УДК 004.92.3

О. Савенко, А. Крищук, С. Лисенко
Хмельницький національний університет,
кафедра системного програмування

ДІАГНОСТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ НА НАЯВНІСТЬ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ АНТИВІРУСНОЇ МУЛЬТИАГЕНТНОЇ СИСТЕМИ

Запропонований новий підхід у діагностуванні комп'ютерних систем на наявність нового шкідливого програмного забезпечення на основі використання мультиагентної системи. Розглянуто загальний принцип роботи агента в мультиагентній антивірусній системі.

Ключові слова: діагностування, шкідливе програмне забезпечення, антивірусний, мультиагентний.

The new approach of computer systems diagnosing for new malware based on the use of multi-agent system is proposed. We consider the general principle work of agent in antiviral multi-agent system.

Key words: diagnosing, malware, antiviral, multi-agent.

Вступ

У сучасному інформаційному просторі зберігається тенденція до збільшення кількості шкідливого програмного забезпечення (ШПЗ). Значну частку шкідливого програмного забезпечення становлять мережні віруси і троянські віруси, які є складовими ботнет-вірусів (див. рис. 1) [1, 2].

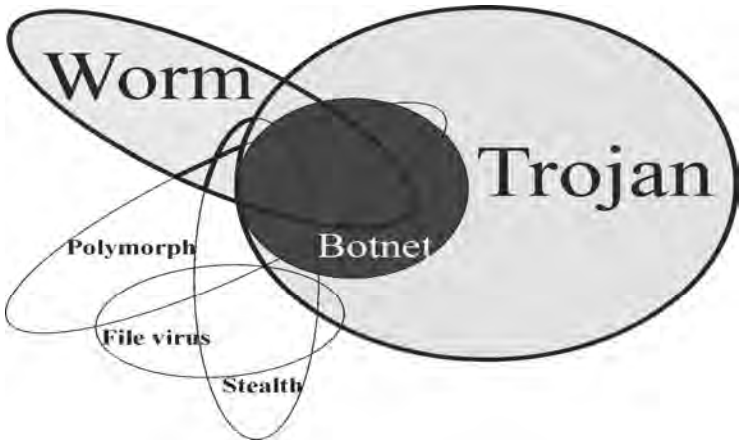

Рис. 1. Перетин множин характеристик вірусів

Поширеними методами, що використовуються в сучасних антивірусних програмних засобах, є не тільки емулятор коду, але й такі, як криптоаналіз, статистичний аналіз, евристичний аналізатор і поведінкове блокування [3]. Проте сучасні тенденції розвитку і поширення ШПЗ вимагають ефективних новацій у галузі. Наявні засоби антивірусного діагностування (АД) комп'ютерних систем (КС) при великому об'ємі вірусних баз відзначаються великою кількістю хибних спрацювань [4].

Антивірусні компанії увесь час займаються активним вивченням інструментів і методів протидії новим небезпекам. Постійне збільшення швидкості випуску нових видів ШПЗ досягли межі, при якій звичайні системи оновлення для протидії виявились недостатніми (див. рис. 2). Результати досліджень компанії NSS Labs, які проводилися в другому кварталі 2011 р., показали, що для блокування загроз антивірусним компаніям необхідно від 4,62 до 92,48 год [5].

