УДК 372.862: 004.492

НАВЧАЛЬНО-МЕТОДИЧНЕ ДОПОВНЕНЯ ЩОДО ВИВЧЕННЯ ТЕМИ «КОМП'ЮТЕРНІ ВІРУСИ ТА БОРОТЬБА З НИМИ»

Пономаренко Олена

Науковий керівник:кандидат технічних наук, доцент, Царенко М.О.

Південноукраїнський національний педагогічний університет імені К. Д. Ушинського

На сьогодні масове застосування персональних комп'ютерів, на жаль, пов'язане з появою самовідтворювальних програм-вірусів, які унеможливлюють їхню нормальну роботу, руйнують файлову структуру дисків, завдають шкоду персональній базі даних користувача. Метою дослідження є впровадження у навчальний процес структурованої інформації, яка дозволяє виокремити особливості підходів, орієнтованих на ефективну боротьбу з комп'ютерними вірусами. Для досягнення цієї мети використано дослідницький метод, що дозволив визначити саме ту групу комп'ютерних вірусів, з якими, на сьогодні, можливо боротися та мінімізувати негативні наслідки від них. Відзначено, що незважаючи на прийняті в багатьох країнах заходи боротьби з комп'ютерними вірусами і розробкою спеціальних програмних засобів захисту від них, кількість нових вірусів постійно зростає. Цей факт свідчить про необхідність розширення означеної в роботі проблематики дослідження.

Ключові слова: *віруси, антивірусна програма, файли, програми-детектори, програми-ревізори, програми-фільтри.*

Educational and methodical addition for studying of the subject "Computer viruses and fight against them"

Olena Ponomarenko

Scientific supervisor: PhD in Technical Sciences, associate professor, **Tsarenko M.O.**

Southern Ukrainian National Pedagogical University named after K. D. Ushinsky

For today, the mass use of personal computers, unfortunately, connected with emergence of programs viruses which make impossible their normal work destroy file structure of disks, do harm to personal base bathing the user. The purpose of the methodical research is implementation in educational process of the structured information which allows to select features of approaches which are oriented to effective fight against computer viruses. For achievement of this purpose the research method which allowed to define that group of computer viruses with which, for today, it is possible to

fight and minimize negative effects from them is used. It is noted that despite of the fight actions for computer viruses and development of special software of protection against them hosted in many countries, the quantity of new viruses constantly grows. This fact testifies to need of expansion of the research perspective noted in work.

Keywords: *viruses, anti-virus program, files, programs detectors, programs auditors, programs filters.*

Очевидно, що комп’ютери стали справжніми помічниками людини і без них вже не може обійтися ані комерційна фірма, ані державна організація [1]. З іншого боку, загострилася проблема захисту інформації [2]. Віруси, що сьогодні широко поширюються в комп'ютерній мережі, розбурхали весь світ [3-7]. Користувачі стурбовані тим, що зловмисники здатні дістатися до конференційної приватної, фінансової, технічної та іншої важливої інформації. Отже, масове застосування персональних комп’ютерів, гаджетів має інший, небажаний бік. Поява нових і нових програм-вірусів перешкоджає нормальному функціонуванню всесвітньої павутини, руйнує не лише файлову структуру дисків, але і створює відповідну психологічну недовіру до виробників, як комп’ютерної техніки так і програмного забезпечення щодо збереження важливої інформації [8]. Зовсім недавно зараження вірусом текстових файлів вважалося абсурдом, а зараз – цим вже нікого не здивуєш. Досить згадати появу «першої ластівки», яка наробила багато шуму – вірусу Win Word Concept, що вражає документи у форматі текстового процесора Microsoft Word for Windows [1]. Незважаючи на прийняті в багатьох країнах закони про боротьбу з комп’ютерними злочинами і розробку спеціальних програмних засобів захисту, кількість нових програмних вірусів теж зростає у геометричній прогресії. Саме така напружена ситуація у світі гаджетів і комп’ютерів визначила напрямок чинного методичного дослідження: систематизація знань користувачів про природу вірусів, способи зараження ними та захисту [5-7].

