УДК 681.323

В.М. Яйчук, Я.В. Максимович
Луцький інститут розвитку людини університету "Україна",
кафедра комп'ютерних технологій

ДО ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД УРАЖЕННЯ КОМП'ЮТЕРНИМИ ВІРУСАМИ

Досліджено проблему захисту інформації від комп'ютерних вірусів. Здійснено спробу виокремити найпоширеніші віруси та проаналізувати способи запобігання їх впливу на комп'ютерну систему.

Ключові слова: захист інформації, вірус, комп'ютерна програма.

The article reveals the problem of information protection within the paradigm of the computer viruses. The author tries to point out the main viruses and the ways how to prevent their influence upon the PC.

Key words: information protection, virus, computer program.

Вступ. Інформація як головне джерело управління, суспільного розвитку та рушій прогресу детермінує усвідомлення необхідності становлення та розвитку інформаційного суспільства. Відтак очевидною є необхідність захисту інформації, що циркулює в комп'ютерних та інформаційних мережах. У комп'ютерній техніці поняття інформаційної безпеки є вельми широким, воно охоплює і надійність роботи комп'ютера, і збереження цінних даних, і захист інформації від внесення до неї змін не уповноваженими персонами (конфіденційність), і збереження таємниці листування в електронному зв'язку. Відсутність аналізу проблеми захисту від комп'ютерних вірусів визначає актуальність статті.

Огляд літературних джерел. Сучасні наукові розвідки націлені на дослідження різних аспектів інформації: зокрема інформаційного забезпечення [3], створення інформаційного суспільства [1], інформаційної безпеки через призму політики [5].

Під комп'ютерним вірусом розуміємо комп'ютерну програму (сукупність програмних кодів), здатну без відома користувача комп'ютера створити свої копії та впровадити програмні коди у різноманітні файли або ресурси комп'ютерних систем [2].

Сьогодні комп'ютерні віруси не тільки швидко поширюються, але й впроваджуються в електронну пам'ять комп'ютера, прикріплюються до файлів і навіть переховуються на скрин-сейверах (різноманітні заставки-екрани). Комп'ютерний вірус може зіпсувати, зокрема змінити неналежним чином, будь-які файли, які містять різноманітну важливу інформацію, що, своєю чергу, завдає неймовірних збитків. До дій, які виконують комп'ютерні віруси, належать вільні або мимовільні спроби порушити працездатність комп'ютерних систем, спроби злому захищених систем, використання і поширення програм, які порушують працездатність комп'ютерних систем та їх надійність.

Виникнення комп'ютерних вірусів пов'язане з ідеєю створення програм, що самовідтворюються, досліджувати які розпочав ще в 1951 році американський вчений Д. фон Нейман. Перші експерименти в цьому напрямку проводилися в 1962 році при створенні комп'ютерної гри Darwin. У 1970 році було створено програму Creeper для однієї з перших комп'ютерних мереж ARPANET, яка саморозмножувалася. Для боротьби з нею створили програму Reaper [2].

Одночасно з появою в 1977 р. перших персональних комп'ютерів Apple II і початком їхнього масового продажу з'явилися і комп'ютерні віруси. Наприкінці 70-х років стали бурхливо розвиватися мережі на базі телефонних ліній. А з появою BBS одержав поширення новий вид комп'ютерного

хуліганства – завантаження в мережу програм, що знищують дані на комп'ютерах користувачів. На початку 80-х років з'явився перший завантажувальний вірус Elk Cloner для Apple II.

В історії комп'ютерних вірусів переломним став 1984 рік, коли італійські програмісти Р. Черути і М. Морокути підготували теоретичну базу для поширення на дискетах завантажувальних вірусів. Вони докладно виклали свої концепції широкій громадськості й опублікували специфікацію завантажувальної (бутової) вірусної програми. Незважаючи на те, що Черути і Морокути відмовилися від подальших практичних досліджень у цьому напрямку, їх ідеї були підхоплені і широко реалізовані на практиці [2].

Ще одним дослідником у галузі реалізації саморозмножувальних програм у 1984 році став співробітник Лехайского університету Ф. Коен, який провів ряд експериментів на системі VAX 11/750, що працювала під керуванням операційної системи UNIX. Опубліковані ним статті стали посібником для розробки вірусних програм. Вважають, що термін «комп'ютерний вірус» уперше ввів Ф. Коен [2].

Раніше віруси найчастіше програмувалися машинно-орієнтованою мовою Assembler, зараз – мовами вищого рівня, наприклад, С. Завдяки макромовам, таким як VBA, програмування вірусів ще більше спрощується.

