виявляти нові невідомі троянські програми та підвищує достовірність і ефективність процесу діагностування комп'ютерних систем на наявність троянських програм.

Розроблено програмне забезпечення, яке дозволяє здійснювати антивірусні моніторинг та сканування, і задачею якого є діагностування КС на наявність як відомих, так невідомих троянських програм. Отримані результати діагностування КС на наявність ТП показали підвищення достовірності ТП до 74 %, що на 5-15 % вище у порівнянні з відомими засобами діагностування КС на наявність нових троянських програм.

Література

1. Савенко О.С. Дослідження методів антивірусного діагностування комп'ютерних мереж / Савенко О.С., Лисенко С.М // Вісник Хмельницького національного університету. – 2007. – № 2, Т.2. – С. 120-126.

2. Савенко О.С. Процес виявлення троянських програм з використанням поведінкової моделі троянських програм на основі матриць відношень / О.С. Савенко, С.М. Лисенко // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2007. – № 1. – С. 69-74.

3. Савенко О.С. Модель процесу пошуку троянських програм в персональному комп'ютері / Олег Савенко, Сергій Лисенко // Радіоелектронні і комп'ютерні системи. – 2008. – № 7. – С. 87-92.

4. Савенко О.С. Использование нечеткой логики для поиска троянских программных продуктов в вычислительных системах / О.С. Савенко, Р.П. Графов, С.М. Лисенко // Вісник Чернівецького національного університету. – 2009. – № 6. – С. 25-31.

5. Савенко О. Розробка процесу виявлення троянських програм на основі використання штучних імунних систем / Олег Савенко, Сергій Лисенко // Вісник Хмельницького національного університету. – 2008. – № 5. – С. 183-188.

6. Савенко О. Алгоритми пошуку троянських програм в персональних комп'ютерах / Олег Савенко, Сергій Лисенко // Радіоелектронні і комп'ютерні системи. – 2009. – № 6. – С. 98-103.

7. Лисенко С.М. Розробка програмного забезпечення реалізації інтелектуального методу пошуку троянських програм в персональних комп'ютерах / С.М. Лисенко, А.П. Гонтар, А.С. Шевцов // Вісник Хмельницького національного університету. – 2010. – № 1, Том 1. – С. 98-105.

Надійшла 16.5.2010 р.

УДК 004.492.3

М.Д. МАРКОВСЬКИЙ, О.В. ПОМОРОВА
Хмельницький національний університет

РОЗРОБКА МЕТОДУ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СЕРВІСІВ В ГЛОБАЛЬНИХ ТА ЛОКАЛЬНИХ МЕРЕЖАХ

В роботі проведено аналіз сучасного стану в галузі антивірусного програмного забезпечення, розроблено новий метод передачі оновлень баз антивірусів, що ґрунтується на зомбі мережі, яка поєднує в собі децентралізовану (P2P) та централізовану топологію.

In operation the analysis of a present status of the anti-virus software has been carried out. The new method of transmission of signatures of anti-virus basises which is grounded on the zombie network which joints in itself decentralised (P2P) and the centralised topology is developed.

Ключові слова: антивірус, p2p, бот, ботнет, передача даних, захист, безпека.

Комп'ютерні технології на сьогодні інтенсивно впроваджуються у різні галузі, зокрема банківські системи та комунікаційні системи, медичні комплекси, системи керування атомними станціями і т. і.

При цьому все більшої актуальності набуває стабільність та надійність функціонування програмного забезпечення (ПЗ). Наряду з корисним програмним ПЗ з'являються і програмні додатки руйнівної та дестабілізуючої дії, зокрема, таке шкідливе програмне забезпечення, як комп'ютерні віруси.

За статистикою, з кожним роком кількість шкідливого програмного забезпечення зростає. З 1992 року по 2007 рік було виявлено близько 2 млн унікальних шкідливих програм, а за період з 2007 до 2008 року – вже 15 мільйонів [1].

Збільшення кількості шкідливого програмного забезпечення призводить до зростання частоти знищення інформації, викрадення паролів та кодів, дестабілізації функціонування комп'ютерних систем (КС), що у результаті збільшує фінансові втрати користувачів. Неможливо в повному обсязі підрахувати світовий фінансовий збиток, що наноситься вірусами. За даними досліджень «Symantec», кожна велика корпорація щорічно втрачає близько 2 млн доларів в результаті кібератак.

