УКРАЇНА **(19) UA** **(11) 108238** **(13) U**

(51) МПК
G06F 21/55 (2013.01)

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2016 00127**
(22) Дата подання заявки: **04.01.2016**
(24) Дата, з якої є чинними права на корисну модель: **11.07.2016**
(46) Публікація відомостей про видачу патенту: **11.07.2016, Бюл.№ 13**

(72) Винахідник(и):
Поморова Оксана Вікторівна (UA),
Савенко Олег Станіславович (UA),
Крищук Андрій Федорович (UA),
Лисенко Сергій Миколайович (UA),
Бобровнікова Кіра Юліївна (UA),
Нічепорук Андрій Олександрович (UA)

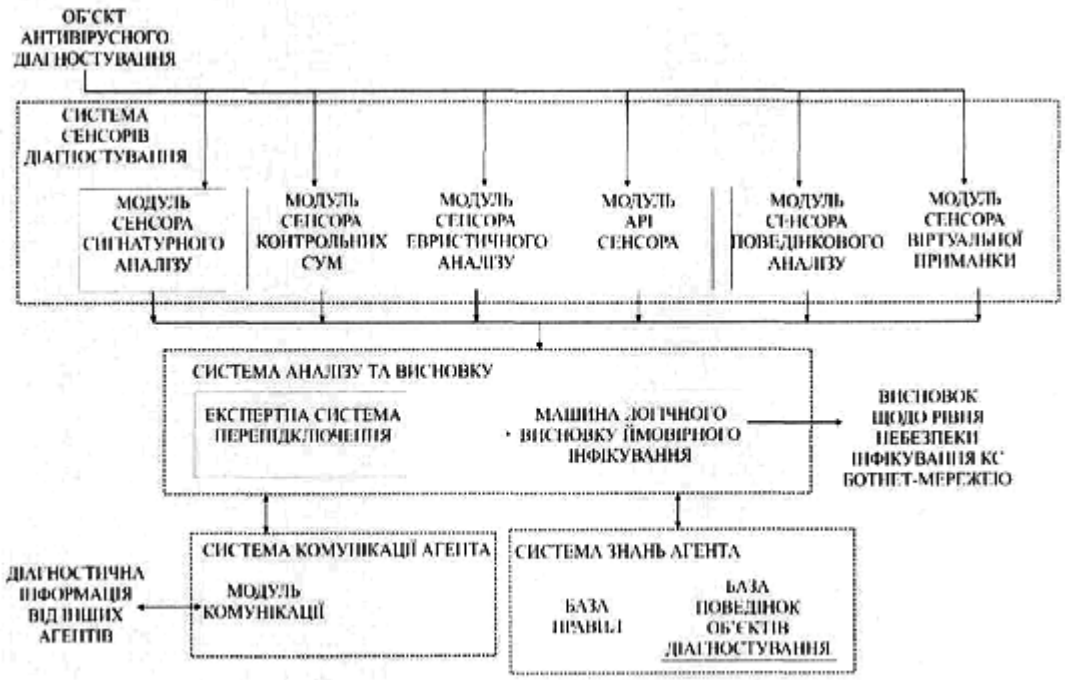
(73) Власник(и):
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ,
вул. Інститутська, 11, м. Хмельницький, 29016 (UA)

(54) МУЛЬТИАГЕНТНИЙ СПОСІБ ЛОКАЛІЗАЦІЇ БОТ-МЕРЕЖ У КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

(57) Реферат:

Мультиагентний спосіб локалізації бот-мереж в корпоративних комп'ютерних мережах включає використання мультиагентної системи для здійснення комунікації між агентами для обміну інформацією між групами агентів для визначення рівня присутності бот-мереж в заданих корпоративних комп'ютерних мережах. Визначають місце знаходження інфікованих комп'ютерних систем і відповідного програмного забезпечення на основі сканування комп'ютерних систем сенсорами S_1, S_2, S_5 агента A і моніторингу комп'ютерних систем сенсорами S_3, S_4, S_6 агента A з подальшим обміном даними рівня прояву $R_{S_3}, R_{S_4}, R_{S_6}$ та параметрами. Здійснюють визначення комп'ютерних систем для зміни підключення з використанням експертної системи та поділом на комп'ютерні системи, на яких розміщені агенти, на 3 групи: "перепідключені", "помічені", "без проявів" і для кожної групи заповнення матриць відношення $S_i = \left|S_{Z,X}\right|$ дій-проявів, виражених через обчислення проявів бота бот-мережі та дій ймовірно інфікованого програмного забезпечення з врахуванням відповідно до моделей поведінок типів ботів бот-мереж генерування матриці згідно з кроками w_i життєвого циклу ботів, тобто прийнявши $\omega_t^j, 0 \le \omega_j^i \le 1$ - за одну з ознак прояву, $j = \overline{1,n}, t = \overline{1,\gamma}$, де γ - кількість проявів ботів, n - кількість комп'ютерних систем в корпоративній мережі, k - кількість матриць відношень дій ботів до проявів, $k = \overline{1,18}$. Оцінка рівня визначеного прояву на кожній комп'ютерній системі обчислюється за формулою.

