Таким чином, якщо багатоланкова $R(\Theta)C$ ШПЛ, в якій ввімкнені терморезистори та постійні ємності, використовуються як ПТ, то його чутливість значно збільшується. Якщо в такій лінії замість терморезисторів ввімкнути фоторезистори, то ми будемо мати високочутливий перетворювач світлового потоку [3].

Терморегулятор ПТР-2-03, який використовується в овочесховищах для регулювання температури повітря в приміщенні, спрацьовує при її зміненні на $\pm 1^{o}C$. При зміненні терморезистора в цьому регуляторі чотирьохланковою $R(\Theta)C$ ШПЛ, в якій використовуються терморезистори МЛТ-9 та конденсатори ємністю 0,1 мкФ типу МБМ, його спрацьовування відбувається при зміненні температури повітря в приміщенні на $\pm 0{,}3^{0}C$.

Література:

1. Демидович Б.П., Марон И.А., Шувалова Э.З. Численные методы анализа. – М.:Государственное издательство физико-математической литературы, 1963. – 400с.
2. Виноградова М.Б., Руденко О.В., Сухоруков А.П. Теория волн. – М.: наука, 1979. – 364с.
3. Нікітін Ю.П., Бондарєв В.Т., Шерман М.І. Електронний індикатор напруги та струму. – Техніка АПК, 1995, - №4.- с.21-24.

УДК 681.3

ТЕХНІЧНІ ТА ОРГАНІЗАЦІЙНІ ЗАХОДИ ЗАХИСТУ ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА

С.А.ПОШИВАЙ – ст.викладач
О.М.ПЛЯШКЕВИЧ – пошукувач, Херсонський ДАУ

При використанні комп'ютерної системи користувачі часто не захищають інформацію від несанкціонованого доступу. Ефективні засоби безпеки повинні забезпечувати достатню захищеність і зручність у використанні.

До втрати інформації може привести:

– випадкове знищення даних;

– апаратний збій;

– відмова програмного забезпечення.

Основне розв'язання цієї проблеми – це створення резервних копій. Резервні копії бажано виконувати згідно із заздалегідь розро-

бленим графіком. Доцільно мати головний архів, де зберігається повний обсяг інформації, що використовується, і програмного забезпечення, а також поточні архіви, куди заносяться тільки зміни з моменту створення головного архіву, програмні продукти і файли. поточних архівів може бути декілька, в залежності від періодичності їх оновлення. Зменшити об'єм резервних копій без втрати інформації дозволяють програми пакувальники або архіватори. Використання архіваторів дозволяє зменшити об'єм резервних копій на 10-90%. Найбільш поширені архіватори мають приблизно однакові можливості, серед них ARJ, PKZIP, PAK, PKPAK.

Метою захисту є створення середовища, що дозволяє ускладнити небажаний доступ і використання своїх даних.

До простих методів захисту відноситься використання атрибутів файлів і каталогів – "тільки для читання" або "прихований".

У DOS і WINDOWS існують такі атрібутиви файла:

тільки для читання. Файли з таким атрибутом можна переглядати і копіювати, цей атрибут привласнюють файлам, що не підлягають змінам;

системний. Цей атрибут привласнюється файлам, необхідним для роботи системи, користувачам вони не доступні. При перегляді каталогів, їх імена не можна побачити, вони захищені від стирання;

прихований. Атрибут "прихований" подібний системному тим, що файли приховані від перегляду командою DIR , але вони не захищені від видалення.

архівний. Атрибут "архівний" при зміні файла.

використання атрибутів забезпечує лише деяку міру захисту. Встановити їх можна за допомогою команди ATTRIB.

Один із способів захисту інформації – це використання паролів. призначення пароля – це зробити неможливим вільний доступ до програмних або апаратних засобів. Безпека інформації залежить від складності "злому" або вгадування пароля. Крім паролів, що використовуються для звернення до місцевої мережі, internet, користувач може використати включаючі паролі – паролі для завантаження комп'ютера, спеціальні захисні програми, що блокують доступ до даних, і захищені паролем архівні файли.