З огляду на тенденції збільшення кількості вірусів та фінансових втрат в результаті їх дій актуальною є задача забезпечення захисту комп'ютерних систем. На підприємствах, зазвичай, усі або велика кількість КС об'єднані в мережу. Якщо хоча б один комп'ютер мережі заражений вірусом, то існує загроза зараження всієї мережі, що призводить до збільшення ризиків фінансових втрат.

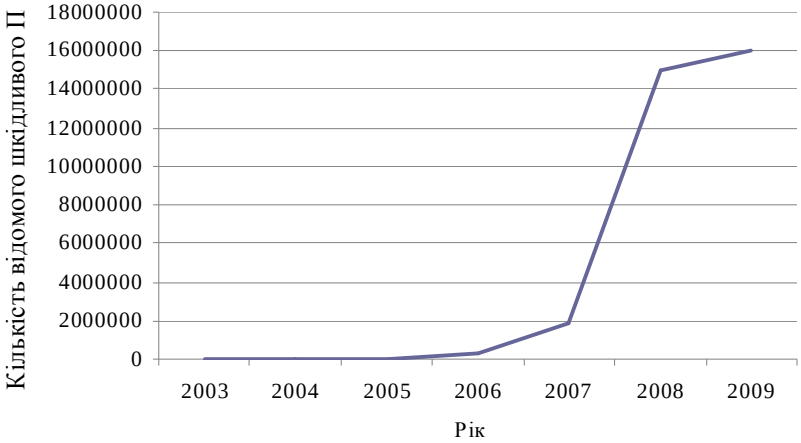

Рис. 1. Графік динаміки зростання кількості шкідливого програмного забезпечення за даними «Лабораторії Касперського»

Використання антивірусного програмного забезпечення значно зменшує ризики зараження КС вірусами. Однак, регулярно з'являються нові віруси, тому антивірусні лабораторії стараються якнайшвидше створити засоби їх виявлення.

Найкращими антивірусами на сьогодні є Dr.WEB, Kaspersky Antivirus та McAfee-GW-Edition (SecureWeb-Gateway). У таблиці 1 наведені результати тестування надійності антивірусного ПЗ.

Таблиця 1

Показники надійності антивірусів на основі тестування в лабораторії FomSoft

Назва антивірусу	Пропущено вірусів за період спостерігання з 10.2008 по 09.2009 р.													Надійність захисту, розрахунок за формулою Pav = (Nvir – Nbad) / Nvir
	Листопад з 20	Грудень з 15	Січень з 16	Лютий з 18	Березень з 6	Квітень з 38	Травень з 26	Червень з 20	Липень з 27	Серпень з 26	Вересень з 57	Жовтень з 25	Всього з 294	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a-squared			2	1	1	6	7	1	0	1	6	5	30 з 259	0.884
AhnLab-V3	10	8	7	8	2	8	10	9	4	10	21	13	110	0.625
AntiVir (AVIRA)	5	1	2	3	0	3	3	2	0	0	2	2	23	0.921
Antiy-AVL					2	9	14	9	12	13	20	9	88 з 225	0.608
Authentium	5	5	7	3	3	10	20	6	13	6	24	5	117	0.602
Avast	2	2	4	1	4	5	5	5	7	0	4	7	46	0.843
AVG	6	5	2	1	4	5	6	4	4	2	4	7	50	0.829
BitDefender	2	1	5	0	4	6	7	4	3	1	8	7	48	0.836
CAT-QuickHeal	11	6	6	4	3	7	6	3	2	6	12	7	73	0.751
ClamAV	8	0	10	6	2	14	19	15	19	15	38	14	160	0.455
Comodo			10	8	3	14	12	7	5	9	18	7	93 з 259	0.640
DrWeb	1	0	1	0	0	2	2	2	0	1	4	3	16	0.945
eSafe	9	6	5	8	3	8	15	10	7	6	27	14	120	0.591
eTrust-Vet	13	8	9	10	5	9	13	14	13	12	25	14	145	0.506
F-Prot	3	5	8	2	2	11	20	6	13	6	23	7	106	0.639
F-Secure	3	0	7	0	0	4	5	2	0	4	4	5	34	0.884
Fortinet	8	4	7	5	2	8	10	6	5	12	20	11	98	0.666
GData	0	0	1	0	4	4	3	3	2	0	2	3	22	0.925
Ikarus	2	0	2	1	1	7	13	8	1	3	6	3	47	0.840
Jiangmin									8	9	19	14	50 з 135	0.629
K7AntiVirus	7	2	5	4	1	6	8	3	4	7	14	10	71	0.758
Kaspersky	3	0	3	0	0	2	6	3	0	4	4	2	27	0.908
McAfee	9	6	8	5	0	5	8	4	1	0	17	7	70	0.761
McAfee+Artemis			6	4	0	5	7	2	0	0	3	5	33 з 259	0.872
McAfee-GW-Edition	5	1	1	3	0	1	1	1	0	0	4	1	18	0.938
Microsoft	6	2	6	3	4	5	6	6	3	4	7	8	60	0.795
NOD32	3	2	3	2	1	3	9	4	3	4	10	5	49	0.833
Norman	9	5	7	4	4	9	10	5	8	9	14	10	94	0.680

