УДК 621.34

С.Г. Семенов, С.Ю. Гавриленко, С.М. Глоба, О.С. Бабенко

Національний технічний університет «Харківський політехнічний інститут», Харків

РОЗРОБКА СИСТЕМИ ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ ВІРУСІВ НА ОСНОВІ НЕЙРОННОЇ МЕРЕЖІ АРТ-1

У роботі пропонується програмна модель евристичного аналізатора на базі нейронної мережі АРТ-1 для ідентифікації стану комп'ютерної системи в умовах впливів комп'ютерних вірусів.

Ключові слова: *антивірусні програми, сигнатурний метод, евристичний метод, нейронна мережа АРТ-1.*

Вступ

Визначення проблеми. Широке застосування комп'ютерної техніки призвело до появи програм-вірусів. Вірусні атаки набули широкого поширення і здатні не тільки завдати величезної шкоди інформації, яка зберігається та обробляється але повністю вивести з ладу комп'ютерну систему. Інформаційні технології стрімко розвиваються, оновлюється програмне забезпечення та апаратні засоби, мережеві атаки постійно змінюються, їх кількість неухильно зростає і остаточно вирішити дану проблему неможливо. На протидію вірусам виділяється велика кількість ресурсів. Однак збитки від шкідливих програм досягають десятків мільярдів доларів. Саме тому актуальною темою являється розробка ефективних методів та технологій протидії комп'ютерним вірусам [1].

Аналіз літератури [2, 3] показав, що існують два основних методи роботи антивірусних програм – сигнатурний та евристичний. Сигнатурний метод побудований на основі сканування та порівняння з еталоном (маскою). Маска містить набір шкідливих команд, характерних для даного типу вірусу.

Евристичний аналіз нерідко використовується спільно з скануванням для пошуку вірусів які шифруються і поліморфних вірусів. Дуже часто евристичний аналіз дозволяє виявляти раніше невідомі інфекції, хоча лікування в цих випадках зазвичай виявляється неможливим. Якщо евристичний аналізатор повідомляє, що файл або завантажувальний сектор, можливо, заражений вірусом, користувачеві необхідно провести додаткову перевірку за допомогою самих останніх версій антивірусних програм-сканерів.

Евристичні методи базуються на основі використання правил або статистичних методів: системи на основі ваг і правил, кластерний аналіз, узгоджені евристики, експертні системи, нейронні мережі.

Проведені дослідження показали, що одним з перспективних напрямків евристичного аналізу комп'ютерних вірусів є використання саме нейронних мереж. Штучні нейронні мережі − математичні моделі, а також їхня програмна та апаратна реалізація, побудовані за принципом функціонування біологічних нейронних мереж − мереж нервових клітин живого організму.

Нейронні мережі не програмуються в звичайному розумінні цього слова, вони навчаються. Здатність до навчання є фундаментальною властивістю мозку. Процес навчання може розглядатися як визначення архітектури мережі і налаштування ваг зв'язків для ефективного виконання спеціальної задачі. Нейромережа налаштовує ваги зав'язків в залежності від наявною навчальної множини. Властивість мереж навчатися на прикладах робить їх більш привабливими в порівнянні із системами, які функціонують згідно визначеній системі правил, сформульованої експертами [4 – 7].

Мета даної статті –дослідження методів антивірусного захисту та розробка системи виявлення комп'ютерних вірусів на основі нейронної мережі АРТ-1.

Результати досліджень

Мережа АРТ являє собою векторний класифікатор. Вхідний вектор класифікується в залежності від того, на яку з множини образів, раніше запам'ятовуваний, він схожий. Своє класифікаційне рішення мережа АРТ виражає в формі збудження одного з нейронів розпізнавального прошарку. Якщо вхідний вектор не відповідає жодному із запам'ятовуваних образів, створюється нова категорія за допомогою запам'ятовування образу, ідентичного новому вхідному вектору. Якщо визначено, що вхідний вектор схожий на один з раніше запам'ятовуваних векторів з точки зору певного критерію схожості, запам'ятовуваний вектор буде змінюватися (навчатися) під впливом нового вхідного вектору таким чином, щоб стати більш схожим на цей вхідний вектор [9].

