючих сигнатур. Функціональності засобу буде достатньо аби завдяки процесу сканування віднайти файл із шкідливим змістом. Для розробки буде розглянуто архітектуру антивірусу та одну з моделей розробки життєвого циклу програмного забезпечення. Також необхідно описати тестування кінцевого продукту. Основні режими роботи, інтерфейс програми, рекомендації для впровадження та використанню засобу. Розроблений продукт дасть можливість сканувати щойно завантажуванні файли та сканувати операційну систему в цілому. Також, можливість занесення підозрілого документу чи програми в карантин для його подальшого ізолювання від інших «здорових» файлів.

Література

1. https://sites.google.com/site/zahistlokalnoiemerezi/zahist/kriptograficnij-zahist.