Продовження табл. 1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
nProtect			4	4	2	14	11	8	11	14	27	14	109 з 259	0.579
Panda	9	5	7	4	4	12	8	2	3	3	10	6	73	0.751
PCTools	11	8	9	5	3	17	20	10	19	20	45	21	188	0.360
Prevx	11	4	9	13	1	7	8	9	7	5	12	9	95	0.676
Rising	9	5	14	9	4	10	14	13	14	16	31	11	150	0.489
Sophos	5	2	4	2	1	4	6	8	3	1	6	8	50	0.829
Sunbelt	10	12	11	8	1	9	13	6	8	6	15	14	118	0.598
Symantec (Norton AV)	9	8	8	2	4	3	8	3	6	2	9	6	68	0.768
TheHacker	10	10	10	6	2	12	9	7	9	9	23	9	116	0.605
TrendMicro	10	7	6	4	4	5	12	13	12	8	21	12	114	0.612
VBA32	6	3	8	4	2	5	6	4	4	6	13	14	75	0.744
ViRobot	6	6	10	8	3	9	16	14	15	11	20	14	132	0.551
VirusBuster	10	4	11	3	3	8	13	6	4	7	10	7	86	0.707

Pav – вірогідна оцінка якості антивірусу, чим ближча вона до одиниці, тим краще антивірус.

Nvir – загальне кількість зафіксованих шкідливих об'єктів на КС.

Nbad – кількість шкідливих об'єктів, котрі антивірус не виявив.

З таблиці видно, що тільки невелика кількість відомого антивірусного ПЗ виявила майже всі віруси.

На сьогодні відомі 4 основні типи ПЗ для боротьби з вірусами [3]:

1. Сканери – перевіряють файли, сектори та системну пам'ять на наявність відомих вірусів. Для детектування вірусу використовують сканування за маскою (маска – певний послідовний код, притаманний тому чи іншому вірусу), евристичні методи та інше.

2. Ревізори диску – підраховують CRC-суми файлів на диску, потім зберігають їх в своїй базі. При наступному запуску перевіряють дані з бази та заново підраховані CRC-суми. Якщо вони не співпадають, антивірус вважає файл зараженим.

3. Резидентні монітори – постійно знаходяться в оперативній пам'яті та слідкують за операціями на жорсткому диску, змінних носіях та оперативній пам'яті.

4. Імунізатори. Найпоширеніші 2 типи імунізаторів: перший перевіряє файл на зміни, шляхом додавання виконуючого коду в кінець файлу, а другий зразу дописує в файл код, який сигналізує вірусу, що цей файл вже заражений.

Кожен день створюються нові віруси, а розробники антивірусного ПЗ намагаються їх знешкодити. Знайшовши алгоритм знешкодження, фірма-розробник антивірусу розповсюджує його серед користувачів даного антивірусу шляхом розміщення на сервері оновлень антивірусних баз. Кожен користувач антивірусу повинен оновлювати свої антивірусні бази, щоб запобігти зараженню свого комп'ютера.

На даний час, механізм отримання баз оновлення у найпоширеніших антивірусів (ESET NOD, Dr.Web, Антивірус Касперського) використовує віддалений або локальний сервер з оновленнями. Клієнти під'єднуються до такого сервера та отримують оновлення антивірусних баз. Даний механізм завантаження оновлень є централізованим.