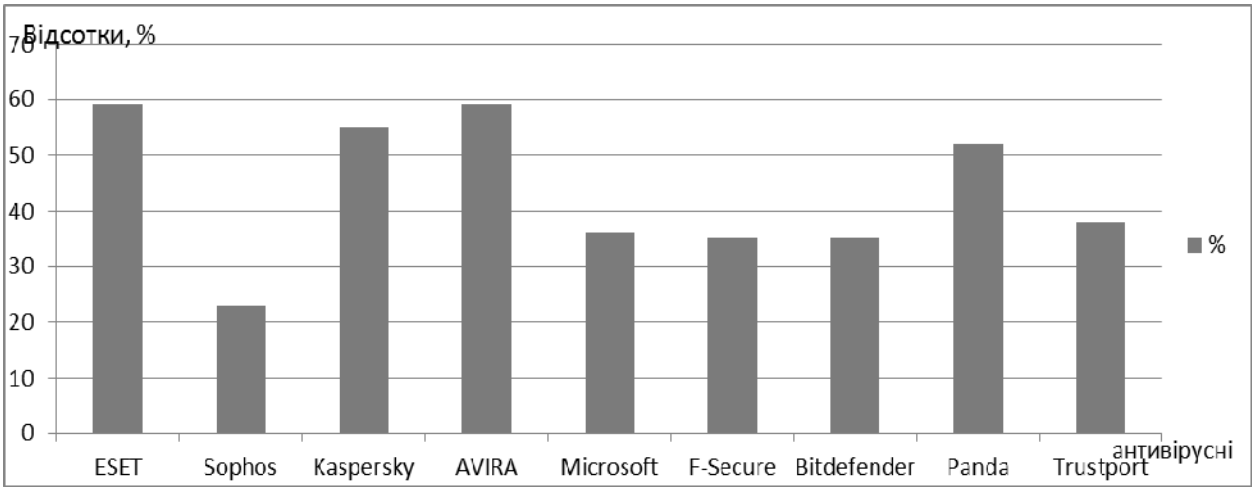

Рис. 2. Достовірність виявлення нового ШПЗ

Подальше використання оновлень антивірусних баз для збільшення швидкості реакції на загрози є неефективним. Навіть новітні підходи до АД комп'ютерних систем, такі як «хмарні обчислення» для виявлення ШПЗ є не достатньо ефективними, оскільки є важкими в реалізації (необхідність великої пропускної здатності, надійності каналів зв'язку та необхідності прямого відкритого доступу до даних користувача) [6].

Постановка задачі

Розробити нові підходи до ефективного антивірусного діагностування КС на наявність нового ШПЗ. Одним із можливих шляхів підвищення достовірності антивірусного діагностування (АД) КС є інтеграція антивірусної мультиагентної системи в КС для виявлення нового ШПЗ. Необхідним є розробка принципів функціонування такої системи із описом особливостей роботи та взаємодії агентів, а також сенсорів та ефекторів як їх складових.

Основна частина

Технологія мультиагентних систем не є просто об'єднанням різних результатів у галузі штучного інтелекту. Інтеграція, яка призводить до парадигми багатоагентних систем, привносить принципово нові властивості і можливості в процес діагностування КС на наявність нового ШПЗ.

Використання мультиагентних систем вимагає наявності у агентів мінімального набору базових характеристик:

– активності – здатності до організації і реалізації дій;

– реактивності – здатності сприймати стан середовища;

– автономності – відносної незалежності від навколишнього середовища, що зумовлює власну поведінку, яка повинна мати відповідне ресурсне забезпечення;

– спілкування – базової характеристики, яка випливає з необхідності виконувати свої завдання спільно з іншими агентами, і в основі якої лежить використання протоколів комунікації;

– суспільної поведінки (social ability) – здатності функціонувати в співтоваристві з іншими агентами, обмінюючись з ними повідомленнями за допомогою деякої загальнозрозумілої мови комунікацій;

– цілеспрямованості – базової характеристики, яка передбачає наявність власних джерел мотивації, а саме особливих інтенціональних характеристик;

– про-активності (pro-activity) – здатності агента брати на себе ініціативу, тобто здатність генерувати цілі і діяти раціонально для їх досягнення, а не тільки реагувати на зовнішні події [6].

Також необхідною умовою реалізації агентом визначеної поведінки є наявність сенсорів (компонентів, що безпосередньо сприймають дію середовища), ефекторів (компонентів, що впливають на середовище), процесора – блока обробки інформації і пам'яті [7].

Для розв'язання задачі виявлення ШПЗ пропонується здійснення детектування із залученням антивірусної мультиагентної системи (МАС).

Антивірусна мультиагентна система для корпоративної мережі складається з визначеної множини агентів. Агенти ідентифіковані, дискретні індивідууми з встановленими характеристиками і правилами, що керують його поведінкою і здатністю приймати рішення.