Запам'ятовуваний образ не буде змінюватися, якщо поточний вхідний вектор не виявиться досить схожим на нього. Таким чином вирішується дилема стабільності-пластичності. Новий образ може створювати додаткові класифікаційні категорії, однак новий вхідний образ не може примусити змінитися існуючу пам'ять. Розроблено кілька видів нейромереж на основі адаптивної резонансної теорії, зокре-

ма, мережа АРТ−1 призначена для роботи із двійковими вхідними зображеннями або векторами. Архітектура нейронної мережі АРТ−1 показана на рис. 1.

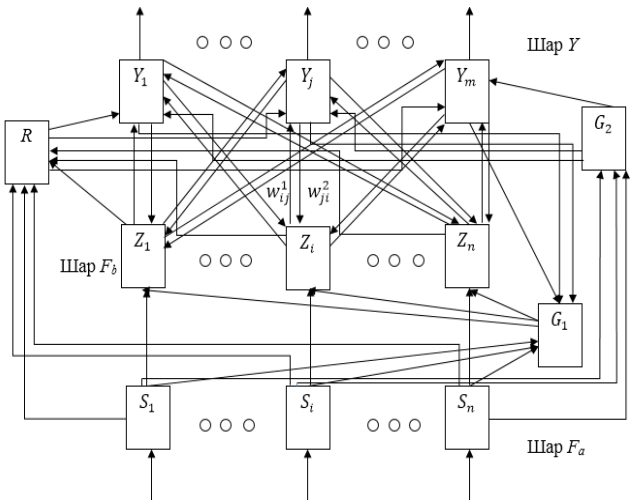

Рис. 1. Архітектура нейронної мережі АРТ−1

Архітектура мереж АРТ−1 має управляючі елементи G_1 та G_2 G_2, що забезпечують керування процесом функціонування [5]. На рис. 1 через наявність великої кількості зв'язків між Z- та Y-шарами елементів наведено позначення тільки однієї узагальненої пари ваг w_{ij}^1 , w_{ji}^2 зв'язків між інтерфейсними нейронами та розпізнавальними нейронами. Більшість зв'язків, наведених на рис. 1., є збудливими: від вхідного шару елементів F_a до нейронів R, G_1, G_2 та F_b − шару, від нейронів G_1, G_2 відповідно до нейронів шарів F_b та Y. Гальмуючі сигнали передають тільки множини зв'язків від інтерфейсних елементів до R-нейрона, від R-нейрона до Y-нейронів та від Y-нейронів до елемента G_1. Всі зв'язки мережі АРТ−1 передають тільки бінарні сигнали 0 або 1. Кожний елемент у інтерфейсному або Y -шарі мережі АРТ-1 має три джерела вхідних сигналів. Довільний інтерфейсний елемент $Z_i \left(i = \overline{1,n}\right)$ може одержувати сигнали від елементів S вхідного шару, та елементів Y-шару й від нейрона G_1. Аналогічно елемент Y_j $\left(j = \overline{1,m}\right)$ може одержувати сигнали від інтерфейсних елементів, нейронів R та G_2 . Для переводу нейронів інтерфейсного або розпізнавального шарів в активний одиничний стан необхідна наявність вхідних збудливих сигналів із двох джерел [7].

Якщо знайдений прототип з певною точністю, що задається спеціальним параметром подібності, відповідає вхідному процесу, то він модифікується, щоб стати більш схожим на пред'явлений процес. Коли вхідний процес недостатньо подібний жодному з наявних прототипів, то на його основі створюється новий клас. Це можливо завдяки тому, що мережа має велике число надлишкових або нерозподілених елементів, які не використовуються доти, поки в цьому немає потреби (якщо немає нерозподілених нейронів, то вхідне зображення не викликає реакції мережі) [7].

Нейронні мережі АРТ – динамічні об'єкти, які описуються системами звичайних диференціальних рівнянь, тому їх навчання в загальному випадку досить трудомістким. Однак моделі мереж АРТ можуть бути спрощені, якщо припустити, що зміна вихідних сигналів нейронів відбувається багато швидше, ніж зміна вагових векторів їх зв'язків. Тому в нейромережах теорії адаптивного резонансу можна вважати, що після виділення для навчання прийнятного Y-елемента (настанні резонансу між пред'явленими і зберігається в пам'яті зображенням), вихідні сигнали всіх нейронів залишаються незмінними протягом тривалого періоду часу, протягом якого відбуваються зміни ваг зв'язків.