Отримання оновлень проходить за розкладом або за командою користувача. При використанні розкладу антивірусне ПЗ раз у певний період часу з'єднується з сервером та опитує його на наявність оновлення антивірусних баз. Якщо оновлення є, клієнт завантажує його та від'єднується від сервера, якщо нема – від'єднується від сервера. Перевагами даного механізму є те, що клієнт має адресу сервера з останніми оновленнями, та може їх отримати в будь-який час, коли сервер доступний.

Однак, існує і ряд недоліків даного механізму:

- при несправності сервера, відсутності з'єднання та відмові у наданні послуг на отримання оновлення комп'ютери не матимуть можливості оновити антивірус;
- перевантаження сервера запитами може призвести до відмови сервісу;
- навантаження на канал передачі даних може значно збільшити час проходження пакетів між сервером та клієнтами (якщо сервер локальний, то найчастіше він надає ще ряд сервісів: пошта, DHCP, сервер баз даних та ін., відмова яких може призвести до додаткових фінансових втрат).

У результаті рівень захищеності КС знижується і зростає імовірність нанесення шкоди користувачам КС, зокрема у локальних та глобальних мереж.

Постановка задачі

Для підвищення ефективності сервісу оновлення антивірусних баз в локальних та глобальних мережах необхідно розробити метод, котрий забезпечить децентралізований доступ до баз оновлень.

Децентралізований метод оновлення антивірусних баз

Для запобігання вище згаданим недолікам пропонується використати метод оновлення антивірусних баз з використанням технології крапка-крапка (P2P), що базується на використанні сервісу, що утворює ботнет.

Ботнет – це мережа комп'ютерів, на кожному з яких встановлено однакове програмне забезпечення (програми-боти), яке без відома користувача може зв'язуватись з іншим комп'ютером цієї мережі та передавати між ними дані, а іноді і керувати КС.

На даний момент існує велика кількість ботнетів, більшість яких шкідливими. Комп'ютерами, що входять до ботнет-мережі, господар може керувати звідки завгодно: з іншого міста, країни або навіть з іншого континенту, а організація мережі Інтернет дозволяє робити це анонімно. Комп'ютер, що входить до складу бот-мережі, називають зомбованим або зомбі.

Ботнети використовуються зловмисниками для розв'язання кримінальних задач різного характеру: від розсилки спаму до атак на державні мережі.

Класифікація ботнетів ґрунтується на архітектурі ботнетів і протоколах, що використовуються для управління програмами-роботами.

Найпоширенішими є 2 типи архітектури ботнету [5]:

1) Ботнети з єдиним центром. У ботнет з такою архітектурою всі зомбі-комп'ютери з'єднуються з одним центром керування, або C&C (Command & Control Centre). C&C очікує підключення нових ботів, реєструє їх у своїй базі, стежить за їх станом та видає їм команди, обрані власником ботнету зі списку всіх можливих команд для бота. Відповідно, в C&C видно всі підключені зомбі-комп'ютери, а для управління централізованою зомбі-мережею господареві мережі необхідний доступ до командного центру (рис. 2).

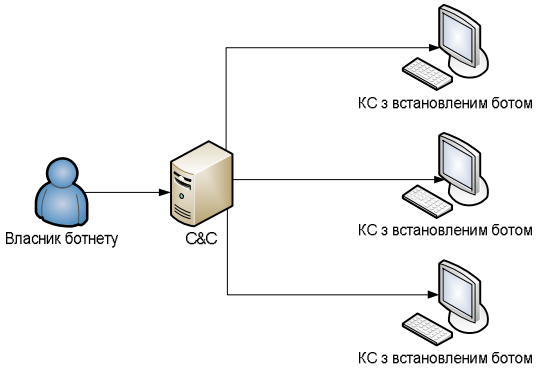

Рис. 2. Централізована топологія (C&C) ботнет

Ботнети з централізованим управлінням є найпоширенішим типом зомбі-мереж. Такі ботнети є простими в реалізації і керуванні, вони швидко реагують на команди. Для нейтралізації ботнету з централізованим керуванням достатньо закрити центр керування.

2) Децентралізовані ботнети, або P2P-ботнети. У випадку децентралізованого ботнету усі боти з'єднуються не з центром керування, а з декількома інфікованими КС з зомбі-мережі. Команди передаються від бота до іншого. У кожного бота є список адрес кількох «сусідів», і при отриманні команди від будь-кого з них він передає її іншим, тим самим поширюючи команду далі. У цьому випадку зловмисникові, щоб керувати всім ботнетом, досить мати доступ хоча б до одного комп'ютера, що входить в зомбі-мережу (рис. 3).