UA 108238 U


ОБ'ЄКТ АНТИВІРУСНОГО ДІАГНОСТУВАННЯ
СИСТЕМА СЕНСОРІВ ДІАГНОСТУВАННЯ
МОДУЛЬ СЕНСОРА СИГНАТУРНОГО АНАЛІЗУ
МОДУЛЬ СЕНСОРА КОНТРОЛЬНИХ СУМ
МОДУЛЬ СЕНСОРА ЕВРИСТИЧНОГО АНАЛІЗУ
МОДУЛЬ API СЕНСОРА
МОДУЛЬ СЕНСОРА ПОВЕДІНКОВОГО АНАЛІЗУ
МОДУЛЬ СЕНСОРА ВІРТУАЛЬНОЇ ПРИМАНКИ
СИСТЕМА АНАЛІЗУ ТА ВИСНОВКУ
ЕКСПЕРТНА СИСТЕМА ПЕРЕПІДКЛЮЧЕННЯ
МАШИНА ЛОГІЧНОГО ВИСНОВКУ ЙМОВІРНОГО ІНФІКУВАННЯ
ВИСНОВОК ЩОДО РІВНЯ НЕБЕЗПЕКИ ІНФІКУВАННЯ КС БОТНЕТ-МЕРЕЖЕЮ
СИСТЕМА КОМУНІКАЦІЙ АГЕНТА
МОДУЛЬ КОМУНІКАЦІЙ
ДІАГНОСТИЧНА ІНФОРМАЦІЯ ВІД ІНШИХ АГЕНТІВ
СИСТЕМА ЗНАНЬ АГЕНТА
БАЗА ПРАВИЛ
БАЗА ПОВЕДІНОК ОБ'ЄКТІВ ДІАГНОСТУВАННЯ

Корисна модель належить до інформаційної безпеки і може використовуватись для локалізації бот-мереж у корпоративних комп'ютерних мережах.

Способи діагностування комп'ютерних систем на наявність бот-мереж спрямовані на збір інформації про стан мережі або на виявлення існуючих бот-мереж. До активних способів можна віднести наступні: Data-mining, метод аналізу графів користувач-користувач, сигнатурний метод. До пасивних способів [1] діагностування належать: спосіб на основі мереж-приманок, способи віддаленої аутентифікації коду, способи пасивного моніторингу трафіку, способи моніторингу груп проявів в DNS-трафіку.

Загальна структура засобів на основі способу "мереж-приманок" полягає в тому, приманка позначає кінцевий "хост", який є дуже вразливим до атак зловмисників і є часто успішно атакованим в дуже короткий проміжок часу. При цьому позначається програмне забезпечення, яке використовується для моніторингу, збору, контролю та зміни трафіку через пастки.

Джеймі Райденом [2| запропоновано механізм виявлення бот-мереж, використовуючи приманки низької взаємодії. Це приманки з використанням PHP і емуляції декількох вразливостей. Жічань Лі, Анап Гоял і Ян Чень [3] запропонували дослідження сканування трафіку бот-мереж. Серед 43 подій, час надходження приблизно 25 (58 %) відповідає експоненціальному розподілу. Це дозволило припустити, що більшість бот-мереж дійсно використовують випадкові стратегії сканування. Запропонована стратегія є неефективною для виявлення P2P бот-мереж. Раджаб Чаллу і Раґхавендра Котапаллі запропонували спосіб виявлення бот-мереж, використовуючи приманки і P2P бот-мережі [3]. Приманки використовуються в синхронізації з P2P бот-мережею.