Поповнюючи своє програмне забезпечення , користувач повинен захистити його від вірусів. Віруси викликають зміни програмних і системних файлів, файлів початкового завантаження. Їх класифікують по типу поведінки:

– вірус, що вражає завантажувальний сектор диска;

– вірус, що інфікує файли;

– багатофункціональні віруси;

– системні віруси.

Найкращий засіб захисту від вірусів – регулярне використання антивірусних програм. Вони призначені для перевірки пам'яті і файлів комп'ютерної системи і виявлення вірусів. Антивірусне програмне забезпечення можна використати декількома способами.

У першому випадку пошук вірусу виконується при початковому завантаженні, для цього команду запуску програми, що активується записують в файл AUTOEXEC. BAT. Це дещо збільшує час початкового завантаження комп'ютера, але зате пошук вірусу виконується автоматично.

Другий спосіб полягає в ручному прочитанні системи за допопмогою антивірусної програми. Наступний спосіб пошуку вірусу полягає в перегляді кожного файла, що завантажується. Для виявлення вірусу на "вінчестері" треба використати антивірусну програму, більш пізнього терміну випуску. Якщо користувач виявив зміну розмірів файлів, особливо COM або EXE:

– зміни в обробці переривання;

– зміни об'єму оперативної пам'яті;

– незвичайна поведінка під час завантаження, а антивірусна програма не може виявити вірус, можливо, ця програма також заражена.

Проблему захисту від вірусів доцільно розглядати, пов'язуючи з питаннями захисту інформації від несанкціонованого доступу. Обов'язково повинно бути декілька рівнів захисту є вхідний контроль придбаних програм і дискет, в тому числі і дистрибутивні дискети.

Велику частину відомих вірусів можна виявити вже на етапі вхідного контролю. Антивірусні програми, що рекомендуються: AIDSTEST, Dr. Web, AVP. Запуск здійснюється за допомогою звичайного bat-файла.

Якщо програмне забезпечення отримане із сумнівного джерела, то корисно перші декілька днів експлуатацію програмного забезпечення виконувати в штучно прискореному комп'ютерному режимі, тобто задавати при кожній новій експлуатації новий місяць і день тижня. Це дає можливість виявити троянський компонент, що спрацьовує в певний місяць або після закінчення певного календарного відрізка часу. Якщо немає можливості для цієї мети виділити окремий комп'ютер, то можна реалізувати цей режим на комп'ютері, що не містить особливо цінних файлів. При роботі у цьому режимі вхід в систему повинен виконуватися за допомогою спеціального імені, якому для запису доступний лише електронний диск і спеціальний розділ "вінчестера". (Операції, що виконуються програмою корисно контролювати резидентними фільтрами, а також заздале-

гідь скопіювати на електронний диск, часто використовувані утиліти (NORTON COMMANDER, DISKCOPY, XCOPY, редактор текстів), і подивитися чи будуть вони змінюватися при запуску). Перевага використання експлуатаційного диска полягає в тому, що його зміст автоматично знищується, що не залишиться на зиску і не розповсюдиться далі.

Нарівні з програмами, зараженими вірусами, визначеними небезпеку представляють програми зі "зламаним" захистом, які ведуть до активації троянського компонента, закладеного в програмі.

Після придбання комп'ютера перевірити зміст жорсткого диска.

"Вінчестер" і всі отримані дискети треба протестувати на наявність вірусу, програмами детекторами, тобто програмами для виявлення і видалення вірусів в файлах і пам'яті комп'ютера, наприклад AIDSTEST, Dr. Web, ADint.

Для перевірки "вінчестера", завантаження необхідно виконати з явно чистої, захищеної від запису, системної дискети.

Наступний рівень захисту пропонує сегментацію "вінчестера" за допомогою драйвера, який привласнює логічним дискетам атрибут READ ONLY, а також найпростішу систему парольного доступу.