Для вирішення даної задачі була розроблена модель евристичного аналізатору на базі нейронної мережі АРТ-1.

Вхідні дані для навчання нейронної мережі сформовані на основі статистичних параметрів мережі та представляють собою параметри мережевої активності, а саме:

num_failed_logins – кількість невдалих спроб входу;

num_root – число спроб входу *root*-користувача, або адміністратора;

src_bytes – кількість даних (в байтах) від джерела до адресата*;*

dst_bytes – кількість даних (в байтах) від адресата до джерела*;*

num_file_creations – число операцій створення файлу*;*

num_shells – число підказок оболонки;

num_access_files – число операцій з файлами доступу.

Вхідні вектори для навчання та розпізнавання однакові за структурою, представляють послідовність параметрів описаних вище (рис. 2).

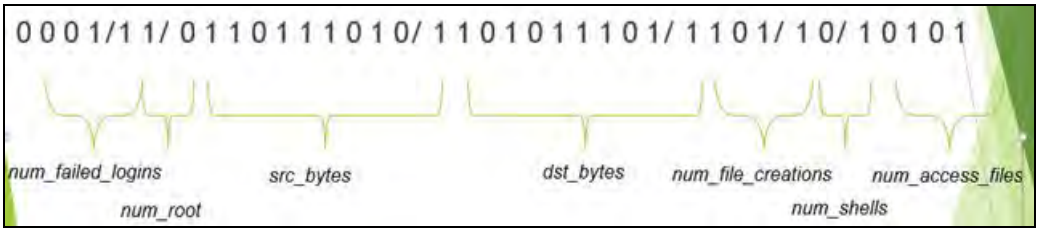

Рис. 2. Структура вхідного вектору

Процес навчання нейронної мережі наведено на рис. 3 та включає в себе такі етапи: 1) подавання вхідних даних в двійковому форматі; 2) аналіз вхідного вектора системою; 3) виконання внутрішньої логіки нейронної мережі, заснованої на значеннях ваг зв'язків нейронів між собою; 4) проведення розрахунку помилки стосовно коефіцієнта подібності, та прийняття рішення щодо навченості мережі, або підстроювання ваг і обробка наступного вхідного вектора.

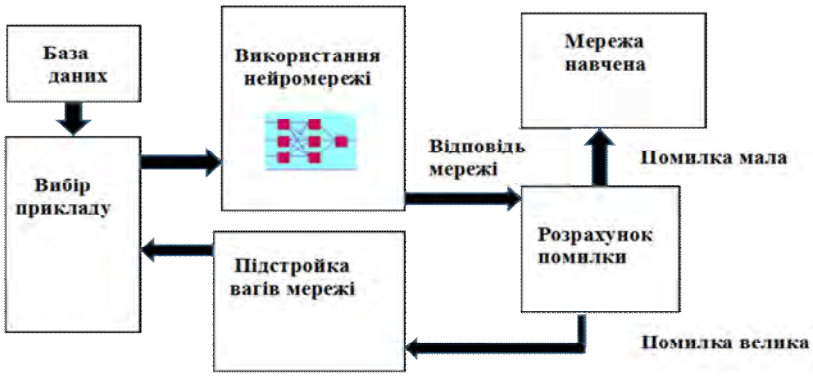

Рис. 3. Процес навчання нейронної мережі

В алгоритмі навчання нейронної мережі прийняті такі позначення: m – максимальне число розпізнавальних елементів в Y-шарі або максимальне число розпізнаваних класів вхідних зображень; n – число компонент у вхідному векторі або зображенні; S^k – n-мірний бінарний вхідний вектор; k = [1, q]; q – число навчальних вхідних векторів; $U_{вихZ}$ – n-мірний бінарний вектор вихідних сигналів інтерфейсного шару елементів; ||X|| – норма вектору X; w_1 – вага зв'язку від інтерфейсного елемента Z_j до елементу Y_j, діапазон допустимих початкових значень такий:

$$0 < w < 1/(L-1+n)$$

а рекомендоване початкове значення: $1/(1+n)$; w_2 – вага зв'язку від елементу Y_j до елементу Z_j, рекомендоване початкове значення: $w^2 = 1$; p – параметр подібності між пред'явленими вектором і вектором ваг переміг нейрона Y-шару, діапазон допустимих значень параметра такий: $0 < p \le 1$, а рекомендоване значення $p \approx 0.9$.