До активних методів належать наступні: Data-mining, метод аналізу графів користувач-користувач, сигнатурний метод. Яо Чжао було запропоновано моделі випадкового графу для аналізу графів користувач-користувач. Вони показують, що групи бот-користувачів диференціюють себе від нормальних груп користувачів, формуючи гігантські компоненти у графі. На основі моделі розроблено ієрархічний алгоритм для вилучення таких сформованих компонентів, як бот-користувачі. Недоліком є те, що цей метод заснований лише на інформації поштової служби. Сигнатурний спосіб базується на виявленні, знаючи його автентичні частини коду. Знання з сигнатур і поведінок існуючих бот-мереж корисні для виявлення бот-мереж. Це рішення не є корисним для невідомих ботів.

Недоліками відомих способів локалізації бот-мереж є невисока достовірність локалізації та, крім збору інформації про стан мережі, визначення присутності бот-мереж та блокування їх, що дозволило б запобігти поширенню снам повідомлень і блокуванню електронних ресурсів.

За аналог можна вважати спосіб виявлення комп'ютерних атак нейромережевою штучною імунною системою, описаний в [4].

Недоліки прототипів. Слабким місцем відомих способів є недостатньо висока достовірність локалізації нових бот-мереж.

Задачею корисної моделі є підвищення достовірності локалізації бот-мереж у корпоративних комп'ютерних мережах.

Поставлена задача вирішується тим, що розроблено мультиагентну систему всередині корпоративної мережі [3]. Вона використовує визначену кількість агентів, які здійснюють антивірусне діагностування за допомогою набору сенсорів $A = \langle S_1, S_2, S_3, S_4, S_5, S_6 \rangle$, де S_1 - сенсор сигнатурного аналізу; S_2 - сенсор контрольної суми; S_3 - сенсор евристичного аналізу; S_4 - сенсор поведінкового аналізу; S_5 - сенсор порівняльного аналізу шляхом застосування інтерфейсу програмування API і драйвера дискової підсистеми за допомогою IOS; S_6 - сенсор "віртуальна приманка". Кожен агент містить набір ефекторів, які впливають на комп'ютерну систему з метою блокування підозрілих програм і подальшим сповіщенням інших агентів в мережі про інфікування для того, щоб активувати виявлення підозрілих програм з подібною поведінкою. Агент містить процесор, який обробляє вхідні дані і визначає рівень присутності бота, як складової бот-мережі в комп'ютерних системах. Функціонування процесу базується на використанні знань. Схему локалізації бот-мереж у корпоративних комп'ютерних мережах зображено на рисунку.

Процес локалізації розпочинається з побудови схематичної карти з'єднань КС деякої корпоративної мережі шляхом генерування відповідних записів в кожному антивірусному агенті мультиагентної системи. Всі агенти на основі цієї інформації спілкуються між собою.

Визначається ступінь присутності бот-мережі. Визначення базується на аналізі дій ботів в ситуації навмисної зміни типу підключення на ймовірно інфікованій комп'ютерній системі. Такий

підхід здійснюється у разі недостатнього (низького) значення підозрілості програмного забезпеченням, але ця підозріла активність присутня в певній кількості комп'ютерних систем корпоративної мережі.

Під час функціонування комп'ютерної системи антивірусне діагностування здійснюється за допомогою сенсорів в кожному агенті. Результати антивірусного діагностування аналізуються на предмет того, який з сенсорів спрацював, і який рівень підозрілості він продукував. Якщо спрацював сигнатурний сенсор або аналізатор контрольної суми чи API-сенсор, то результати інтерпретуються, як 100 % виявлення шкідливих програм. У цій ситуації виконується блокування відповідного програмного забезпечення та його подальше видалення.

В тих випадках, коли спрацювали сенсори евристичного S_3, поведінкового S_4 аналізу або сенсор "віртуальна приманка" S_6, то аналізуються рівні підозрілості R_{S_3}, R_{S_4} і R_{S_6}, і в разі подолання певного порогу n, $n \le \max(R_{S_3}, R_{S_4}, R_{S_6}) \le 100$, виконується блокування програмного забезпечення і його подальше видалення. Якщо вказаний поріг для прийняття остаточного рішення про присутність шкідливого програмного забезпечення в комп'ютерній системі не подоланий, то він належать проміжку $m \le \max(R_{S_3}, R_{S_4}, R_{S_6}) < n$. Якщо значення належить проміжку $\max(R_{S_3}, R_{S_4}, R_{S_6}) < m$, то очікуються нові результати від сенсорів антивірусного агента. У всіх випадках інформація антивірусного агента про інфікування або підозрілу поведінку програмного забезпечення в комп'ютерній системі повинна передаватись на інші агенти.

