УДК 004.058

КОМП'ЮТЕРНІ ВІРУСИ ТА ПРОТИДІЯ ЇМ

Омелечко А.А., студ. гр. АГ-181
Гур'єв В.І., к.т.н., доцент
Чернігівський національний технологічний університет

Комп'ютерний вірус - це невелика програма, що написана програмістом високої кваліфікації. Основна відмітна характеристика комп'ютерного вірусу - здатність до самопоширення. Подібно біологічному вірусу для життя й розмноження він активно використає зовнішнє середовище - пам'ять комп'ютера, операційну систему. На сьогоднішній день відомо понад 50 тис. комп'ютерних вірусів.

В даний час не існує єдиної системи класифікації і іменування вірусів (хоча спроба створити стандарт була зроблена на зустрічі CARO у 1991 році).

Прийнято розділяти віруси:

- по вразливих об'єктах (файлові віруси, завантажувальні віруси, скриптові віруси, макровіруси, віруси, що вражають вихідний код);
- по вразливим операційним системам і платформам (DOS, Microsoft Windows, Unix, Linux);
- за технологіями, використовуваними вірусом (поліморфні віруси, стелс-віруси, руткіти);
- за мовою, на якій написано вірус (асемблер, високорівнева мова програмування, скриптова мова та ін);
- по додатковій шкідливої функціональності (бекдори, кейлоггери, шпигуни, ботнети та ін).

Основними джерелами вірусів є:

- диск, на якому знаходяться заражені вірусом файли;
- комп'ютерна мережа, в тому числі система електронної пошти та Internet;
- жорсткий диск, на який потрапив вірус в результаті роботи з зараженими програмами;
- вірус, що залишився в оперативній пам'яті після попереднього користувача.

Основними ранніми ознаками зараження комп'ютера вірусом є:

- зменшення обсягу вільної оперативної пам'яті;
- сповільнення завантаження та роботи комп'ютера;
- незрозумілі (без причин) зміни у файлах, а також зміни розмірів та дати останньої модифікації файлів;
- помилки при завантаженні операційної системи;
- неможливість зберігати файли в потрібних каталогах;
- незрозумілі системні повідомлення, музикальні та візуальні ефекти і т.д.

Декілька фактів про віруси:

1. Найчастіше збій операційної системи комп'ютера відбувається через віруси, так як віруси не тільки завдають шкоди системі але можуть бути і не сумісні з системою комп'ютера, що і призводить до збоїв.

2. Віруси можуть створювати копії себе, впроваджуватися в інші програми, видаляти файли, блокувати користувача, поширяться по всім носіям (флешки, харди, зовнішні харди і т.п), які ми використовуємо і багато іншого.

3. Один з найзнаменитіших вірусів називається «Чорна п'ятниця». Цей шкідливий вірус пробирається в комп'ютер, але спрацьовує не відразу. А в той день, коли п'ятниця випадає на 13 число.

4. Найбезпечнішим вірусом вважається Blaster. Він отримав широку популярність завдяки численним згадуванням у ЗМІ. Ніякої небезпеки вірус не несе. На екрані зараженого комп'ютера просто іноді вискакує напис «Біллі, як це можливо? Припини обманювати людей і заробляти гроші». Присвячений він Біллу Гейтсу. Творцеві Blaster не пощастило. Джеффрі Лі Парсон отримав півтора роки в'язниці, за те, що знущався над Біллом Гейтсом.

5. Найбільш руйнівним вважається вірус з романтичною назвою «I Love You». Листи з таким текстом приходили людям по всьому світу, починаючи з 2000 року. За любовним визнанням переховувався комп'ютерний вірус, який завдав шкоди світовій економіці в 10 млрд євро. Він вразив більше 3 мільйонів комп'ютерів на планеті, ставши ще й найдорожчим за всю історію.

Найнебезпечніші комп'ютерні віруси 2000-х років:

- «Nimda», 2001 рік, вірус з правами адміністратора.
- «My Doom», 2004 рік, лідер за швидкістю зараження Мережі.
- Conficker, 2008 рік, невловимий і дуже небезпечний.
- «Win32 / Stuxnet», 2010 рік, перший вірус, створений для промислових систем.

Отже, що таке комп'ютерний вірус ми розібрали. Але постає питання: Як їм пропидіяти? Адже ніхто не застрахований від віруса. На даний момент існує безліч антивірусних програм, що використовуються для запобігання попадання вірусів в ПК. Однак немає гарантії, що вони зможуть впоратися з новітніми розробками. Фахівці підрахували, що антивіруси застарівають в середньому за 1-2 дні. Тому близько 15%

вірусів проникають у комп'ютери, незважаючи на антивірусний захист. Хакери придумують все нові й нові способи заразити техніку.