На рис. 3 наведена загальна схема функціонування агента пропонованої системи антивірусного діагностування.

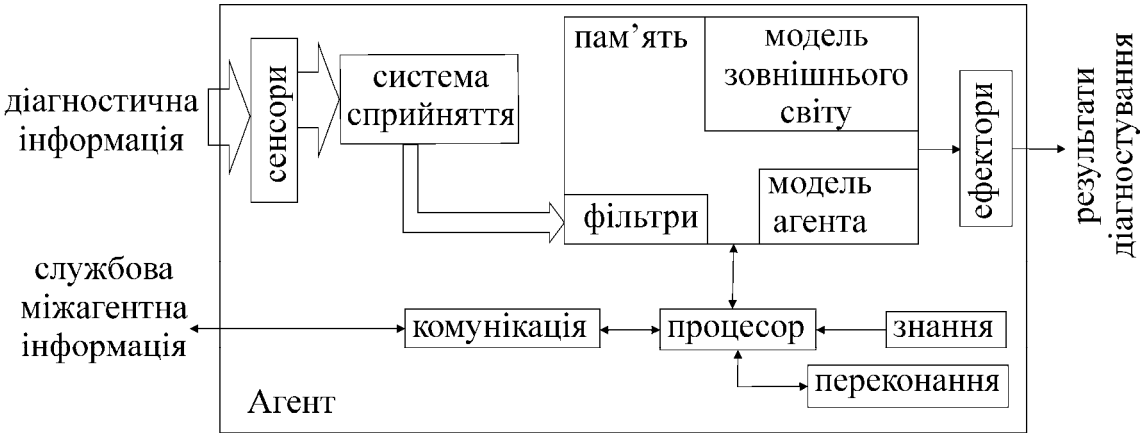

Рис. 3. Загальна схема функціонування агента

Подамо агента цієї системи кортежем:

$$A = \langle P, R, K, S_1, S_2, S_3, S_4, S_5, S_6 ... S_n \rangle, \quad (2.1)$$

де P – процесор, який забезпечує об'єднання і переробку даних, опрацювання оптимальної реакції на вхідну інформацію про стан КС, прийняття рішення про виконання необхідних дій;

R – переконання; правила, що змінюють правила поведінки агента; це ті знання, які можуть змінюватись з часом і стає неправильним, однак агент може не містити інформації про це і продовжувати роботу в переконанні, що їх можна брати за основу своїх висновків;

K – знання агента – частина правил і знань, які не змінюються під час його функціонування;

S_1 – сенсор з встановленими протоколами (правилами) спілкування з іншими агентами;

S_2 – сенсор сигнатурного аналізу, за яким розпізнавання вірусів здійснюється за допомогою сигнатур вірусів. Під час антивірусного діагностування комп'ютерної системи сенсор шукає в базі сигнатуру і в разі виявлення повідомляє про зараження;

S_3 – сенсор контрольних сум, який здійснює перевірку цілісності даних, які передаються в цифровому представленні. Розраховується значення, додаючи всі числа з вхідних даних;

S_4 – сенсор евристичного аналізу, за яким виявляють шкідливе програмне забезпечення за його типовою поведінкою, здатний визначати невідоме ШПЗ. Аналіз проводиться за допомогою пошуку у файлах потенційно небезпечних команд і їх послідовностей;

S_5 – сенсор порівняльного аналізу, за яким здійснюється звернення до файлів. Через інтерфейс програмування додатків API і через драйвер дискової підсистеми IOS. Якщо дані про файл, отримані за першим способом, відрізняються від аналогічних, отриманих за другим способом, відповідно об'єкт однозначно інфікований;

S_6 – сенсор – «віртуальна приманка», який наражається на атаки чи несанкціоноване дослідження, що надалі дає змогу вивчати стратегію зловмисника і визначати перелік засобів, за допомогою яких можуть бути здійснені атаки на реально існуючі об'єкти КС. Якщо не проводиться віддалене адміністрування мережі, то весь вхідний ssh-трафік перенаправляється на даний сенсор.

