УДК 004.056

Смоляр В.Г., к.т.н., доцент,
Бубирєв І.С., студент групи 601-ТСм,
Черницька І.О., асистент
Полтавський національний технічний університет
імені Юрія Кондратюка

ПІДВИЩЕННЯ СИСТЕМИ ЗАХИСТУ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ З ВИКОРИСТАННЯ КОМПЛЕКСУ АНТИВІРУСНИХ ПРОГРАМ

В статті розглянуто підхід щодо захисту локальної комп'ютерної мережі (ЛКМ) від шкідливого програмного забезпечення (вірусів і т.і.). Наведено результати досліджень підвищення захисту ЛКМ за рахунок встановлення різних антивірусних програмних комплексів на комп'ютерні пристрої однієї мережі. Проведено аналіз результатів досліджень.

Ключові слова: *локальна комп'ютерна мережа, шкідливе програмне забезпечення, антивірусні програми.*

Вступ

На сьогоднішній день проблема захисту комп'ютерних мереж від вірусних атак є актуальною. За оцінками мережевих аналітиків загальний збиток від шкідливого програмного забезпечення (ПЗ) складає мільйони доларів [1]. При цьому вірусна небезпека з кожним роком зростає все більше і більше. Пояснюється це, з одного боку зростаючою кількістю і різноманітністю шкідливого ПЗ, а з іншого - вразливістю локальних мереж у зв'язку з проникненням в них вірусів з зовнішніх носіїв та мереж.

Як показує практика експлуатації комп'ютерів та мереж проблемі захисту від вірусних атак не приділяється належної уваги. Навіть розробники комплексних систем інформаційної безпеки часто обмежуються

рекомендаціями з вибору антивірусного ПЗ, а також надають допомогу в його налаштуванні. Небезпека зараження локальних мереж реальна для будь-якого підприємства,організації чи установи, але реальний розвиток вірусної епідемії може набути в локальних мережах великих господарсько-виробничих комплексів з територіально-розгалуженою інфраструктурою. Їх обчислювальні мережі, як правило, створені поетапно, з використанням різного апаратного і програмного забезпечення. Очевидно, що для таких підприємств питання антивірусного захисту стає дуже складним, причому не тільки в технічному, а й у фінансовому плані, тому що не кожна установа може дозволити собі придбання таких комплексів.

Підхід до захисту локальної комп'ютерної мережі

Рішення питання щодо захисту ЛКМ від вірусних загроз досягається шляхом поєднання організаційних заходів та програмно-технічних рішень. Даний підхід не вимагає великих технічних і негайних фінансових витрат, і може бути застосований для комплексного антивірусного захисту локальної мережі в будь-якому підприємстві. При цьому передбачається, що в основу побудови системи антивірусного захисту можуть бути покладені наступні принципи [2]:

- принцип реалізації єдиної технічної політики при обґрунтуванні вибору антивірусних продуктів для різних сегментів локальної мережі;
- принцип повноти охоплення системою антивірусного захисту всієї локальної мережі організації;
- принцип безперервності контролю локальної мережі підприємства, для своєчасного виявлення комп'ютерної інфекції;
- принцип централізованого управління антивірусним захистом.

Принцип реалізації єдиної технічної політики передбачає використання у всіх сегментах локальної мережі тільки антивірусного ПЗ, рекомендованою статистикою антивірусного захисту та на основі власних досліджень. Ця політика носить довгостроковий характер, затверджується керівництвом

підприємства і є основою для цільового і довготривалого планування витрат на придбання антивірусних програмних продуктів і їх подальше оновлення.

Принцип повноти охоплення системою антивірусного захисту локальної мережі передбачає впровадження в мережу антивірусних програмних засобів захисту з організаційно-режимними заходами захисту інформації [3].

Принцип безперервності контролю за антивірусним станом локальної мережі мають на увазі таку організацію її захисту, при якій забезпечується постійна можливість відстеження стану мережі для виявлення вірусів.

Принцип централізованого управління антивірусним захистом передбачає управління системою з одного органу з використанням технічних і програмних засобів. Саме цей орган організовує централізований контроль в мережі, отримує дані контролю або доповіді користувачів зі своїх робочих місць про виявлення вірусів і забезпечує впровадження прийнятих рішень з управління системою антивірусного захисту.