Антивірус - програмний засіб, призначений для боротьби з вірусами. Антивіруси можна розділити на дві великі категорії:

• **Призначені для безперервної роботи** - до цієї категорії відносяться засоби перевірки при доступі, поштові фільтри, системи сканування трафіку Інтернет, інші засоби, що сканують потоки даних.

• **Призначені для періодичного запуску** - різного роду засобу перевірки за запитом, призначені для однократного сканування певних об'єктів. До таких засобів можна віднести сканер на вимогу файлової системи в антивірусному комплексі для робочої станції, сканер на вимогу поштових скриньок і загальних папок в антивірусному комплексі для поштової системи.

Як показує практика, запобігти виникненню проблеми набагато простіше, ніж намагатися згодом неї вирішити. Саме тому сучасні антивірусні комплекси здебільшого мають на увазі безперервний режим експлуатації. Проте, засобу періодичної перевірки набагато ефективніше при боротьбі з наслідками зараження й тому не менш необхідні.

Але також можна захиститись від віруса без допоміжних програм націлених на захист. До загальних засобів, що допомагають запобігти зараженню та його руйнівних наслідків належать:

• резервне копіювання інформації (створення копій файлів і системних областей жорстких дисків);

• уникнення користування випадковими й невідомими програмами. Найчастіше віруси розповсюджуються разом із комп'ютерними вірусами;

• перезавантаження комп'ютера перед початком роботи, зокрема, у випадку, якщо за цим комп'ютером працювали інші користувачі;

• обмеження доступу до інформації, зокрема фізичний захист дискети під час копіювання файлів із неї.

Список використаних джерел

1. Комп'ютерні віруси та їх основна характеристика [Електронний ресурс] // Режим доступу до ресурсу - https://sites.google.com/site/diresideinaction/komp-uterni-virusi-ta-ieh-osnovna-harakteristika.
2. Комп'ютерні віруси та антивіруси: погляд програміста [Електронний ресурс] // Режим доступу до ресурсу - https://books.google.com.ua/books?id=9z7mCQAAQBAJ&pg=PA5&lpg=PA5&dq=вируси+та+антивируси&source=bl&ots=rKPupAdx7j&sig=ACfU3U1Ftw9VY1FG-M_vqinEQH4dq_tVlw&hl=ru&sa=X&ved=2ahUKEwj4woHy1JvhAhUx4KYKHcdTCBw4ChDoATACegQICRAB#v=onepage&q=вируси%20та%20антивируси&f=false.
3. Методичні матеріали з інформатики [Електронний ресурс] // Режим доступу до ресурсу - https://www.ua5.org/virus/
4. Довідник цікавих фактів та корисних знань [Електронний ресурс] // Режим доступу до ресурсу - https://dovidka.biz.ua/tsikavi-fakti-pro-komp-yuterni-virusi/

УДК 004.056.55

ЗАДАЧА РОЗПІЗНАВАННЯ ОБРАЗІВ В ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ ВИЯВЛЕННЯ КІБЕРАТАК

Петренко Т.А., ст. викладач кафедри кібербезпеки та математичного моделювання,
Коротка Г.М., студ.гр. КБ-161
Чернігівський національний технологічний університет

Існує багато задач, які вирішують системи штучного інтелекту: задачі розпізнавання образів, розуміння тексту, створення експертних систем, доведення теорем, моделювання процесів і явищ, діагностики та постановки діагнозу. Проте, однією з основних є задача розпізнавання образів.

Розпізнавання образів (об'єктів, сигналів, явищ чи процесів) – задача, яку людині доводиться вирішувати практично кожну секунду. Для вирішення цієї задачі людина застосовує великі ресурси свого мозку, включаючи одночасно біля 10 – 12 млрд. нейронів. Саме це дає можливість людям миттєво впізнавати один одного, з великою швидкістю читати печатні та рукописні тексти, безпомилково водити автомобілі у складному вуличному трафіку, здійснювати відбраківку деталей на конвеєрі, розгадувати коди та інше.

Розпізнавання являє собою задачу перетворення вхідної інформації, в якості якої доречно розглядати деякі параметри, ознаки розпізнаваних образів, в вихідну, що представляє собою висновок про те, до якого класу належить розпізнаваний образ. Розпізнавання використовуються в різноманітних сферах життя людини: у медицині, металургії, банківській справі, інформаційних технологіях, біометрії, охоронній системі, тощо. У кожній галузі розпізнавання виконує певну роль. Такі системи набули широкого розповсюдження і в кібербезпеці під час розпізнавання загроз, аномалій та кібератак в інформаційних системах на основі аналізу даних що зчитуються з певних датчиків інформаційної системи (службового програмного забезпечення, операційних систем, апаратного забезпечення комп'ютерів та мереж, тощо). Крім того, методи розпізнавання застосування і в робототехніці, так як роботи повинні безпосередньо сприймати зовнішній світ, і, відповідно, мати пристрої машинного зору.