В основу корисної моделі поставлена задача розробки мультиагентного способу для ситуації, коли результати виявлення антивірусними агентами ступеня присутності бот-мереж належать проміжку $m \le \max(R_{S_3}, R_{S_4}, R_{S_6}) < n$. У цьому випадку, антивірусний агент комп'ютерної системи запитує в інших агентів корпоративної мережі про аналогічні підозрілі поведінки деякого програмного забезпечення, яке схоже на бот-мережу. Якщо визначений агент отримує інформацію від одного або декількох агентів про аналогічну підозрілу поведінку певного програмного забезпечення, то ймовірно інфіковані комп'ютерні системи "помічаються" і будується нова карта мережі з врахуванням помічених комп'ютерних систем. З множини "помічених" комп'ютерних систем вибирається деяка комп'ютерна система для зміни типу мережного з'єднання (перепідключення) - спеціальні налаштування мережі, які перешкоджають функціонуванню мережі бота в комп'ютерній системі. Використовуючи експертну систему з визначеними правилами, здійснюється вибір однієї комп'ютерної системи з "помічених".

Вибір комп'ютерної системи для зміни типу підключення здійснюється наступним чином. Вибирається комп'ютерна система з найбільш актуальними антивірусними базами, з найвищою неперервною тривалістю роботи, операційною системою з найнижчим рівнем уразливості і кращим результатом від сенсорів. Використовуючи дані отримані від агентів інших комп'ютерних систем корпоративної мережі засобами експертної системи визначається "відповідна" комп'ютерна система для зміни типу підключення. Рівень "відповідності" комп'ютерних систем визначається кожним агентом автономно. Після зміни типу підключення комп'ютерних систем у корпоративній мережі формується три групи комп'ютерних систем: комп'ютерні системи із зміненим типом підключення ("перепідключені комп'ютерні системи"), комп'ютерні системи із схожими проявами ("помічені комп'ютерні системи") і решта комп'ютерних систем ("комп'ютерні системи без визначених проявів"). Після чого визначається рівень прояву присутності бот-мережі у кожній групі.

Визначення рівня прояву бот-мережі стало можливим завдяки характерним особливостям функціонування бот-мереж. Боти можуть проявити свою присутність, коли комп'ютерна система змінює тип підключення до мережі. Також характерною особливістю є виконання зловмисних дій групою, відповідно прояви на одній комп'ютерній системі відповідають проявам на інших комп'ютерних систем в заданий проміжок часу.

У разі, якщо комп'ютерна система є сервером мережі і об'єднує під мережі корпоративної мережі, то змінювати тип мережного з'єднання цієї комп'ютерної системи заборонено.

Відповідно до розробленого способу локалізації бот-мереж мультиагентна система здійснює комунікацію між агентами для обміну інформацією між групами агентів для визначення рівня присутності бот-мереж в заданій корпоративній мережі.

Кожен тип агентів має різну складність. Наприклад, при типі синхронізації агенти знають, що кожного разу, коли вони спілкуються, вони знають глобальний стан, і в результаті попередня історія часто стає менш важливою, тому що агенту не потрібна хронологічна інформація невизначених станів агентів і системи визначення наступних станів агентів.

Оскільки агенти можуть не спілкуватися і, таким чином, не завжди можуть синхронізувати свої стани, та ж сама попередня інформація, в одному агенті може відповідати різним шляхам в інших агентах, загалом, рішення кожного окремого агента про зв'язок/дії можуть базуватись на всій локально наявній інформації, в тому числі історії та поточній інформації.

Різниця між дією зв'язку та регулярною дією наступна: дія комунікації розглядається обома агентами у той час, як регулярна дія відома агенту тільки локально.

Для обчислення ознаки прояву побудуємо матриці відношень прояву бота бот-мережі та дій ймовірно інфікованого програмного забезпечення. Приймемо $\omega_t^j, 0 \le \omega_j^i \le 1$ - одна з ознак прояву, $j = \overline{1,n}, t = \overline{1,\gamma}$, де γ - кількість проявів ботів, n - кількість комп'ютерних систем в корпоративній мережі, k - кількість матриць відношень дій ботів до проявів, $k = \overline{1,18}$. Оцінка рівня визначеного прояву на кожній комп'ютерній системі обчислюється за формулою:

$$\omega_t^j = \sum_{l=1}^{k} \left(\frac{\sum_{i=1}^{n_k} k_i^l \cdot S_{i,s}^j}{S_t^j} \right) / k, \quad (1)$$

де k_i^l - коефіцієнти небезпеки деяких проявів, $\sum_{l=1}^{k} k_i^l = 1$; $S_{i,t}^j$ - значення матриці відношень дій ботів до проявів, $S_t^j = \sum_{i=1}^{n_k} S_{i,t}^j$.