Число логічних дисків і їх вміст залежить від вигляду задач, що вирішуються, і об'єму "вінчестера". Хорошим доповненням до програм AIDSTEST, Dr. Web, ADint є використання програми-сторожа (фільтра), яка перевіряла б дискети, вставлені в комп'ютер і файли, що запускаються на наявність в них вірусів, наприклад, програма NAVTSR. EXE.

Для запуску цієї програми треба вставити в файл AUTOEXEC. BAT команду виклику NAVTSR. EXE.

Одним з важливих засобів захисту від вірусів є система перевірки ідентичності програми дистрибутивної копії. Для реалізації цього методу використовуються спеціальні програми ревізори. Перевірка суцільності файлів за допомогою ревізора повинна проводитися не менш, як один раз на день, наприклад, при вмиканні комп'ютера.

Коли проводиться щоденна перевірка дисків спочатку виконується програма-ревізор ADinf, яка аналізує зміни на дисках, при цьому виводиться даіграма, яка повідомляє про хід перевірки. Якщо на дисках не виявлено ніяких змін у програмних файлах та системних областях, то програма автоматично завершує свою роботу.

При виявленні підозрілих змін програма виводить повідомлення і список цих змін.

Ревізори є єдиним засобом, які дозволяють стежити за цілісністю системних файлів та змінами у каталогах. Це особливо важли-

во при роботі на комп'ютерах колективного користування. Одним із специфічних прикладів захисту є використання дискет захищених від запису. Захист повинен зніматися тільки під час запису інформації. Необхідно використовувати тільки захищену від запису дискету для зберігання копії операційної системи та антивірусних програм, що використовуються, щоб бути впевненим в їх цілісності.

Оскільки командний процесор найчастіше вражається файловими вірусами, необхідно приділяти більше уваги його цілісності. Використовуючи команду SHELL у файлі CONFIG.SYS, доцільно розмістити командний процесор у захищеному від запису розділі "вінчестера". Бажано періодично контролювати розміри командного процесора та програм, які визиваються, за допомогою AUTOEXEC. BAT, оскільки вони заражуються, як правило, першими.

Це можливо зробити за допомогою програми-ревізора або звичайної програми порівняння файлів, яка входить до MS-DOS. Оригінал повинен зберігатися на захищеній від запису дискеті.

Незалежно від того, наскільки добре розроблені програмні засоби захисту, їх ефективність в багатьох випадках залежить від правильності дій тих, хто ці програми використовує, дій в яких можливі помилки та злі наміри.

У зв'язку з цим, доцільно було б прийняти організаційні заходи. Забезпечити захист комп'ютера з цінними даними від використання випадковими людьми. Окрім небезпеки зараження вірусами, незаконне копіювання або зміни конфіденційної інформації може принести велику шкоду.

Головною вимогою запобігання зараження комп'ютера вірусами – це певний рівень освіти співробітників.

Чим менше обізнаний той чи інший співробітник з комп'ютерами тим більшу загрозу він становить з точки зору можливості зараження вірусами.

Забезпечити фізичну безпеку комп'ютера і магнітних носіїв, розробити правила архівації, зберігати окремі файли у шифрованому вигляді, скласти та відпрацювати план встановлення "вінчестера".

Операційна система MS-DOS і WINDOWS облишені засобів захисту від несанкціонованого доступу. Це дозволяє складати програми, які працюють під керівництвом системи і в той же час мають доступ до всіх ресурсів комп'ютера. Для нормального функціонування вірусу достатньо мати доступ лише до деяких засобів файлової системи, які використовуються звичайними програмами.

Тому створення універсального засобу боротьби з вірусами не можливо. В той же час багато вірусних програм дуже чутливі до

будь-яких змін операційної системи. Це можливо використати для того щоб зробити систему нечутливою до вірусів.

Література:

1. Эд Тайли. Безопасность компьютера. – пер. с англ. Попурри, Минск, 1997.
2. Фигурнов В.Э. IBM PC для пользователя. Краткий курс – инфра, Москва, 1998
3. Миклев А. Настольная книга пользователя. – 2-е изд. , Солон, Москва, 1997.