Мета статті полягає у систематизації відомих методів боротьби з вірусами. Підготовлений матеріал є додатковою інформацією, який може бути

використаний у форматі лабораторної роботи щодо вивчення та аналізу основних вірусів, які можуть вплинути на роботу програмного забезпечення.

Згідно до мети визначені *задачі* роботи*:* вивчити, дослідити та проаналізувати факти існування деяких груп вірусів, можливостей боротьби з ними з метою мінімізації впливу негативних наслідків на роботу систем персонального комп'ютера.

*Методи дослідження***.** Для досягнення поставленої мети та вирішення завдань дослідження використано сукупність взаємопов'язаних методів: *загальнонаукових***:** аналіз, синтез, абстрагування, *порівняння та узагальнення* – для з'ясування особливостей концептуальних підходів покладених в основу боротьби з вірусами; *конкретно наукових* метод термінологічного аналізу, застосування якого дозволило уточнити основоположні поняття дослідження; хронологічний, на основі якого було визначено основні етапи створення вірусів.

Виклад основного матеріалу. У літературі досить наполегливо пропагується, що позбутися вірусів можна лише за допомогою складних і дорогих антивірусних програм, і нібито тільки під їхнім захистом ви можете відчувати себе в цілковитій безпеці. Це не зовсім так – знайомство з особливостями будови і способами впровадження комп'ютерних вірусів допоможе вчасно їх виявити і локалізувати, навіть якщо під рукою не виявиться підходящої антивірусної програми. Зараз застосовуються персональні комп'ютери, в яких користувач має вільний доступ до всіх ресурсів ПК. Саме це відкрило можливість для небезпеки, яка отримала назву комп'ютерного вірусу. Вірус – це програма яка здатна до самовідтворення. Така здатність є єдиним засобом, властивим всім типам вірусів. Але не тільки віруси здатні до самовідтворення. Будь-яка операційна система і ще безліч програм здатні створювати власні копії. Копії ж вірусу можуть взагалі не збігатися з оригіналом! Вірус не може існувати в «повній ізоляції»: сьогодні не можна уявити собі вірус, який не використовує код інших програм, інформацію про файлову структуру або навіть просто імена інших програм. Причина

зрозуміла: вірус повинен якимось способом забезпечити передачу собі управління [1]. Залежно від середовища перебування віруси можна розділити на мережеві, файлові, завантажувальні і файлово-завантажувальні. Мережні віруси поширюються по різним комп'ютерним мережам. Файлові віруси впроваджуються, головним чином, у модулі які виконуються, тобто у файли, які мають розширення COM або EXE. Завантажувальні віруси впроваджуються в завантажувальний сектор диска (Boot-сектор) або в сектор, що містить програму завантаження системного диска (Master Boot Record). Файлово-завантажувальні віруси вражають як файли, так і завантажувальні сектори дисків.

За ступенем впливу віруси можна розділити на наступні види:

• Безпечні, не заважають роботі комп'ютера, але зменшують обсяг вільної оперативної пам'яті і пам'яті на дисках, дії таких вірусів проявляються в будь-яких графічних або звукових ефектах.

• Небезпечні віруси, які можуть привести до різних порушень в роботі комп'ютера.

• Дуже небезпечні, вплив яких може призвести до втрати програм, знищення даних, стирання інформації в системних областях диска.

За особливостями алгоритму віруси важко класифікувати через великі розмаїття. Найпростіші віруси – паразитичні, вони змінюють вміст файлів і секторів диска і можуть бути досить легко виявлені і знищені. Можна відзначити віруси – реплікатори, звані хробаками, які поширюються по комп'ютерних мережах, обчислюють адреси мережних комп'ютерів і записують за цими адресами свої копії [1].

Відомі віруси-невидимки, так звані стелс-віруси, які дуже важко знайти й знешкодити, оскільки вони перехоплюють звертання операційної системи до вражених файлів і секторів дисків і підставляють замість свого тіла незаражені ділянки диска. Найбільш важко виявити віруси-мутанти, що містять алгоритми шифрування-розшифровки, завдяки яким копії одного і того ж вірусу не мають ні

одного повторювального ланцюжка байтів. Є й звані квазівірусні або «троянські» програми, які хоч і не здатні до самопоширення, але дуже небезпечні, оскільки, маскуючись під корисну програму, руйнують завантажувальний сектор і файлову систему дисків.