Процесор обробляє вхідні дані та визначає рівень небезпеки визначеного об'єкта в КС. У базі знань запропоновано розміщення списку наперед відомих файлів, що не несуть загрози. Блок «переконання» забезпечить агент знаннями в нестандартних ситуаціях. Це забезпечить зниження кількості хибних спрацювань під час діагностування КС на наявність нового ШПЗ. Системою відповідних фільтрів для кожного з сенсорів запропоновано встановлювати коефіцієнти для

оцінювання небезпеки об’єктів. Перевищення встановленої межі значень коефіцієнтів, зокрема досвід усіх агентів, свідчитиме про наявність ШПЗ в КС.

Рівень суб’єктивності агента антивірусної мультиагентної системи безпосередньо залежить від того, чи наділений він символьними уявленнями, що вимагаються для організації міркувань, або на противагу цьому він працює тільки на рівні образів (субсимвольних), пов'язаних з сенсомоторним регулюванням. Для виконання умови пошуку нового ШПЗ агенти антивірусної МАС повинні бути інтелектуальними. Інтелектуальні агенти повинні мати яскраво виражену індивідуальність і характеризуватися відповідною поведінкою в співтоваристві з агентами, а також прагненням використовувати ресурси інших агентів для досягнення поставлених цілей. Переваги інтелектуальних агентів зведені у таблиці.

Агент є гнучкою компонентою системи, оскільки кількість сенсорів обмежується тільки потужністю комп’ютерної системи або кількістю допустимих ресурсів, які забезпечують необхідний рівень продуктивності наявної КС. З появою нових методів АД можливим залишається нарощувати кількість сенсорів в агенті. Під час функціонування агент має можливість навчатись і адаптувати власну поведінку, опираючись на власний досвід і досвід інших агентів. Принцип функціонування агента наведено на рис. 4.

Переваги інтелектуальних агентів над неінтелектуальними

Характеристика	Когнітивні агенти	Реактивні агенти
Внутрішня модель зовнішнього світу	Розвинута	Примітивна
Роздуми	Складні і рефлексивні роздуми	Прості однокрокові роздуми
Мотивація	Розвинута система мотивації, переконання, бажання, наміри	прості переконання, пов’язані з виживанням
Пам’ять	Є	Немає
Реакція	Повільна	Швидка
Адаптивність	Мала	Висока
Модульна архітектура	Є	Немає
Склад багатоагентної системи	Невелике число автономних агентів	Велика кількість залежних одне від одного агентів