Після обміну результатами визначення ознаки прояву бота, будуємо матрицю відношення ознаки проявів бота w_i до кількості комп'ютерних систем у визначеній групі n.

Рівень прояву присутності бот-мережі в визначеній групі комп'ютерних систем визначимо, як:

$$P_\alpha = \frac{\sum_j \sum_i \omega_j^i}{\alpha}, \quad (2)$$

де α - кількість ненульових проявів ботів. Після цього число P_α визначається й інтерпретується, як ступінь прояву бот-мережі в групі комп'ютерних систем. Отриманий результат знаходиться в межах від 0 до 1.

Основні кроки мультиагентного способу локалізації бот-мереж в корпоративних мережах такі:

1) сканування комп'ютерних систем сенсорами S_1, S_2, S_5 агента А;

2) моніторинг комп'ютерних систем сенсорами S_3, S_4, S_6 агента А;

3) обмін даними рівня прояву $R_{S_3}, R_{S_4}, R_{S_6}$ та параметрами;

4) визначення комп'ютерних систем для зміни підключення з використанням експертної системи;

5) поділ на комп'ютерні системи, на яких розміщені агенти, на 3 групи: "перепідключені", "помічені", "без проявів";

6) заповнення матриць відношення $S_i = \left| S_{Z,X} \right|$ дія-прояв;

7) обрахунок рівнів проявів на визначених комп'ютерних систем (формула 1);

8) обмін значеннями рівня прояву між агентами визначених груп;

9) заповнення матриці проявів групи комп'ютерних систем ω,

10) обчислення рівня прояву присутності бот-мережі у групі комп'ютерних систем (формула 2).

Розроблений мультиагентний спосіб локалізації бот-мереж в корпоративних комп'ютерних мережах, відмінною рисою якого є використання поведінкових моделей ботів і бот-мереж та мультиагентних технологій, дозволяє визначній місце знаходження інфікованих комп'ютерних систем і відповідного програмного забезпечення.

Джерела інформації:

1. Погребенник В.Д. Пасивні методи виявлення ботнет-мереж / Погребенник В.Д., Хромчак П.Т. // Вісник національний університет "Львівська політехніка". - № 741. - 2012. - с. 97-104.

2. Rajarajan M. Detection and prevention of botnets and malware in an enterprise network / Rajarajan M., Piper P., Wang H., [та in.] // International Journal of Wireless and Mobile Computing. 2012. - С. 144-153.

3. Savenko O. Multi-agent based approach of botnet detection in computer systems/ Savenko O., Lysenko S., Kryschuk A. // Computer Networks 19th International Conference, 2012. Volume 291. P. 171 180, DOI: 10.1007/978-3-642-31217-5 J 9.

4. Пат. № 74822 Україна, МПК(2012) H04W 12/08, G06F 21/00, G06F 12/14. Спосіб виявлення комп'ютерних атак нейромережевою штучною імунною системою. Комар М.П., Саченко А.О., Головко В.А., Безобразов С.В.; заявник і патентовласник Тернопільський національний економічний університет. - №u201205349; заявл. 28.04.12; опубл. 12.11.12, Бюл. № 21.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