З урахуванням цих принципів в комплексній системі інформаційної безпеки створюється підрозділ антивірусного захисту, яка повинна вирішувати такі завдання:

- придбання, установка і своєчасна заміна антивірусних пакетів на серверах і робочих станціях користувачів;
- контроль правильності застосування антивірусного ПО користувачами;
- виявлення вірусів в локальній мережі, їх оперативне лікування, видалення заражених об'єктів, локалізація заражених ділянок мережі;
- своєчасне оповіщення користувачів про виявлені або можливих віруси, їх ознаках і характеристиках.

Структура системи захисту локальної комп’ютерної мережі з використання комплексу антивірусних програм

Одним з підходів захисту локальної комп’ютерної мережі є використання комплексу антивірусних програм.

Жодна антивірусна компанія не може дати сто відсоткової гарантії захисту свого продукту. Але ж проблема захисту існує і кожен системній адміністратор організації, установи чи підприємства або ж простий користувач хоче мати якомога надійніший захист своїх персональних або комерційних даних. Тому було запропоновано цей підхід. Суть якого полягає в тому, щоб в одній локальній мережі (рис. 1) на різних комп'ютерах, встановити різні антивірусні програмні забезпечення. Та цим самим підвищити захист ОС.

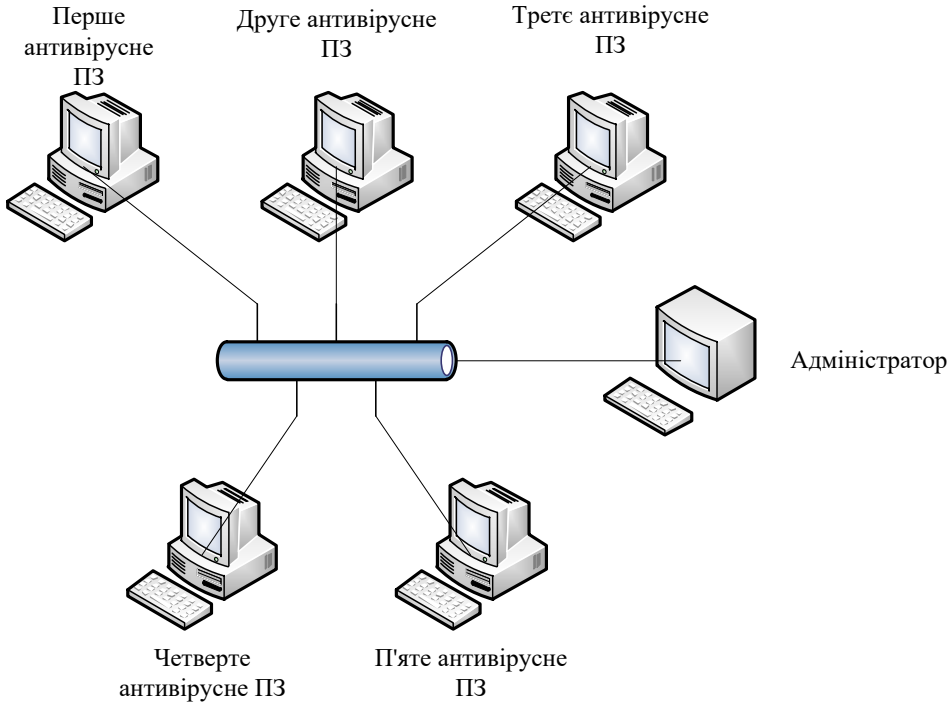

Рис. 1. Схема встановлення антивірусного програмного забезпечення

Після реалізації даного методу можна розрахувати підвищення захисту локальної комп'ютерної мережі на основі власного дослідження за допомогою класичної формули [5,6]:

$$P(A) = 1 - \big(1 - P(A1)\big) * \big(1 - P(A2)\big) * \ldots * \big(1 - P(An)\big), \quad (1)$$

де $P(A)$ – загальна імовірність знайдення вірусів,

$P(A1) - P(An)$ – імовірності знайдення вірусу кожною з установлених програм.

Аналіз ефективності системи захисту у ЛКМ за допомого даного методу

Провівши дослідження над комплексами антивірусних програм, взятих на основі опитування з 17 травня по 5 липня 2016 року [4], у порталі "Comss.one Антивіруси", було вибрано десять комплексів [3,7-14]. З них п’ять коштовні та п’ять безкоштовні. Кожен з цих комплексів були встановлені окремо та протестовані.

Таблиця 1.