Троянські коні, програмні закладки та мережеві «черв'яки». Троянський кінь – це програма, що містить у собі деяку руйнуючу функцію, яка активізується при настанні деякої умови спрацьовування. Зазвичай такі програми маскуються під які-небудь корисні утиліти. Віруси можуть нести в собі троянських коней чи "троянізовувати" інші програми – вносити в них руйнівні функції [2]. Зазвичай вони маскуються під ігрові або розважальні програми та завдають шкоди під красиві картинки або музику. Якщо віруси і «троянські коні» завдають шкоди за допомогою лавиноподібного саморозмноження або явного руйнування, то основна функція вірусів типу «хробак», діючих в комп'ютерних мережах, це злом, атакується система, тобто подолання захисту з метою порушення безпеки і цілісності.

У понад 80% комп'ютерних злочинів, розслідуваних ФБР, "зломщики" проникають в атаковану систему через глобальну мережу Internet. Коли така спроба вдається, майбутнє компанії, на створення якої пішли роки, може бути поставлено під загрозу за якісь секунди [3]. Цей процес може бути автоматизований за допомогою вірусу, званого мережевим хробаком.

Хробаками називають віруси, які поширюються по глобальним мережам, вражаючи цілі системи, а не окремі програми. Це найнебезпечніший вид вірусів, так як об'єктами нападу в цьому випадку стають інформаційні системи державного масштабу. З появою глобальної мережі Internet цей вид порушення безпеки представляє найбільшу загрозу, оскільки його в будь-який момент може зазнати будь-який з 40 мільйонів комп'ютерів підключених до цієї мережі.

Шляхи проникнення вірусів у комп'ютер і механізм розподілу вірусних програм. Основними шляхами проникнення вірусів у комп'ютер є змінні диски, а

також комп'ютерні мережі. Враження жорсткого диска вірусами може відбутися при завантаженні програми з диску, що містить вірус. Таке враження може бути і випадковим, наприклад, якщо диск не вийняли з дисководу і перезавантажили комп'ютер, при цьому диск може бути і не системним [3]. Вразити диск набагато простіше. На нього вірус може потрапити, навіть якщо диск просто вставили в дисковод враженого комп'ютера і, наприклад, прочитали його зміст.

Вірус, як правило, впроваджується в робочу програму таким чином, щоб при її запуску управління спочатку передалося йому і тільки після виконання всіх його команд знову повернулося до робочої програми. Отримавши доступ до управління, вірус, перш за все, переписує сам себе в іншу робочу програму і вражає її [4]. Після запуску програми, що містить вірус, стає можливим враження інших файлів.

Найчастіше вірусом вражаються завантажувальний сектор диска і виконувані файли, що мають розширення EXE, COM, SYS, BAT. Вкрай рідко вражаються текстові файли.

Після враження програми вірус може виконати диверсію, не дуже серйозну, щоб не привернути уваги. І, нарешті, не забуває повернути управління тій програмі, з якої був запущений. Кожне виконання враженої програми переносить вірус у наступну. Таким чином, з часом буде вражене все програмне забезпечення.

Ознаки появи вірусів. При враженні комп'ютера вірусом важливо його виявити. Для цього слід знати про основні ознаки прояву вірусів. До них можна віднести наступні:

• Припинення роботи або неправильна робота раніше успішно функціонуючих програм;

• Повільна робота комп'ютера;

• Неможливість завантаження операційної системи;

• Зникнення файлів і каталогів чи спотворення їх вмісту;

• Зміна дати і часу модифікації файлів;

• Зміна розмірів файлів;

• Несподіване значне збільшення кількості файлів на диску;

• Істотне зменшення розміру вільної оперативної пам'яті;

• Виведення на екран непередбачених повідомлень або зображень;

• Подача непередбачених звукових сигналів;

• Часті зависання і збої в роботі комп'ютера;

Незважаючи на те, що загальні засоби захисту інформації дуже важливі для захисту від вірусів, все ж їх недостатньо. Необхідно застосовувати спеціалізовані програми для захисту від вірусів [5]. Ці програми можна розділити на кілька видів: детектори, лікарі (фаги), ревізори, лікарі-ревізори, фільтри та вакцини (іммунізатори).