Постановка задачі. *Об'єктом* дослідження є методики захисту інформації від комп'ютерних вірусів. Для досягнення *мети* необхідно провести пошук способу уникнення ураженості інформаційних даних вірусами за допомогою розв'язання наступних *завдань*: з'ясування типів можливих вірусів та аналізу можливих шляхів боротьби з ними.

Типи і особливості вірусів та антивірусних прикладних програм

Коло найпоширеніших вірусів окреслюється такими [2; 4]:

W97M/Melissa. Це найвідоміший приклад, оскільки вірус виявився першим, що активно поширюється через Internet.

Explore-Zip (також він Zip-Explorer): набуває поширення через повідомлення електронної пошти. Він поширюється повільніше, ніж Melissa, однак може бути причиною більших ушкоджень, оскільки безповоротно видаляє файли.

W32/Ska-Happy99: Цей вірус відкриває на екрані монітора в Windows-вікні мультиплікаційний фрагмент з надписом "Щасливого Нового 1999 року!" Дія цього вірусу проявляється в імітації зміни тисячоліть з попередженням про так звану помилку Y2K.

W95/CIH: Перший вірус, який уражає BIOS-Setup і тим самим виводить з дії комп'ютер. Крім того, переписується частина жорсткого диску, так що руйнується приблизно один мегабайт інформації, а решта вмісту жорсткого диску стає недоступною. Один різновид вірусу активізується 26 квітня, другий – 26 числа кожного місяця.

W97M/Class: Це спеціально розроблений для MS Word 97 макровірус.

W97M/Ethan: Цей макровірус вишукує і витісняє вірус Class. Правда, після цього комп'ютер все ж залишається зараженим, цього разу вірусом Ethan.

XM/Laroux: Перший і все ще поширений макровірус MS Excel. Цей вірус не має руйнівних функцій.

WM/Concept: Це прародитель усіх макровірусів MS Word. Вперше з'явився влітку 1995 року. На щастя, він не має руйнівних функцій.

Parity Boot: Давно відомий, і подібно Antiexe або Form, доволі невинний Boot-вірус, що видає повідомлення «PARITY CHECK» і зупиняє комп'ютер, у результаті чого користувач може помилково пояснити це несправністю пристроїв ПК.

Stoned. Empire. Monkey: Boot-вірус, що так змінює Master-Boot жорсткого диска, що його можна безперешкодно видалити тільки за допомогою антивірусної програми (але не за допомогою FDISK/MBR), оскільки в іншому випадку виникає загроза втрати даних.

Вважаємо, що одним із ефективних програмних методів захисту є використання антивірусних прикладних програм. До відомих програм, здатних видаляти коди вірусів із програм, належать: Aidstest (Д.М. Лозинський), Doctor (О.О. Чижов), Anti-Kot (О.Г. Котик), Dr.Web (І. Данилов).

Розглянемо найвідоміші та ефективні антивірусні прикладні програми.

Існуюча антивірусна прикладна програма – AVP (Лабораторія Касперського) – забезпечує антивірусний контроль на операційних системах DOS, WINDOWS 95/98/NT/2000, NetWare, Linux, FreeBSD. Також підтримує Microsoft Office 2000, Checkpoint Frewall-1, поштові сервери UNIX-sendmail qmail.

Друга антивірусна прикладна програма – McAfee Active Virus Defense придатна майже для всіх операційних систем та додатків, які використовуються в корпоративних мережах: клієнтські WINDOWS 3.x/95/98/ME/NT, Workstation/ 2000 Professional, OS/2, DOS, Macintosh; серверні ОС WINDOWS NT Server, Windows 2000 Server/ Advanced Server/ Novell Netware, Linux, HP-UX, AIX, SCO, Solaris; додатки Microsoft Office; інтернет-шлюзи MS Proxy Server.

Третя програма, що забезпечує програмний метод захисту – антивірусна прикладна програма Norton AntiVirus (Symantec Corp.). Вона містить набір антивірусних прикладних додатків і придатна для серверів Windows NT та Novell, робочих станцій, комунікаційних пакетів Lotus Notes та MS Exchange, SMTP поштових серверів та брандмауерів. Працює в трьох режимах: автоматичний захист, пошук і вакцинація. Автоматичний захист дає змогу виявити і знищити відомі вірусні програми, забороняє доступ до системи нових вірусних програм, виявляє віруси в архівних файлах (*.ZIP, *.LZH), контролює підозрілі дії, автоматично перевіряє і лікує дискети.

На нашу думку, програмний антивірусний захист є важливою та постійною функцією профілактики комп’ютерної безпеки.