Крок 1. Ініціюються параметри L, p і ваги.

Крок 2. Поки не виконуються умови зупинки, реалізуються кроки 3 – 14.

Крок 3. Для кожного навчального вхідного вектору виконуються кроки 4 – 13.

Крок 4. Здається нульова активація всіх розпізнавальних елементів Y-шару:

$$U_{вих} = 0, \quad j = \overline{1,m}.$$

Вхідним навчальним вектором встановлюється активація S-елементів вхідного шару:

$$U_{вихSi} = S_j^k, \ i = \overline{1,n}.$$

Крок 5. Обчислюється норма вектору вихідних сигналів вхідного шару:

$$\|U_{вихS}\| = \|S^k\| = \sum_{i=1}^{n} S_j^k .$$

Крок 6. Формують вхідні і вихідні сигнали елементів інтерфейсного шару:

$$U_{вхZi} = U_{вихSi}, U_{вихZi} = U_{вхZi}, i = \overline{1,n}.$$

Крок 7. Для кожного незагальмованого Y-нейрона, тобто у якого вихідний сигнал не дорівнює –1, розраховуються його вхідний і вихідний сигнали:

$$U_{вхYj} = U_{вихYj} = n\sum_{i=1}^{n} w^1 U_{вихZi} .$$

Крок 8. Поки не знайдений Y-нейрон, ваговий вектор якого при заданому параметрі подібності p відповідає вхідному вектору S^k виконуються кроки 9 – 12.

Крок 9. У Y-шарі визначається нейрон Y_J який задовольняє умові

$$U_{вихYj} \ge U_{вихYj}, j = 1,m .$$

Якщо таких нейронів декілька, то вибирається елемент з найменшим індексом. Якщо $U_{вихYj} = -1$, то всі елементи загальмовані і вхідне зображення не може бути класифіковане.

Крок 10. Розраховуються вихідні сигнали Z-елементів:

$$U_{вихZi} = U_{вихSi} w_{Ji}^2 .$$

Крок 11. Обчислюється норма вектору вихідних сигналів інтерфейсного шару:

$$\|U_{вихZ}\| = \sum_{i=1}^{n} U_{вихZi} .$$

Крок 12. Перевіряється умова на можливість навчання виділеного Y-нейрона:

якщо $\|U_{вихZ}\| / \|S^k\| < p$, то $U_{вихYj} = -1$, тобто загальмовується елемент Y_J і продовжується виконання з кроку 9;

якщо $U_{вихZ} / \|S^k\| \ge p$, то перехід до кроку 13.

Крок 13. Адаптуються ваги зв'язків елемента Y_J:

$$w_{iJ}^1 = LU_{вихZi} / (L-1+\|U_{вихZ}\|), w_{Ji}^2 = U_{вихZi}, i = 1,n.$$

Крок 14. Перевіряються умови зупину. Умовами зупину можуть бути: відсутність змін ваг мережі, досягнення заданого числа епох і т.д. Якщо умови зупинки не виконуються, то перехід до кроку 2 алгоритму, інакше – до кроку 15.

Крок 15. Зупинка.

Результати евристичного аналізатора на основі нейронної мережі АРТ-1 можна аналізувати опираючись на дані, які представляються програмою шляхом логування. Атаки знайдені за допомогою нейронної мережі будуть відображені у файлі *logs.log*.

Для можливості повної конфігурації нейронної мережі, визначення файлу для базових знань, визначення файлу для вхідних даних, повної конфігурації процесу логування, рівнів логування у проекті створено два файли *config.properties* та *log4j.properties*. Перший файл *config.properties* містить налаштування для нейронної мережі. Другий файл *log4j.properties* містить повні налаштування фреймворку призначеного для логування проекту. Нейронна мережа працює безперервно та з певною періодичністю обробляє дані, які приходять зі сторонньої системи. Періодичність також налаштовується в конфігураційному файлі, значення задається у мілісекундах та має ключ *file.reading.timeout*. В процесі роботи евристичний аналізатор обробляє вхідні дані за алгоритмом, визначеним архітектурою нейронної мережі АРТ-1, визначає атаки та їх модифікації на основі попередньо навчених атак. Опираючись на отримані знання в процесі навчання та аналізуючи нові вхідні дані нейронна мережа поповнює свої знання безперервно.