Програми-детектори дозволяють виявляти файли, вражені одним з декількох відомих вірусів. Ці програми перевіряють, чи є у файлах на зазначеному користувачем диску специфічна для даного вірусу комбінація байтів. При її виявленні в якомусь файлі на екран виводиться відповідне повідомлення. Багато детекторів мають режими лікування або знищення вражених файлів. Слід підкреслити, що програми-детектори можуть виявляти тільки ті віруси, які їй "відомі". Програма Scan фірми Mc Afee Associates і Aidstest Д. Н. Лозинського дозволяє виявляти близько 9000 вірусів, але всього їх більше двадцяти тисяч! Деякі програми-детектори, наприклад Norton Anti Virus або AVSP фірми "Діалог", можуть налаштовуватись на нові типи вірусів, їм необхідно лише вказати комбінації байтів, властивих цим вірусам.

Багато програм-детекторів (у тому числі і Aidstest) не вміють виявляти враження "невидимими" вірусами, якщо такий вірус активний в пам'яті комп'ютера. Справа в тому, що для читання диска вони використовують функції DOS, що перехоплюються вірусом, який говорить, що все добре. Правда, Aidstest та інші детектори намагаються виявити вірус шляхом перегляду оперативної пам'яті, але проти деяких "хитрих" вірусів це не допомагає. Так що надійний

діагноз програми-детектори дають тільки при завантаженні DOS з "чистою", захищеного від запису диску, при цьому копія програми-детектора також повинна бути запущена з цього диску. Деякі детектори (скажімо ADinf фірми "Діалог-Наука") вміють ловити "невидимі" віруси, навіть коли вони активні. Для цього вони читають диск, не використовуючи виклики DOS.

Щоправда, цей метод працює не на всіх дисководах. Більшість програм-детекторів мають функцію "лікаря", тобто вони намагаються повернути вражені файли або області диска в їх початковий стан [6]. Ті файли, які не вдалося відновити, як правило, робляться непрацездатними або видаляються. Більшість програм-лікарів вміють "лікувати" тільки від деякого фіксованого набору вірусів, тому вони швидко застарівають. Але деякі програми можуть навчатися не тільки способам виявлення, а й способам лікування нових вірусів. До таких програм відноситься AVSP фірми "Диалог".

Програми-ревізори мають дві стадії роботи. Спочатку вони запам'ятовують відомості про стан програм і системних областей дисків (завантажувального сектора і сектора з таблицею розбиття жорсткого диска). Передбачається, що в цей момент програми та системні області дисків не вражені. Після цього за допомогою програми-ревізора можна в будь-який момент порівняти стан програм і системних областей дисків з вихідним. Про виявлені невідповідності повідомляється користувачеві. Щоб перевірка стану програм і дисків проходила при кожному завантаженні операційної системи, необхідно включити команду запуску програми-ревізора в командний файл AUTOEXEC BAT. Це дозволяє виявити враження комп'ютерним вірусом, коли він ще не встиг завдати великої шкоди. Більше того, та ж програма-ревізор зможе знайти ушкоджені вірусом файли. Останнім часом з'явилися дуже корисні гібриди ревізорів і лікарів, тобто ЛІКАРІ-ревізора – програми, які не тільки виявляють зміни у файлах і системних областях дисків, а й можуть у разі змін автоматично повернути їх в початковий стан [7]. Такі програми можуть бути набагато більш універсальними, ніж програми-лікарі,

оскільки при лікуванні вони використовують заздалегідь збережену інформацію про стан файлів і областей дисків. Це дозволяє їй вилікувати файли навіть від тих вірусів, які не були створені на момент написання програми. Але вони можуть лікувати не від усіх вірусів, а тільки від тих, які використовують "стандартні", відомі на момент написання програми, механізми враження файлів.