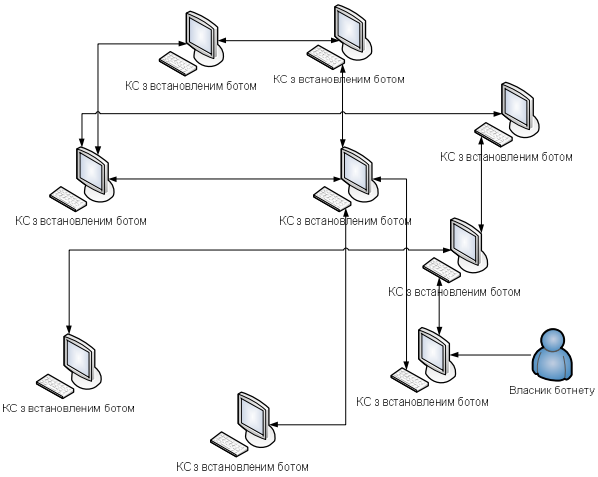

Рис. 3. Децентралізована топологія (P2P)

На практиці побудова децентралізованого ботнету не дуже зручна, оскільки кожному новому інфікованому комп'ютеру необхідно надати список тих ботів, з якими він буде зв'язуватися у зомбі-мережі. Набагато простіше спочатку направити бот на централізований сервер, де він отримає список пошукових роботів-«сусідів», а потім вже перемкнути бот на взаємодію через P2P-підключення. Така змішана топологія також відноситься до типу P2P, хоча на окремому етапі боти використовують C&C. Боротися з децентралізованими ботнетами набагато складніше, оскільки вони не мають центру керування.

Децентралізований метод завантаження оновлень антивірусних баз

Суть методу полягає в наступному: на кожній КС в мережі, де є антивірусне ПЗ, встановлюється програма-бот, котра відповідає за завантаження оновлень антивірусних баз. Кожен з таких ботів має зв'язок з декількома іншими ботами для обміну оновленими антивірусними базами. Зв'язок кожного бота з сервером оновлень не обов'язковий.

Антивірус завантажує оновлення на КС і замінює стандартний механізм завантаження оновлень антивірусних баз на механізм, що використовує ботнет. Після цього завантажується карта ботнету для локальної мережі.

Карта ботнету – це база відповідності MAC-адрес до IP-адрес. Карта потрібна для ідентифікації КС з встановленим ботом. Це зроблено з огляду на те, що близько 80 % IP-адрес в мережах – динамічні. Така база дає можливість боту знайти IP-адресу КС, на який встановлено інший бот.

При завантаженні антивірусу на КС, бот з'єднується з сервером для реєстрації на карті ботнету своєї мережі, перевіряє на доступність з'єднання з «друзями».

Якщо з'єднатися з сервером неможливо, то бот буде використовувати раніше завантажену карту. При відсутності карти бот починає сканувати свою підмережу на наявність ботів, встановлює з ними зв'язок та будує свою карту, а, в той же час перевіряє на наявність у цих ботів більш нової версії антивірусної бази (рис. 4).

Якщо бот встановив зв'язок з сервером та завантажив карту, на її основі він визначає «друзів», тобто КС, на яких встановлені такі ж боти і обирає серед них оптимальні за певними параметрами та відправляє їм пропозицію «дружби» – занесення адреси бота в список адрес, куди потрібно звертатись за оновленнями в першу чергу. Бот, до якого звертаються з пропозицією «дружити», може відхилити пропозицію. Операцію визначення «друзів» бот буде проводити один раз у певний період часу, який визначається самим ботом на основі аналізу частоти змін карти ботнету. Після цього бот регулярно звертається до «друзів» та запитує оновлення антивірусних баз. Якщо жоден з друзів не відповідає, бот використовує карту і з'єднується з ботами, що не входять до списку друзів або завантажує оновлення з сервера.

