ТЕХНОЛОГІЇ РОЗРОБКИ АНТИВІРУСНИХ ПРОГРАМ

Станіщук К.А.
Національний авіаційний університет, Київ
Науковий керівник – Кучерява О.М., канд. фіз.-мат. наук

Під терміном «кібератака» розуміють замах на інформаційну безпеку комп'ютерної системи. Головною метою кібератак є порушення конфіденційності, цілісності та доступності електронних інформаційних ресурсів.

На сьогодні розроблено багато програмного забезпечення, яке забезпечує безпеку персонального комп'ютера, ноутбука, планшета або смартфона. Такі програмні засоби захисту зазвичай називають антивірусними програмами, метою яких є виявлення та видалення комп'ютерних вірусів і інших шкідливих програм.

Сучасні антивірусні програми включають в себе програмні модулі, кожен з яких виконує свою функцію, загальна дія яких складає антивірусний захист пристрою. Антивірусна програма «Zillya!» є програмним продуктом української антивірусної «Лабораторії Zillya!» [1]. Цей антивірус забезпечує захист від вірусів, троянських програм, шпигунських програм, руткітів, рекламних програм, а також невідомих загроз за допомогою проактивного захисту. Залежно від того, яка загроза нейтралізується, антивірус здійснює реактивний захист – захист від відомих загроз, або проактивний захист – захист від невідомих вірусів.

Принцип роботи антивірусної програми «Zillya!» полягає в наступному: після виявлення шкідливого файлу, що був заражений вірусом, користувачеві надається можливість вибрати, що саме він хоче зробити: спробувати видалити з зараженого файлу шкідливі ділянки коду, не видаляючи файл; видалити інфікований файл; якщо ж цей файл містить важливу інформацію, то його можна помістити до карантину, а потім звернутися до фахівця; нічого не робити, якщо користувач впевнений, що файл не заражений.

Антивіруси захищають комп'ютер постійно, запускаючись разом із запуском операційної системи: контролюють оперативну пам'ять і файлову систему комп'ютера, перевіряють на наявність вірусів дані, що можуть потрапити в комп'ютер через змінні накопичувачі USB, слідкують за програмами, встановленими на комп'ютер, з метою виявлення шкідливої активності, виконують блокування проникнення спам-повідомлень на комп'ютер користувача, тощо. Якщо вірус буде знайдено, антивірусна програма неодмінно дасть інформацію про це.

Основні складові сучасної антивірусної програми «Zillya!» виконують всі функції антивірусного захисту. Брандмауер відстежує будь-які спроби додатків отримати доступ до мережі, що дозволяє захистити систему від спроб отримати до неї доступ ззовні. Блокування доступу до небезпечних сайтів у браузері забезпечує WEB-фільтр. Також є різні аналізатори, серед яких, наприклад, евристичний, перевіряє коди файлів, чи мають вони шматочки коду, які були раніше помічені в антивірусних програмах. Сигнатурний аналізатор перевіряє файли на відповідність базі вірусних сигнатур. Поведінковий аналізатор сканує

та аналізує програми на можливість появи у них шкідливої поведінки. USB-фільтр забезпечує контроль підключення накопичувачів до USB-портів. Фільтр e-mail перевіряє всі повідомлення, як вхідні так і вихідні на наявність шкідливих об'єктів. Антиспам налаштовує так звані чорні списки сайтів та електронних поштових адрес, де були помічені СПАМ-розсилки. Батьківський контроль дозволяє контролювати відвідування неповнолітніми користувачами комп'ютерів різних сайтів. Антифішинг дозволяє уникнути попадання на сайти, які використовують дані користувача задля незаконного збагачення. Самозахист виключає можливість відключення захисту комп'ютера вірусами.

Для розробки антивірусних програм використовують евристичний аналізатор. Робота евристичного аналізатора заснована на пошуку характерних для вірусів і шпигунських програм особливостей (фрагментів програмного коду, визначених ключів реєстру, файлів і процесів). Крім того, евристичний аналізатор намагається оцінити ступінь схожості досліджуваного об'єкта на відомі віруси [2].

Евристичний аналіз – це метод виявлення шкідливих програм, при якому антивірусна програма контролює всі дії, що виконуються програмою. В ході евристичного аналізу відслідковуються потенційно небезпечні дії, характерні для вірусів і шкідливих програм інших типів. Контролюючи дії перевірених програм, евристичний аналізатор сучасних антивірусів здатний виявити нові, невідомі віруси ще до того, як ці віруси почали діяти. Проте, евристичний аналіз не дає повної гарантії виявлення будь-яких нових вірусів. Крім того, евристичний аналізатор може прийняти «нешкідливу» програму за шкідливу. Це відбувається в тих випадках, коли програма виконує будь-які дії, характерні для вірусів або шкідливих програм іншого типу [3].

На даний момент антивірусне програмне забезпечення «Zillya!» розробляється в основному для операційної системи (ОС) сімейства Windows від компанії Microsoft, що викликано великою кількістю шкідливих програм саме під цю платформу. На даний момент було випущено антивірус «Zillya! Mobile Antivirus» для ОС Android. Це викликано початком розповсюдження шкідливих програм під цю платформу, а це, в свою чергу, викликане великою популярністю цієї ОС.

Евристичний аналізатор «Zillya!» – це інтелектуальний модуль захисту. На основі «коду» програмного забезпечення комп'ютера користувача він може визначити вірусне походження програми та знешкодити її, навіть, якщо така програма не була раніше включена до списку шкідливих.

Список використаних джерел:

1. Zillya! [Електронний ресурс]. – Режим доступу: https://zillya.ua/

2. Эвристический анализатор [Електронний ресурс]. – Режим доступу: AVZ https://z-oleg.com/secur/avz_doc/term_ha.htm

3. Эвристический анализ. [Електронний ресурс]. – Режим доступу: https://www.dialognauka.ru/support/golossary/4636/