Програми-фільтри – розташовуються резидентно в оперативній пам'яті комп'ютера і перехоплюють ті звернення до операційної системи, які використовуються вірусами для розмноження і нанесення шкоди, і повідомляють про них користувача. Користувач може дозволити або заборонити виконання відповідної операції. Однак переваги використання програм-фільтрів дуже значні – вони дозволяють виявити багато вірусів на самій ранній стадії, коли вірус ще не встиг розмножитися і щось зіпсувати. Тим самим можна звести збитки від вірусу до мінімуму.

Програми-вакцини, або іммунізатори, модифікують програми і диски таким чином, що це не відбивається на роботі програм, але той вірус, від якого виробляється вакцинація, вважає ці програми або диски вже враженими. Ці програми є вкрай неефективними.

Антивірусні програми. Отже, що ж таке антивірус? Відразу ж розвіємо одну часто виникаючу ілюзію. Чомусь багато хто вважає, що антивірус може виявити будь-який вірус, тобто, запустивши антивірусну програму або монітор, можна бути абсолютно впевненим у їх надійності. Така точка зору не зовсім правильна. Справа в тому, що антивірус – це теж програма, написана професіоналом. Але ці програми здатні розпізнавати і знищувати лише відомі віруси. Тобто антивірус проти конкретного вірусу може бути написаний лише в тому випадку, коли у програміста є у наявності хоча б один екземпляр цього вірусу. От і триває нескінченна війна між авторами вірусів і антивірусів, щоправда, перших чомусь завжди більше, ніж других. Але і у творців антивірусів є перевага! Справа в тому, що існує велика кількість вірусів, алгоритм яких практично скопійований з

алгоритмів інших вірусів. Як правило, такі варіації створюють непрофесійні програмісти. Для боротьби з такими "копіями" придумано нову зброю – евристичні аналізатори. З їхньої допомоги антивірус здатний знаходити подібні аналоги відомих вірусів, повідомляючи користувачеві, що у нього, схоже, завівся вірус. Природно, надійність евристичного аналізатора не 100%, але все ж його коефіцієнт корисної дії більший 50%. Таким чином, в цій інформаційній війні, як, втім, і в будь-який іншій, перемагають найсильніші. Віруси, які не розпізнаються антивірусними детекторами, здатні написати тільки найбільш досвідчені й кваліфіковані програмісти. При запуску Aidstest перевіряє себе, оперативну пам'ять на наявність відомих йому вірусів і знешкоджує їх. При цьому паралізувано буде тільки функції вірусу, пов'язані з розмноженням, а інші побічні ефекти можуть залишатися. Тому програма після закінчення знешкодження вірусу в пам'яті видає запит про перезавантаження. Слід обов'язково робити це, якщо оператор ПК не є системним програмістом, який звивчає властивості вірусів. Причому слід перезавантажитися кнопкою RESET, тому що при "теплому перезавантаженні" деякі віруси можуть зберігатися. Краще запустити ПК і Aidstest із захищеного від запису диску, оскільки при запуску із враженого диску вірус може записатися на згадку резидентом і перешкоджати лікуванню. Як показала практика, найоптимальніший режим для щоденної роботи задається ключами: /g (перевірка всіх файлів, а не тільки з розширенням EXE, COM, SYS) та /s (повільна перевірка). Збільшення часу при таких опціях практично не відчутна, зате вірогідність виявлення на порядок вища. При звичайному тестуванні не слід ставити ключ /f (виправлення заражених програм і стирання не підлягають відновленню), навіть з ключем /q (видавати запит про видалення файлу), оскільки будь-яка програма, в тому числі і антивірусна, не застрахована від помилок. Ключ /f слід використовувати тоді, коли Aidstest, а також інші антивіруси вказують на наявність вірусу у файлі [7, 8]. При цьому слід перезапустити комп'ютер із захищеного від запису диску, так як система може бути заражена резидентним

вірусом, і тоді лікування буде неефективним, а то й просто небезпечним. При виявленні вірусу в коштовному файлі слід переписати його на електронний диск і там спробувати вилікувати за допомогою вказівки Aidstest – в опції /f. Якщо спроба не увінчається успіхом, то треба видалити всі заражені копії файла і перевірити диск знову. Якщо у файлі міститься важлива інформація, яку слід зберегти, то необхідно провести архівацію файлу до виходу нової версії Aidstest, або іншої антивірусної програми, здатної лікувати цей тип вірусу. Для прискорення процесу можна направити заражений файл, як зразок Лозинському. Для створення у файлі протоколу роботи програми Aidstest служить ключ /p. Протокол потрібен, коли користувач не встигає переглянути імена вражених файлів. Для підтримки антивірусного програмно-апаратного комплексу Sheriff служить ключ /z.