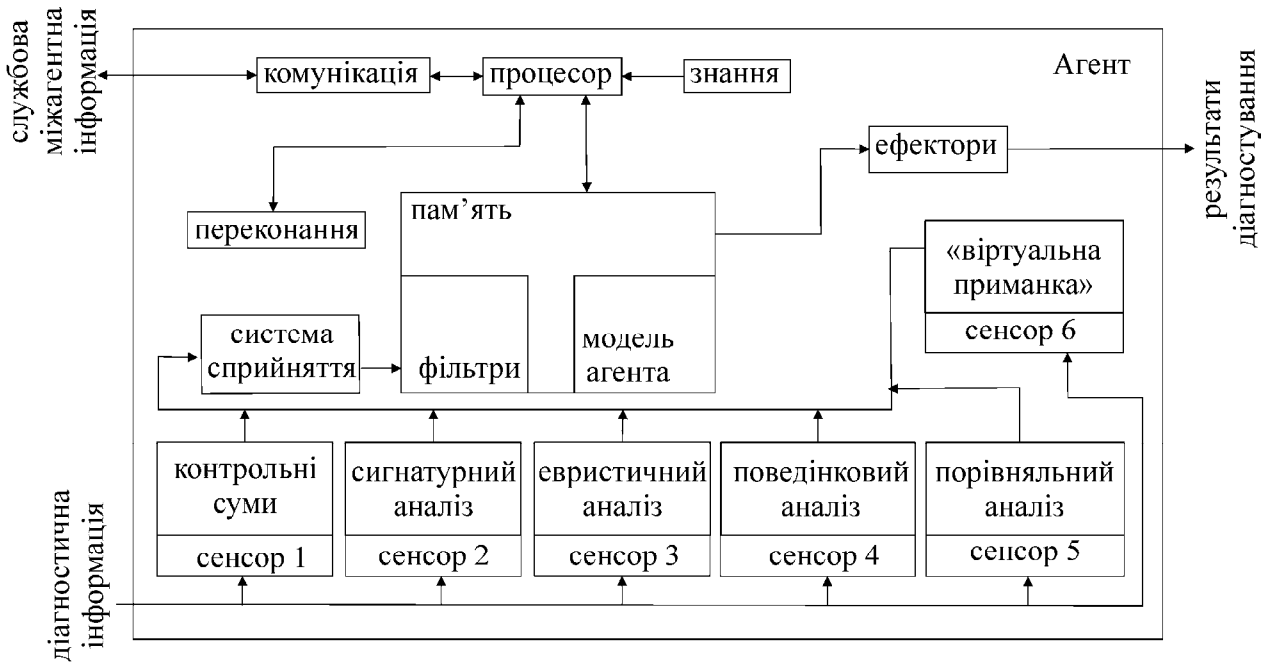

Рис. 4. Загальна схема функціонування агента антивірусної мультиагентної системи

На вхід кожного сенсора подається діагностична інформація відповідно до їх функційних можливостей.

Результати роботи сенсорів контрольних сум та сигнатурного аналізу можуть не потребувати повного залучення до роботи агента для сигналізування появи вірусів, але в сукупності із результатами інших сенсорів і комунікації з іншими агентами може сигналізувати виявлення такого ШПЗ, як ботнет.

Блок системи сприйняття проводить зведення інформації до загального вигляду для подальшої роботи.

Інформація зведеного вигляду надходить на вхід фільтрів. Отримуючи дані з блока переконань, фільтри відкидають дані, які генеруються довіреними програмами чи вузлами (див. рис. 5).

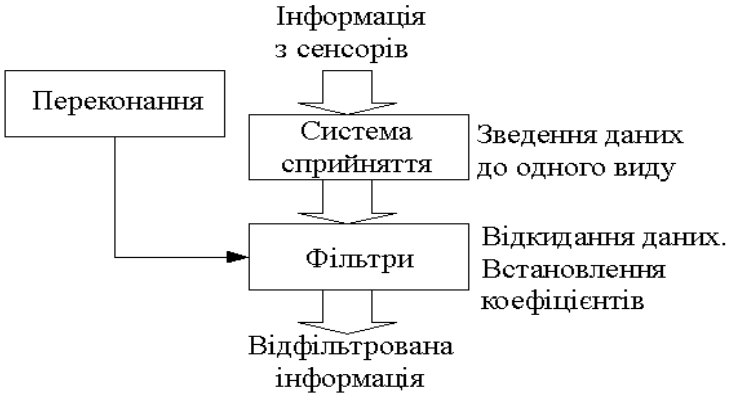

Рис. 5. Структура блока виконання фільтрування вхідних даних

Залежно від рівня небезпеки виявлених атак фільтрами встановлюються коефіцієнти.

Отримані дані від фільтрів подаються на процесор агента, який визначає чи є КС інфікованою. За недостатньої кількості даних, агент спілкується з іншими агентами на наявність подібних проявів у діях програм. Наявність чи відсутність інформації від інших агентів впливає на остаточне рішення агента щодо конкретного файла чи процесу (див. рис.6).