Результати роботи виводяться в двох напрямках, у консоль, з якої було відкрито програму та файл логування, який знаходиться по відносному шляху *\logs\logs.log*. Консольний варіант результатів зображено на рис. 4.

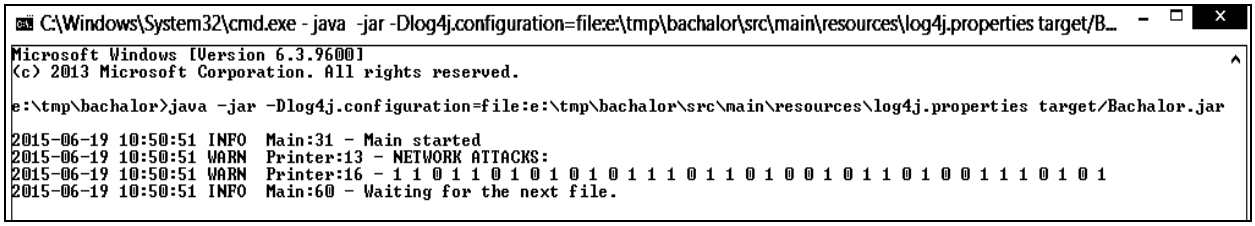

Рис. 4. Результати знаходження мережевої атаки

Висновки

В роботі проаналізовано методи побудови антивірусних програм. Розглянуто методи побудови евристичних сканерів на базі нейронної мережі АРТ-1. Вхідні дані для навчання нейронної мережі сформовані на основі статистичних параметрів мережі та представляють собою параметри мережевої активності. Розроблено програмну модель евристичного аналізатора на базі нейронної мережі АРТ-1 та проведено тестування розробленої системи виявлення комп'ютерних вірусів.

Список літератури

1. Гошко С.В. Технологии борьбы с компьютерными вирусами / С.В. Гошко. – М.: Солон-Пресс, 2009. – 352 с.

2. Джон Сноу. Вирус на блюдечке [Електронний ресурс].– Режим доступу: https://xakep.ru/2002/02/18/14534/.

3. Матвеев И.В. Классификация компьютерных вирусов. Примеры вирусов [Електронний ресурс] / И.В. Матвеев. – Режим доступу: http://dom8a.ru/seminar-ib/05.06.2014/matveev/paper.pdf.

4. Горбань А.Н. Нейронные сети на персональном компьютере / А.Н. Горбань, Д.А. Россиев. – Н-ск: Наука, 1996. – 276 с.

5. Основи нейрокомп'ютингу: навчально-методичний посібник / В.Д. Дмитрієнко, О.Ю. Заковоротний, В.І. Носков, М.В. Мезенцев. – Х.: НТМТ, 2014. – 140 с.

6. Круг П.Г. Нейронные сети и нейрокомпьютеры / П.Г. Круг. – М.: МЭИ, 2002. – 176 с.

7. Оссовский С. Нейронные сети для обработки информации / С. Осовский. Пер. с польск. И.Д. Рудинского. – М.: Финансы и статистика, 2002. – 344 с.

Надійшла до редколегії 20.08.2015

Рецензент: д-р техн. наук, проф. Г.А. Кучук, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

РАЗРАБОТКА СИСТЕМЫ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ НА ОСНОВЕ НЕЙРОННОЙ СЕТИ АРТ-1

С.Г. Семенов, С.Ю. Гавриленко, С.Н. Глоба, О.С. Бабенко

В работе предлагается программная модель эвристического анализатора на базе нейронной сети АРТ-1 для определения состояния компьютерной системы в условиях воздействия компьютерных вирусов.

Ключевые слова: *антивирусные программы, сигнатурный метод, эвристический метод, нейронные сети, АРТ-1.*

DEVELOPMENT OF COMPUTER VIRUSES DETECTION SYSTEM BASED ON ART-1 NEURAL NETWORK

S.G. Semenov, S.Y. Gavrilenko, S.M. Globa, O.S. Babenko

Nowadays computer viruses become stronger and try to hide themselves deeper in order to complicate virus detection or even get round of it. This article represents program model of heuristic analyzer based on the ART-1 neural network intended to determine status of the computer system while being under viruses attack. Architecture of the neural network allows to train it with new and modified attacks just in runtime, while scanning.

Keywords: *antivirus software, signature-based method, a heuristic method, neural network, ART-1.*