Doctor Web. Останнім часом стрімко зростає популярність іншої антивірусної програми – Doctor Web (Dr.Web). Ця програма разом з Aidstest належить до класу детекторів-лікарів, але на відміну від останнього, він має так званий "евристичний аналізатор" – алгоритм, що дозволяє виявляти невідомі віруси. "Лікувальна павутина", як перекладається з англійської назва програми, стала відповіддю програмістів на навалу самомоіндифікуючих вірусів-мутантів. Останні при розмноженні модифікують своє тіло так, що не залишається жодного характерного ланцюжка байтів, присутніх у вихідній версії вірусу. Dr.Web можна назвати антивірусом нового покоління в порівнянні з Aidstest та його аналогами.

Управління режимами як і в Aidstest здійснюється за допомогою ключів. Користувач може вказати програмі, тестувати весь диск, або окремі підкаталоги чи групи файлів, або ж відмовитися від перевірки дисків і тестувати тільки оперативну пам'ять. У свою чергу можна тестувати або тільки базову пам'ять, або, ще і розширену (вказується з допомогою ключа /H). Як і Aidstest Doctor Web може створювати звіт про роботу (ключ /P), завантажувати знакогенератор Кирилиці (ключ /R), підтримує роботу з програмно-апаратним комплексом Sheriff (ключ /

Z) [3]. Але, звичайно, головною особливістю "Лікувальної павутини" служить наявність евристичного аналізатора, який підключається ключем /S. Балансу між швидкістю і якістю можна домогтися, вказавши ключу рівень евристичного аналізу: 0 - мінімальний, 1 - оптимальний, 2 - максимальний; при цьому, природно, швидкість зменшується пропорційно збільшенню якості. До того ж Dr.Web дозволяє тестувати файли, вакциновані CPAV, а також упаковані LZEXE, PKLITE, DIET. Для цього слід вказати ключ / U (при цьому розпакування файлів проведуть на поточному пристрої) чи / U диск: (де диск: це пристрій , на якому буде здійснюватися розпакування), якщо диск, з якого запущений Doctor Web захищений від запису. Багато програм упаковані таким способом, хоча користувач може і не підозрювати про це. Якщо ключ / U не встановлено, то Doctor Web може пропустити вірус,який заліз в запаковану програму. Важливою функцією є контроль враження тестованих файлів резидентним вірусом (ключ / V). При скануванні пам'яті не має стовідсоткової гарантії, що "Лікувальна павутина" знайде всі віруси, які перебувають там. Так от, при завданні функції / V Dr.Web намагається перешкодити тим, які залишилися резидентним вірусам, вразити тестовані файли. Тестування вінчестера Dr.Web-ом займає на багато більше часу, ніж Aidstest-ом, тому кожен користувач не може собі дозволити витрачати стільки часу на щоденну перевірку всього жорсткого диску. Таким користувачам можна порадити ретельніше (з опцією / S2) перевіряти внесені ззовні диски. Якщо інформація на диску знаходиться в архіві (а останнім часом програми і дані переносяться з машини на машину тільки в такому вигляді; навіть фірми-виробники програмного забезпечення, наприклад Borland, купують свою продукцію), слід розпакувати його в окремий каталог на жорсткому диску і відразу ж, не відкладаючи, запустити Dr.Web, поставивши йому як параметр замість імені диска повний шлях до цього підкаталогу. І все ж потрібно хоча б раз на два тижні робити повну перевірку "вінчестера" на віруси із завданням максимального рівня евристичного аналізу.