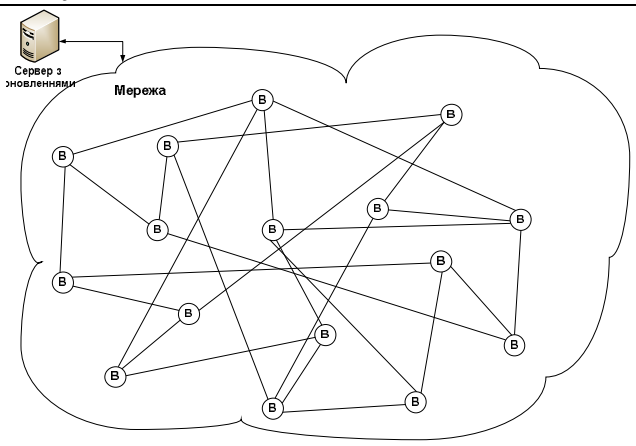

Рис. 4. Приклад встановлення зв'язків між ботами, де В – КС з встановленим сервісом

У випадку, якщо бот звертається до іншого з запитом на оновлення бази, а у бота-донора антивірусна база старіша ніж у бота-реципієнта – бот-донор завантажує новішу базу у бота-реципієнта.

Завантаження оновлень може проводитись 2-а шляхами:

1) якщо завантаження проходить з серверу оновлень, то база оновлень завантажується повністю з цього сервера;

2) використовуючи ботнет можна завантажувати базу від декількох ботів одночасно.

Розглянемо детальніше 2-й випадок. Оновлення від ботів будуть завантажуватись частинами. Бот-реципієнт підключається до першого бота-донора та починає завантажувати частину оновлення, розміром 128Кб (розмір може змінюватись). Як тільки почалось завантаження бот починає з'єднуватись з наступним ботом та завантажує наступну частину файлу. Так продовжується поки не завантажиться весь файл. Якщо в процесі завантаження один з ботів донорів встиг віддати свою частину файлу, від нього починає завантажуватись інша частина, згідно з чергою частин антивірусних баз (рис. 5).

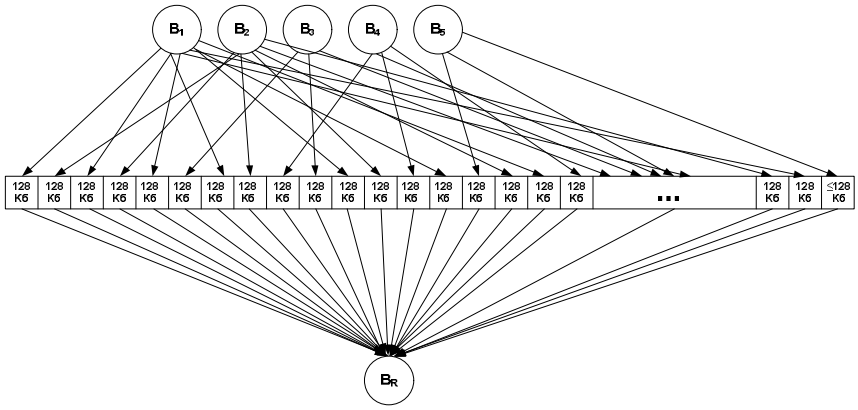

Рис. 5. Процес завантаження оновлень в ботнеті, де B_r – бот-реципієнт, $B_1 \ldots B_5$ – боти-донори, з яких завантажуються оновлення

Якщо в процесі завантаження буде виявлена новіша версія антивірусної бази ніж та, що завантажуються, всі завантаження будуть припинені і почнеться завантаження більш нової бази.

Можливості запропонованого методу представлені у табл. 2

Таблиця 2

Порівняльна характеристика методів завантаження оновлень

Можливість методу	Поєднання децентралізованого та традиційного методу	Традиційний метод
Завантаження оновлень з сервера	Так	Так
Завантаження оновлень з будь-якого комп'ютера в мережі, де встановлено антивірусне ПЗ	Так	Ні
Вимога оновлення антивірусних баз за розкладом	Так	Так

Основною перевагою запропонованого методу є те, що при оновленні антивірусної бази одного з комп'ютерів локальної мережі оновляться бази всіх інших комп'ютерів в мережі, що підвищує швидкість оновлення антивірусних баз в локальних мережах, а відповідно і їх надійність.

Висновки

Запропонований метод, на прикладі оновлення антивірусних баз, дає нам можливість оцінити його

переваги. Всі КС в мережі оновляться антивірусні бази, якщо хоча б одна КС має оновленні антивірусні бази.

Доступ до серверу оновлень для всіх КС в мережі стає не обов'язковим, і у випадку неможливості отримання останніх оновлень з сервера даний метод дозволяє завантажити оновлення у тих КС, які отримали його раніше, або якщо мають зв'язок з іншим сервером (віддаленим або локальним).