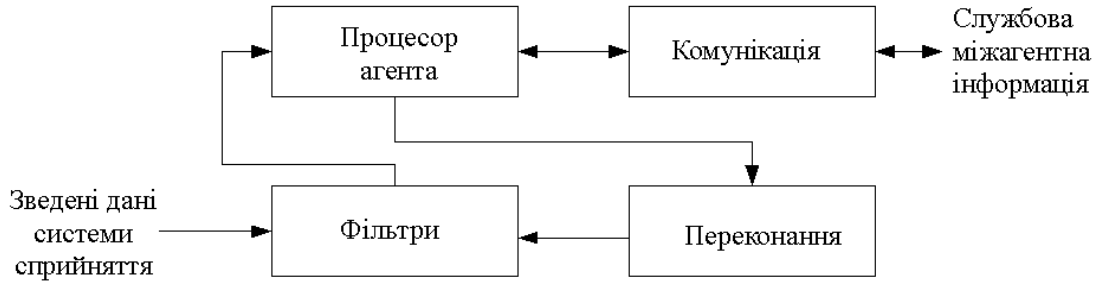

Рис. 6. Структура блока виконання зміни переконань

Під час порівняння отриманих результатів з даними в блоці переконань проводяться зміни системи коефіцієнтів та довірених вузлів. Відповідно проводиться самонавчання системи.

Блок комунікації відповідає за шифрування і дешифрування міжагентної інформації (див. рис. 7).

Рис. 7. Структура блока комунікації

Результати роботи агента подаються на ефектори, які є засобами впливу на КС. У разі виявлення ШПЗ агент за посередництвом ефекторів блокує процес чи процеси, які відповідають за роботу ШПЗ, і як засіб сповіщення повідомляє користувача візуальними і звуковими повідомленнями.

Модель агента забезпечує цілісність структури агента, яка реалізується системою контрольних точок, що характеризують роботоздатність цього агента. Також після перевірки систематично зберігаються критичні елементи агента для подальшого їх відтворення у разі атаки на антивірусну МАС чи можливих збоїв у системі.

Агент може активувати для повторної перевірки вибрану кількість сенсорів для уточнення результатів.

За можливих ситуацій, пов'язаних з тимчасовою відсутністю зв'язку, антивірусний агент є роботоздатною автономною одиницею, яка забезпечує комплекс заходів для виявлення ШПЗ, опираючись на останні оновлення знань і корекції у системі переконань.

Висновки

Запропонована стратегія антивірусного діагностування комп'ютерних систем на наявність шкідливого програмного забезпечення за рахунок використання мультиагентної системи, що дозволяє зменшити час виявлення шкідливого програмного забезпечення та зменшити кількість хибних спрацювань.

Розроблено структуру агента мультиагентної системи для антивірусного діагностування комп'ютерних систем.

Ця стратегія є основою для розроблення нового методу антивірусного діагностування комп'ютерних систем на наявність шкідливого програмного забезпечення на базі антивірусної МАС для підвищення достовірності антивірусного діагностування комп'ютерних систем.

1. Савенко О.С. Дослідження антивірусних технологій діагностування комп'ютерних систем на наявність шкідливого програмного забезпечення / О.С. Савенко, С.М. Лисенко, А.Ф. Крищук // Тр. XII междунар. научн.-практ. конф. "Современные информационные и электронные технологии" (СИЭТ-2011), Т. 1 – Одесса: Нац. политехн. Ун-т, 2011. – С. 95–96. 2. Гошко С.В. Энциклопедия по защите от вирусов / С.В. Гошко. – М.: СОЛОН-Пресс, 2005. – 352 с. 3. Касперски К. Техника и философия хакерских атак / К. Касперски. – М. : СОЛОН-Пресс, 2004. – 272 с. 4. AV Comparatives laboratories [електронний ресурс] – Режим доступу http://www.av-comparatives.org. – Назва домашньої сторінки. 5. Corporate Endpoint Protection Products Group Test: Socially-Engineered Malware Q2 2010 [електронний ресурс] – Режим доступу http://www.nsslabs.com/research/endpoint-security /anti-malware/q2-2010-endpoint-protection-product-group-test.html 6. Shoham Y. Multiagent Systems Algorithmic, Game-Theoretic, and Logical Foundations / Yoav Shoham, K. Leyton-Brown. – Cambridge University Press, 2009. – 504 p. 7. Alkhateeb F. Multi-Agent Systems / Faisal Alkhateeb, Eslam Al Maghayreh, Iyad Doush. – Modeling, Control, Programming, Simulations and Applications, 2011. – 522 p.