УДК 004.056.53
Т.Ф. Скумін, Р.М. Стасишин
Тернопільський національний економічний університет, Україна

ІНТЕЛЕКТУАЛЬНА СИСТЕМА КІБЕРЗАХИСТУ

T.F. Skumin, R.M. Stasyshyn

INTELLIGENT CYBER DEFENSE SYSTEM

Будь-яка сучасна комп’ютерна система не може використовуватися без належного захисту від зовнішніх кібератак. Робота в мережі Інтернет супроводжується високим ризиком мережевих атак. Компанія CIS [1] повідомила, що протягом останніх років кожна друга організація була атакована. Існує величезна кількість мережевих атак, які мають тенденцію до зростання. Зокрема, у третьому кварталі 2015 року тільки продукти «Лабораторії Касперського» заблокували більше 1 мільярда шкідливих атак на комп’ютерах і мобільних пристроях користувачів. Всього в даних інцидентах було зафіксовано більше 145 мільйонів унікальних шкідливих і потенційно небезпечних об’єктів [2].

Розв’язанню задачі виявлення мережевих атак присвячено багато робіт як зарубіжних так і вітчизняних вчених [3-7]. В даній роботі запропонована нейромережева штучна імунна система кіберзахисту. Нейромережева штучна імунна система кіберзахисту – це набір «інтелектуальних» датчиків (імунних детекторів) і правил, що описують їх поведінку. Імунні детектори проходять через такі етапи: створення, навчання, відбір, функціонування і т.д. Кожен етап може бути представлений як окремий модуль системи захисту. На рисунку 1 показана архітектура такої системи.

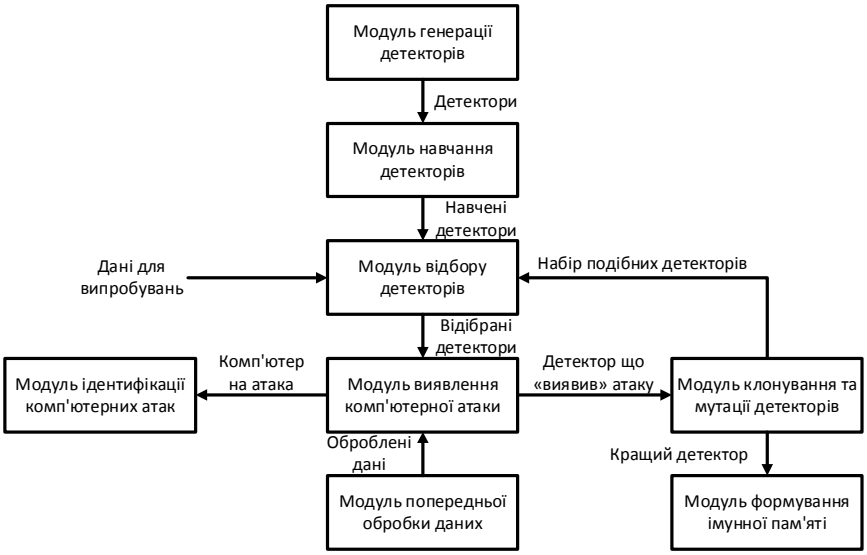

Рис. 1. Архітектура інтелектуальної системи для виявлення комп’ютерних атак

Модуль генерації детекторів створює, так звані, попередні детектори, які проходять через декілька етапів, перш ніж набути здатності правильної класифікацій об’єктів. Кожен імунний детектор має обмежений час служби, протягом якого він «живе» в системі. В кінці терміну служби детектор замінюється іншим новим детектором.

В результаті навчання, імунні детектори набувають здатність правильної класифікації різних об’єктів та процесів в комп’ютерному середовищі для виявлення кібератак. Після навчання всі імунні детектори проходять через етап відбору, де

детектори проходять перевірку на коректність, щоб мінімізувати помилкову роботу.

Всі відібрані детектори використовуються для захисту комп'ютерної системи від кібератак. Набір активних імунних детекторів утворює мультиагентну систему, де кожен імунний детектор має свій власний список завдань. Якщо жоден з детекторів не знайшов аномалію, то дані передаються на обробку операційній системі і відповідним програмам.

Якщо детектор знайшов загрозу, то активуються процеси клонування та мутації. Метою модулів клонування та мутацій є створення копії імунного детектора, який знайшов атаку. Такі клони здатні реагувати на знайдені шкідливі програми і перевіряти всі об'єкти в комп'ютерному середовищі за короткий період часу.

Коли створюються клони, то в їх структурі відбувається процес мутації. Це дозволяє імунним детекторам набути нову здатність, адаптуватися до нових атак і збільшити швидкість виявлення атак. При виявленні і ліквідації атак, доцільно зберігати їх параметри і зразки з метою подальшого детального аналізу. Це дозволяє підвищити ймовірність виявлення і класифікації атак, а також забезпечити гнучкість системи. Новостворені детектори навчатимуться вже на нових даних.

«Кращий» детектор визначається і перетворюється в детектор «пам'яті». Детектори пам'яті мають необмежений термін роботи і забезпечують швидку реакцію на неодноразові кібератаки. Таким чином, множина детекторів «пам'яті» утворюють «імунну пам'ять» і зберігають інформацію про всі кібератаки, які відбулися та забезпечує високий рівень реакції на неодноразові спроби мережевих атак.

Модуль ідентифікації загроз використовується для класифікації виявлених загроз.

Отже, запропонована нейромережева штучна імунна система може бути використана для кіберзахисту. Вона здатна виявляти не тільки відомі атаки, але й нові кібберзагрози, раніше не відомі мережі.

Література

1. Center for Internet Security [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisecurity.org/.

2. Securelist [Електронний ресурс] – Режим доступу до ресурсу: https://securelist.ru/analysis/malware-quarterly/27153/razvitie-informacionnyx-ugroz-v-tretem-kvartale-2015-goda/

3. Cannady J. Artificial neural networks for misuse detection / J. Cannady // Proceedings of the 21st national information systems security conference. – Arlington (USA), 1998. – P. 368-381.

4. Mukkamalaa S. Intrusion detection using an ensemble of intelligent paradigms / S. Mukkamalaa, A.H. Sung, A. Abraham // Journal of Network and Computer Applications. – 2005. – Vol. 28(2). – P.167-182.

5. Grediaga A. Application of neural networks in network control and information security / A. Grediaga, F. Ibarra, F. García [et al.] // LNCS. – 2006. – Vol. 3973. – P. 208-213.

6. Intelligent system for detection of networking intrusion / M. Komar, V. Golovko, A. Sachenko, S. Bezobrazov // Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2011). – Prague (Czech Republic), 2011. – Vol.1. – P. 374-377.

7. Development of neural network immune detectors for computer attacks recognition and classification / M. Komar, V. Golovko, A. Sachenko, S. Bezobrazov // Proceedings of the 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2013). – Berlin (Germany), 2013. – Vol.2. – P. 665-668.