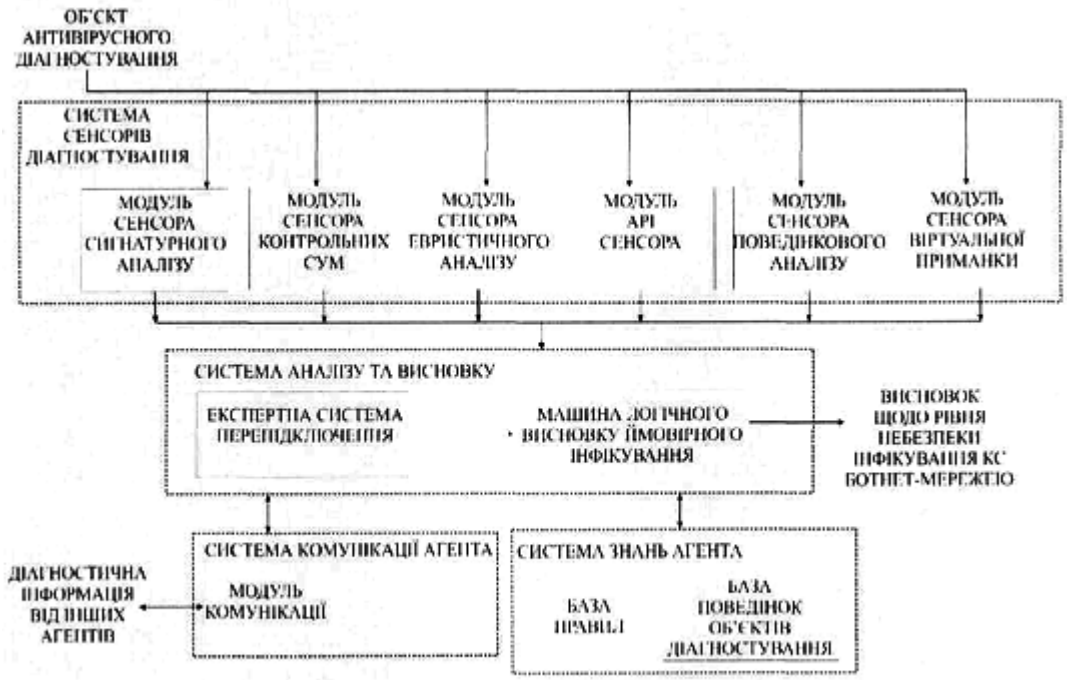
Мультиагентний спосіб локалізації бот-мереж в корпоративних комп'ютерних мережах, який включає використання мультиагентної системи для здійснення комунікації між агентами для обміну інформацією між групами агентів для визначення рівня присутності бот-мереж в заданих корпоративних комп'ютерних мережах, який **відрізняється** тим, що використання поведінкових моделей ботів і бот-мереж та мультиагентних технологій дозволяє визначити місце знаходження інфікованих комп'ютерних систем і відповідного програмного забезпечення на основі сканування комп'ютерних систем сенсорами S_1, S_2, S_5 агента А і моніторингу комп'ютерних систем сенсорами S_3, S_4, S_6 агента А з подальшим обміном даними рівня прояву $R_{S_3}, R_{S_4}, R_{S_6}$ та параметрами з можливістю визначення комп'ютерних систем для зміни підключення з використанням експертної системи та поділом на комп'ютерні системи, на яких розміщені агенти, на 3 групи: "перепідключені", "помічені", "без проявів" і для кожної групи заповнення матриць відношення $S_i = \left|S_{Z,X}\right|$ дій-проявів, виражених через обчислення проявів бота бот-мережі та дій імовірно інфікованого програмного забезпечення з врахуванням відповідно до моделей поведінок типів ботів бот-мереж генерування матриці згідно з кроками w_i життєвого циклу ботів, тобто прийнявши $\omega_t^j, 0 \le \omega_j^i \le 1$ - за одну з ознак прояву, $j = \overline{1,n}, t = \overline{1,\gamma}$, де γ - кількість проявів ботів, n - кількість комп'ютерних систем в корпоративній мережі, k - кількість матриць відношень дій ботів до проявів, $k = \overline{1,18}$, то оцінка рівня визначеного прояву на кожній комп'ютерній системі обчислюється за формулою:

$$\omega_t^j = \sum_{l=1}^{k} \left(\frac{\sum_{i=1}^{n_k} k_i^l \cdot S_{i,s}^j}{S_t^j} \right) / k,$$

де k_i^l - коефіцієнти небезпеки деяких проявів, $\sum_{l=1}^{k} k_i^l = 1$; $s_{i,t}^j$ - значення матриці відношень дій ботів до проявів, $S_t^j = \sum_{i=1}^{n_k} S_{i,t}^j$ і для оцінки стану різних комп'ютерних систем в мережі здійснення обміну значеннями рівня прояву між агентами визначених груп та заповнення матриці проявів групи комп'ютерних систем ω і обчислення рівня прояву присутності бот-мережі у визначеній групі за формулою:

$$P_\alpha = \frac{\sum_j \sum_i \omega_j^i}{\alpha},$$

де α - кількість ненульових проявів ботів, після чого число P_α визначається й інтерпретується в межах від 0 до 1 як ступінь прояву бот-мережі в групі комп'ютерних систем.



Комп'ютерна верстка Г. Паяльніков

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601