Основним організаційним методом захисту інформації є резервне копіювання найцінніших даних. У разі втрати інформації, коли комп’ютер уражений вірусом, а жодна з відомих йому антивірусних програм не дала позитивного результату, жорсткі диски необхідно переформатувати і підготувати до нової експлуатації. На відформатований диск встановлюють оновлену операційну систему з дистрибутивного компакт-диску, потім під її управлінням встановлюють всі необхідні прикладні додатки, які також беруть з дистрибутивних носіїв. Відновлення комп’ютера завершується відновленням інформації з резервних носіїв. При резервуванні даних потрібно також мати на увазі й те, що слід окремо зберігати всі реєстраційні і парольні дані для доступу до мережевих служб Інтернету. Їх не треба зберігати на комп’ютері. Створюючи план заходів щодо резервного копіювання інформації, необхідно враховувати, що резервні копії повинні зберігатися окремо від комп’ютера. Резервування інформації на іншому жорсткому диску того ж комп’ютера тільки створює ілюзію безпеки. Відносно новим і доволі надійним прийомом зберігання цінних, але неконфіденційних даних є їх зберігання в Web-папках на видалених серверах в Інтернеті. Сервери, що знаходяться в мережі, за допомогою служби WWW, безкоштовно надають віртуальний простір (до декількох Мбайт) для зберігання даних користувача.

Резервні копії конфіденційних даних зберігають на зовнішніх носіях, бажано в окремих приміщеннях. Розробляючи організаційний план резервного копіювання, враховують необхідність створення не менше двох резервних копій, що зберігаються в різних місцях. Між копіями здійснюють ротацію. Наприклад, протягом тижня щодня копіюють дані на носії резервного комплекту А, а через тиждень їх замінюють комплектом Б.

Допоміжними засобами захисту інформації є антивірусні засоби апаратного захисту. Так, наприклад, просте вимкнення перемички на материнській платі не дасть змоги здійснити стирання перепрограмованої мікросхеми ПЗУ (флеш-BIOS), незалежно від того, хто буде намагатися це зробити: комп’ютерний вірус, зловмисник чи непідготовлений користувач.

До основних профілактичних напрямків поширення комп'ютерних вірусів належать такі:

- Проведення регулярних організаційних методів захисту інформації від розповсюдження комп'ютерних вірусів шляхом створення образу жорсткого диска на зовнішніх носіях (наприклад, на гнучких дисках). Цей самий засіб може захистити від втрати даних при апаратних збоях і при випадковому форматуванні жорсткого диска.
- Проведення регулярних програмних методів захисту інформації шляхом встановлення антивірусних програм та сканування цією програмою жорстких дисків у пошуках комп'ютерних вірусів. Сканування зазвичай виконується автоматично при звичайному вімкненні комп'ютера і при розміщенні зовнішнього диска в пристрої для читання. При скануванні потрібно мати на увазі, що антивірусна програма шукає вірус шляхом порівняння коду сканованої програми з кодами відомих їй вірусів, які зберігаються в базі даних. Якщо база даних застаріла, а вірус є новим, скануюча програма його не виявить. Для надійної роботи потрібно регулярно оновлювати антивірусну програму. Бажано оновлювати її один раз на два тижні.
- Контроль за зміною розмірів та інших атрибутів файлів. Комбіновані віруси на етапі розмноження змінюють параметри заражених файлів. Тому контролююча програма може виявити їх діяльність і попередити користувача.
- Контроль за зверненнями до жорсткого диска тієї чи іншої програми. Оскільки найнебезпечніші операції, пов'язані з роботою комп'ютерних вірусів, так чи інакше звернені на модифікацію даних, записаних на жорсткому диску, антивірусні програми можуть контролювати звернення до нього і попереджати користувача про підозрілу активність.

Висновки. На даному етапі дослідження доходимо висновку, що захист інформації від комп'ютерних вірусів передбачає тріадну єдність методів: програмний, апаратний та організаційний. Беручи до уваги невпинне зростання швидкості розповсюдження вірусів, появи їх нових різновидів, активного проникнення у мережу Internet, виникає потреба створення чіткої законодавчої бази кримінального покарання представників ринку вірусного програмного забезпечення, що окреслює перспективу подальшого нашого дослідження.

1. Береза Т.А. Інформаційне суспільство. Шлях України / Т.А. Береза. – 2004. [Електронний ресурс]. Режим доступу: www. isu. org.ua. 2. Касперский Е.В. Компьютерные вирусы MS DOS / Е. Касперский. – М.: Эдаль. – 1992. – 346 с. 3. Калюжний Р.А. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики / Р.А. Калюжний. – К., 2002. – 296с. 4. Козлов Д. Энциклопедия компьютерных вирусов / Д. Козлов. – М.: Салон-Р, 2001. – 461 с. 5. Чукут С., Литвиненко О. Інформаційна політика / С. Чукут, О. Литвиненко. – К.: Вид-во НАДу, 2003. – 100 с.