3. Про основні засади забезпечення кібербезпеки України: Законопроект від 19.06.2015 р. № 2126а. – Режим доступу: www.rada.gov.ua

4. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 р. № 2824-IV. – Режим доступу: www.rada.gov.ua

5. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 р. № 96/2016. – Режим доступу: www.rada.gov.ua

6. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» // Правова інформатика. – 2014. - №2(42). – 54-62 с.

7. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В.Л. Бурячок, С.В. Толюпа, В.В. Семко, Л.В. Бурячок, П.М. Складанний, Н.В. Лукова-Чуйко / - К. : ДУТ – КНУ, 2016. – 178 с.

8. Фурашев В.М. Кіберпростір та інформаційний простів, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. – 2012. - №2. – С. 162-169.

Інтелектуальна адаптивна система для виявлення та нейтралізації кібератак

Постіл С.Д.
кандидат технічних наук, ст.н.с.,
доцент кафедри інтелектуальних управляючих та
обчислювальних систем
Університету державної фіскальної служби України,
Любушкін Д.В.
директор інформаційних технологій (CIO)
компанії RISA Tehnologies (USA)

Сьогодні захист комп'ютерних систем від кібератак є важливою та актуальною проблемою. Для захисту комп'ютерних систем від кібератак в основному використовується спеціалізоване програмне забезпечення таке як антивіруси, мережеві екрани, IPSec, та спеціалізовані апаратні засоби. Проте в даний час більшість зловмисних програм можуть протидіяти багатьом цим засобам захисту, тому використання даного програмного забезпечення не гарантує захист від вторгнення. Функції операційної системи можуть бути перехоплені під час атак – це запобігає ідентифікації та нейтралізації шкідливих програм за допомогою спеціалізованого програмного забезпечення. Крім того, зловмисне програмне забезпечення може протидіяти роботі спеціалізованого програмного забезпечення, відслідковувати його операції, відновлювати видалені шкідливі процеси, змінювати параметри в системному реєстрі тощо. Комбінований метод ідентифікації та класифікації кібератак (програмно-апаратний) може забезпечувати відносно високу ефективність захисту комп'ютерної системи при достатній кваліфікації фахівців служби інформаційної безпеки (ІБ). При цьому для реалізації ІБ необхідно дотримуватись принципу «До-Під час-Після», тобто боротись з атакою потрібно протягом всього її життєвого циклу.

Якісно нового рівня ІБ можна досягти при застосуванні нейронних мереж, так як стає уже неможливим аналізувати ті об’єми даних, які генерують засоби захисту і деякі атаки просто пропускаються [1, 2].

Спеціально навчена нейронна мережа може вважатися головним детектором системи для ідентифікації вторгнень. Для підвищення ефективності такої системи можливо використати основні принципи та механізми біологічних імунних систем. Цей підхід базується на інтеграції нейронних мережних детекторів в штучну імунну систему. Завдяки такому підходу система захисту від кібератак зможе адаптуватися до невідомих вторгнень, що виникли внаслідок клонування та мутації, так званих атак нульового дня (zero-dayattack).

Таким чином, ця інтелектуальна система виявлення вторгнень може використовувати набір спеціалізованих детекторів. Кожен детектор несе відповідальність за ідентифікацію та класифікацію певного типу вторгнення, а набір таких детекторів несе відповідальність за весь захист системи. Проте реалізація цього методу має всі недоліки програмного захисту, про які йшлося вище. Таким чином, існує суперечність між надійністю комп'ютерної системи і вторгненням та основною вразливістю інструментів, забезпечуючи такий захист від кібератак. Вирішення цього протиріччя можливе лише у випадку зміни парадигми виготовлення інструментів забезпечення захисту від вторгнень.

Можна сформулювати наступні вимоги до інтелектуальної системи захисту та підходи щодо її удосконалення. Для надійного захисту від кібератак потрібно використовувати апаратне забезпечення.

Апаратне забезпечення не працює на зараженій операційній системі. Тому будь-яке зловмисне програмне забезпечення не може протидіяти або змінювати апаратні операції без ідентифікації та нейтралізації. Всі його спроби будуть невдалими і кібератаки будуть швидко нейтралізовані.

Для реалізації цього підходу інтелектуальна система захисту апаратного забезпечення від комп'ютерних атак повинна забезпечувати відповідність наступним вимогам:

1. Висока надійність кібератак підсистеми для виявлення та нейтралізації поточних типів атак. Це можна досягти лише за допомогою апаратної реалізації підсистеми.

2. Висока гнучкість підсистеми для поточного виявлення різних типів кібератак та їх модифікацій. Це можна досягти шляхом періодичного динамічного оновлення нейронних детекторів за результатами поточного аналізу кібератак.

3. Для поточного аналізу кібератак слід надати виділений комп'ютер для безперервного аналізу поточних атак та створення відповідних засобів захисту, включаючи нейродетектори, які будували систему виявлення кібератак.

4. Підготовка пристроїв для виявлення, нейтралізації вторгнення і оновлення повинна виконуватися на виділеному комп'ютері, який не буде підключений до мережі. Цим буде забезпечена висока надійності системи до кібератак, їх аналізу та навчання нейронних мереж. Необхідно також розділяти пам'ять, що містить аналізовані підозрілі коди, та пам'ять з програмним забезпеченням, яке здійснює аналіз.

5. Підсистема високої продуктивності для поточного виявлення та нейтралізації різних типів кібератак повинна бути забезпечена в процесі адаптації до вірогідності виявлення атак.

Ці вимоги можуть бути виконані в процесі впровадження підсистеми для поточного виявлення та нейтралізації кібератак у програмованих логічних масивах (ПЛМ). Крім того, ПЛМ необхідно перепрограмувати на спеціально розробленому комп'ютері, який використовується для аналізу кібератак, і не підключеному до мережі. Комп'ютери, підключені до мережі, не повинні мати:

- ✓ метод ре-конфігурації ПЛМ, де виконується підсистема виявлення та нейтралізації поточних кібератак;
- ✓ доступ до результатів ПЛМ, контроль за його перепрограмуванням.

Слід зазначити, що ПЛМ є апаратними вузлами, тоді як підсистема виявлення та нейтралізації поточних кібератак має відносно високу складність. Тому проблема оптимізації виникає, зокрема, для процесу зменшення кількості необхідних макроелементів. З цією метою, відповідно до аналізу функцій захисту від кібератак, доцільно визначити функції кожної підсистеми. Таким чином, слід надавати наступні функції:

- ✓ виявлення нинішньої комп'ютерної безпеки та її класифікації;
- ✓ прийняття рішень про наявність кібератаки;
- ✓ подолання кібератак;
- ✓ аналіз модифікації кібератаки;
- ✓ створення відповідних засобів виявлення кібератак, тобто нейронних детекторів;
- ✓ статистична обробка кібератак з метою з'ясування їх походження;
- ✓ забезпечення адаптації до ймовірності нападів.

Висновок. Для організації ефективної ІБ необхідно впроваджувати інноваційні технології на основі штучного інтелекту, що базуються на здатності служби ІБ описувати та налаштовувати відповідні моделі, а також інтерпретувати отримані результати.

Література:

1. Лукацкий А. Предотвращение атак необходимо, но уже недостаточно [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/forum /topic/33876.

2. Постіл С. Д. Інтелектуальна система на основі нейронної мережі для прогнозування показників фінансових ринків. / С. Д. Постіл, Д. В. Любушкін // Науковий вісник Національного університету державної податкової служби України. - 2012. - №2(57). 68 -76.