Microsoft Antivirus. До складу сучасних версій MS-DOS входить антивірусна програма Microsoft Antivirus (MSAV). Цей антивірус може працювати в режимах детектора-лікаря і ревізора. MSAV має дружній інтерфейс в стилі MS-Windows, природно, підтримується миша [2]. Добре реалізована контекстна допомога: підказка є практично до кожного пункту меню, до будь-якої ситуації. Універсально реалізований доступ до пунктів меню: для цього можна використовувати клавіші управління курсором, ключові клавіші (F1-F9), клавіші, відповідні одній з літер назви пункту, а також миша. Прапорці установок у пункті меню Options можна встановлювати як клавішею ПРОБІЛ, так і клавішею ENTER. Серйозною незручністю при використанні програми є те, що вона зберігає таблиці з даними про файли не в одному файлі, а розкидає їх по всіх директоріях.

Слід ще раз зазначити, що комп'ютерний вірус – це спеціально написана програма, яка здатна мимовільно приєднуватися до інших програм, створювати свої копії і упроваджувати їх у файли, системні області комп'ютера і в обчислювальні мережі з метою порушення роботи програм, псування файлів і каталогів, створення всіляких перешкод в роботі комп'ютера.

Підводячи підсумок, зазначимо, що, на сьогодні, існує майже п'ять тисяч вірусів і їх кількість безперервно збільшується. Відомі випадки, коли створювалися навчальні посібники, які допомагають у написанні вірусів. Основні види вірусів: завантажувальні, файлові, файлово-завантажувальні. Самий небезпечний вид вірусів – поліморфний. Причини появи і розповсюдження вірусів приховані з одного боку в психології людини, з другого боку – з відсутністю засобів захисту у операційної системи. Навіть, якщо загрози вірусів начебто немає, необхідно заздалегідь провести заходи антивірусного захисту, в тому числі організаційного характеру.

Висновки

Таким чином, в роботі систематизовані та проаналізовані основні програми-віруси, які можуть вплинути на роботу програмного забезпечення гаджетів та

персональних комп’ютерів. Наведені сучасні методи і прийоми боротьби з вірусами.

Вирішені наступні *задачі:* вивчені, досліджені та проаналізовані факти існування деяких груп вірусів, можливості боротьби з ними з метою мінімізації впливу негативних наслідків на роботу систем персонального комп’ютера. Показано, що першим, хто захищає персональний комп’ютер є програми-фільтри. Другу групу складають програми-ревізори, програми-лікарі та лікарі-ревізори. Надана в статті інформація може бути використана під час виконання лабораторної роботи за відповідною темою.

Список використаної літератури

1. Норок А.П. Сучасні технології боротьби з вірусами / А.П. Норок // – № 8. – 2011.
2. Использование криптографии – Энциклопедия безопасности – [Цит. 2011 26 листопада] – Доступний з:http//www.opasno.net/st.832html.
3. Фейнштайн К. Защита ПК от спама, вирусов, всплывающих окон и шпионских программ / К Фейнштайн; Пер с англ. О.Б.Вереиной // М.:НТ Пресса, 2015. – 240с.:ил.- (Самоучитель).
4. Чігірьов С.П. Методи автентифікації даних. Електронний цифровий підпис / С.П. Чігірьов, С.І. Ганжела // Збірник тез доповідей Всеукраїнського студентського науково-практичного семінару "Сучасні інформаційні технології та програмне забезпечення комп’ютерних систем" – Кіровоград: Вид-во "КОД" 2012. – С. 45-47.
5. Лутченко О.В. Цифровий підпис із застосуванням кода автентифікації повідомлення / О.В. Лутченко, С.І. Ганжела // Студентські наукові записки (Збірник наукових статей студентів фізико-математичного факультету). – Кіровоград: РВВ КДПУ ім. В.Винниченка, 2012. – Випуск 5. – С. 21–23.
6. Компьютерный вирус. - Лаборатории Касперского – [Цит. 2011 29 листопада]. – Доступний з: http://ru. kaspersky org./faq/Компьютерний вирус.
7. Троянские програмы – AnVir – [Цит. 2011 14 грудня] – Доступний з: http//www.anvir.net/trojanskie-programmyi.html.
8. Способы борьбы с програмами-вымогателями класса Trojan-Ransom - Служба технической поддержки Лаборатории Касперского – [Цит. 2011 25 грудня]. - Доступний з: http://support.kaspersky.ru/faq/?qid=208637133.