Завантаження оновлень в кількох ботів одночасно дозволяє в процесі отримання оновлень перевіряти КС-донорів на наявність новішої антивірусної бази.

Використання розробленого методу отримання оновлень антивірусних баз підвищує рівень захищеності КС в мережі від шкідливого програмного забезпечення, що, в свою чергу, дозволяє скоротити фінансові втрати.

Література

1. Гостев А. Kaspersky Security Bulletin 2009. Развитие угроз в 2009 году [Електронний ресурс] / Гостев А., Масленников Д., Асеев Е. – Режим доступу: http://www.securelist.com/ru/analysis/208050608/Kaspersky_Security_Bulletin_2009_Razvitie_ugroz_v_2009_godu. – 2010.

2. Савенко О.С. Дослідження методів антивірусного діагностування комп'ютерних мереж / О.С. Савенко, С.М. Лисенко // Вісник Хмельницького національного університету. – 2007. – № 2, Т. 2. – С. 120-126.

3. Текущий рейтинг антивирусов. Лучший антивирус [Електронний ресурс]. – Режим доступу: http://www.antivirus.ru/AntiVirPS.html. – 2009.

4. Дериев И. Корпоративные антивирусы: богатство выбора / И. Дериев // Компьютерное обозрение – 2007. – № 24 (690). – С. 19-23.

5. Гуркин Ю.Н. P2P. Файлообменные сети: принципы работы, используемые протоколы, безопасность / Ю.Н. Гуркин, Ю.А. Семенов // Телекоммуникационные сети и системы. – 2006. – № 11. – С. 62.

6. Камлюк В. Ботнеты / В. Камлюк [Електронний ресурс]. – Режим доступу: http://www.securelist.com/ru/analysis/204007610/Botnety. – 2008.

Надійшла 16.5.2010 р.

УДК 621.382

Ю.С. КРАВЧЕНКО, В. С. ОСАДЧУК, С. Ю. КРАВЧЕНКО
Вінницький національний нехнічний університет

ДОСЛІДЖЕННЯ ЕМІСІЙНО-СПЕКТРАЛЬНОГО ПЕРЕТВОРЮВАЧА ДЛЯ КОНТРОЛЮ ПЛАЗМОХІМІЧНОГО ПРОЦЕСУ

Розроблена математична модель частотного емісійно-спектрального перетворювача для контролю плазмохімічного процесу. Перетворювач містить лямда-діод, який утворено на базі двох біполярних транзисторів, активний індуктивний елемент та фоторезистор. Отримано аналітичний вираз функції перетворення та чутливості. Проведено теоретичні та експериментальні дослідження, які показали, що їх розбіжність складає ± 5 %.

A mathematical model is developed frequency emission-spectral transformer for control of plasmo-chemical process. A transformer is contained by a λ-diode which is formed on the base of two BPT, active inductive element and photoresistor. Analytical expression of function of transformation and sensitiveness is got. Theoretical and experimental researches, which rotined that their divergence made, are conducted ± 5 %.

Ключові слова: емісійно-спектральний перетворювач, плазмо-хімічні процеси.

Вступ

Основним напрямком в технології ВІС та НВІС при формуванні топології інтегральної схеми є застосування методів "сухого" травлення, які ґрунтуються на застосуванні принципів фізичної, хімічної або фізико-хімічної взаємодії активних частинок низькотемпературної нерівноважної плазми (атомів, іонів, радикалів) з поверхнею оброблюваного матеріалу [1, 2].

Серед сучасних методів контролю і діагностики плазмових процесів [3 – 6] найбільше застосування знайшли методи безконтактного контролю [7], які базуються на реєстрації та використанні власного оптичного випромінювання нерівноважної плазми, дослідженні спектру такого випромінювання і розробці ефективних перетворювачів оптичного випромінювання для аналізу та контролю параметрів нерівноважної плазми і технологічного процесу. Такі методи діагностики і контролю вирізняються високим ступенем достовірності, надійності та економічності. Оптична емісійна діагностика і контроль не впливають на хід цільового процесу, не вносять додаткових збурень у саму плазму, достатньо просто вписуються в системи автоматизованого контролю і управління загальним технологічним процесом.

Експериментальні дослідження

Електрична схема оптичного частотного перетворювача надана на рис. 1.