Результати дослідження антивірусних комплексів

Антивірусний комплекс	Коштовні	Безкоштовні	Відсоток знайдених вірусів	Відсоток заблокованих посилань
Norton Security Premium	Так	-	93%	92%
McAfee LiveSafe (2016)	Так	-	89%	91%
Webroot SecureAnywhere Internet Security Plus (2016)	Так	-	87%	72%
Kaspersky Internet Security (2016)	Так	-	86%	68%
Trend Micro Internet Security 2016	Так	-	91%	88%
Avast Free Antivirus 2016	-	Так	98%	74%
AVG Antivirus Free (2016)	-	Так	86%	79%
Panda Free Antivirus (2016)	-	Так	89%	81%
Avira Free Antivirus 2016	-	Так	93%	95%
Qihoo 360 Total Security 8.6	-	Так	75%	36%

Підрахувавши середнє значення за виразом (1) дослідження можна зробити підсумки на скільки підвищилась загальний захист.

1) Середнє значення захисту мережі від знайдених шкідливих програм:

$$P(A) = 1 - (1 - 0{,}93) * (1 - 0{,}89) * (1 - 0{,}87) * (1 - 0{,}86) * (1 - 0{,}91) = 0.999873874$$

$$P(B) = 1 - (1 - 0{,}98) * (1 - 0{,}86) * (1 - 0{,}89) * (1 - 0{,}93) * (1 - 0{,}75) = 0.99999461$$

2) Середнє значення захисту мережі від заблокованих посилань:

$$P(\mathrm{C}) = 1 - (1 - 0{,}92) * (1 - 0{,}91) * (1 - 0{,}72) * (1 - 0{,}68) * (1 - 0{,}88) = 0.9999225856$$

$$P(D) = 1 - (1 - 0{,}74) * (1 - 0{,}79) * (1 - 0{,}81) * (1 - 0{,}95) * (1 - 0{,}36) = 0.999668032$$

Висновки

Отже, використовуючи запропонований підхід до захисту локальної комп'ютерної мережі, який полягає у встановленні декількох різних антивірусних програм на комп'ютери, дозволяє наблизити імовірність виявлення вірусів наскільки завгодно близько до одиниці (в залежності від кількості задіяних комп'ютерів та використаних антивірусних програм). Отримані експериментальні результати достовірні тільки для конкретних антивірусних програм та задіяних вірусів. За інших умов можливі відмінності. Саме запропонований підхід дозволяє нівелювати недоліки окремих програм.

Література:

1. *ТОП-10 комп'ютерних вірусів в історії. Частина 1[Електронний ресурс]. – Режим доступу: http://zillya.ua/top-10-kompyuternikh-virusiv-v-istori-chastina-1*
2. *Інформатика та інформаційні технології. Навчальний посібник / І. Г. Ліснича, І. В. Міссінг, Ю. Д. Романова, В. І. Шестаков, 2-е вид. - М.: Видавництво Ексмо, 2006. - 544с.*
3. *Офіційний сайт Kaspersky [Електронний ресурс]. - Режим доступу: http://www.kaspersky.ru/internet-security-center*
4. *Кращий антивірус 2016. Рейтинг користувачів [Електронний ресурс]. - Режим доступу: http://www.comss.ru/page.php?id=2758*
5. *Академія В.І.Смірнов / Курс вищої математики. Державне видавництво технічно - теоретичної літератури, Москва 1951. 627 с.*

6. Вентцель Е. С. Теория вероятностей / Е. С. Вентцель. – М.: Наука. Главная редакция физико-математической литературы, 1969. – 576 с.

7. Офіційний сайт Norton [Електронний ресурс]. - Режим доступу: https://ru.norton.com/security-101/

8. Офіційний сайт Webroot [Електронний ресурс]. - Режим доступу: https://www.webroot.com/

9. Офіційний сайт Mcafee [Електронний ресурс]. - Режим доступу: http://www.mcafee.com/ru/index.html

10. Офіційний сайт Trend Micro [Електронний ресурс]. - Режим доступу: http://www.trendmicro.com.ru

11. Офіційний сайт Avast [Електронний ресурс]. - Режим доступу: https://www.avast.ru/index

12. Офіційний сайт Panda [Електронний ресурс]. - Режим доступу: http://www.pandasecurity.com/ukraine/

13. Офіційний сайт Avira [Електронний ресурс]. - Режим доступу: http://www.avira.com/ru/free-antivirus-windows

14. Офіційний сайт 360 Total Security [Електронний ресурс]. - Режим доступу: https://www.360totalsecurity.com