МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

МЕТОДИЧНІ МАТЕРІАЛИ ЩОДО ЗАБЕЗПЕЧЕННЯ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

з дисципліни

“КОМП’ЮТЕРНА ВІРУСОЛОГІЯ”

(для бакалаврів)

Київ
ДП «Видавничий дім «Персонал»
2011

Підготовлено кандидатом технічних наук, доцентом кафедри інформатики та інформаційних технологій *В. М. Ахрамовичем*

Затверджено на засіданні кафедри інформатики та інформаційних технологій (протокол № 3 від 30.10.08)

Схвалено Вченою радою Міжрегіональної Академії управління персоналом

Ахрамович В. М. Методичні матеріали щодо забезпечення самостійної роботи студентів з дисциплін "Комп'ютерна вірусологія" (для бакалаврів). — К.: ДП «Вид. дім «Персонал», 2011. — 39 с.

Методична розробка містить пояснювальну записку, тематичний план дисциплін "Комп'ютерна вірусологія", питання для самостійного вивчення та самоконтролю, теми рефератів, тестові завдання, глосарій, список літератури.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Історично виникнення вірусів пов'язане з ідеєю створення програм, що самовідтворюються, і припадає на п'ятдесяті роки. Ідея механізмів, що самовідтворюються, досліджувалася ще Джоном фон Нейманом, який у 1951 р. запропонував метод їх створення. Таким чином, попередниками вірусів були різного роду програми (деякі з них у вигляді ігор), принцип роботи яких полягав у здатності самовідтворюватися.

Щорічно промислові та фінансові підприємства зазнають серйозних загроз у зв'язку з постійними атаками комп'ютерних вірусів — найбільшого класу, що спричиняють дестабілізацію програмних дій, це приводять до переривання контролю над виробничими процесами з можливими катастрофічними наслідками — ризиком для людських життів і навколишнього середовища. Кількість вірусних атак різко зростає в міру того, як усе більше підприємств зв'язують системи управління виробництвом із внутрішніми комп'ютерними мережами й глобальною мережею Інтернет.

Наведемо лише декілька фактів. У серпні 2005 р. 13 заводів промислової компанії Chrysler в США зупинилися через комп'ютерний вірус Zotob, він же атакував комп'ютери близько 100 компаній, серед них General Electric, Caterpillar, CNN. У лютому 2006 р. в результаті атаки комп'ютерного вірусу годину не працювали ринки Російської торгівельної системи.

Проблема безпеки інформації за часів загальної інформатизації, широкого впровадження електронних технологій — одна з найгостріших. Комплексне вирішення проблеми безпеки інформації як складової національної безпеки держави в цілому ґрунтується на розробці загальної стратегії. Основна властивість комп'ютерних вірусів — саморозмноження. Тому процедура, що здійснює цю функцію, в алгоритмі вірусу є центральною, усі інші (прояв, засоби маскування і т. д.) мають другорядне значення. Комп'ютерний вірус — це невелика програма, розроблена програмістом відповідної кваліфікації, здатна до саморозмноження та виконання різних деструктивних дій.

Бурхливий розвиток сучасних інформаційних технологій, комп'ютерних систем та обчислювальної техніки поряд із безперечними перевагами та позитивними результатами діяльності в сфері обробки найрізноманітнішої інформації спричинив також небажані і навіть шкідливі наслідки. Насамперед це масове поширення та "уко-

рінення" в інформаційних системах так званих програм-вірусів, які в результаті певних дій комп'ютера можуть створювати свої копії з подальшим інфікуванням інформації, в першу чергу на зовнішніх носіях даних.

Вплив вірусів різноманітний — від звичайного жарту до повного зруйнування даних. Користувачі часто несвідомо розповсюджують віруси, переписуючи дискети із різних машин. Нині найсприятливішим середовищем для існування та розмноження вірусів є популярна мережа Internet.

Існує чимало категорій комп'ютерних вірусів, які стали предметом аналізу експертів та незалежних дослідників. Установлено, що більшість вірусів можна виявити й легко знешкодити. Прогрес у цій сфері з'являється за умови, що власники обчислювальних машин повідомляють про віруси дослідникам та спеціалістам, які професійно займаються їх знешкодженням, створюючи потужні антивірусні програми та системи.

Основний зміст самостійної роботи студентів над дисципліною полягає у вивченні та застосуванні системи знань у галузі теорії та практики побудови і принципів функціонування обчислювальних машин, організацію обчислювальних процесів на персональних комп'ютерах (ПК) та їх алгоритмізацію, програмне забезпечення, захист інформації, а також ефективне використання сучасних інформаційно-комунікаційних технологій у професійній діяльності.

Самостійна робота — це також вивчення та засвоєння методичних вказівок до лабораторних робіт і додаткової літератури, зокрема нормативних документів з організації робіт.

Лише постійне самостійне навчання дає можливість наблизитися до вершини знань певної галузі, оволодіти такою сумою знань і вмінь, які дали б змогу заявити про себе як про професіонала. Студент, який хоче якомога краще оволодіти професією, має добре розуміти: на занятті викладач подає основи знань, навчає учитися, виділяє ті ключові істини дисципліни, які пробуджують у молодої людини потяг до поглиблення й удосконалення знань. Збагачення загальною сумою знань, накопичених людством, розширення загального світогляду, усвідомлення наявної перспективи щодо реалізації певних знань є основним мотивом сумлінного відношення до навчання. Самостійна навчальна діяльність студента буде лише тоді результативною, коли ґрунтуватиметься на внутрішній потребі. Виховання такої здатності

потребує чіткого узгодження процесу самоосвіти із цілями навчання та виховання студента.

Згідно з державними стандартами матеріал навчальної дисципліни, передбачений робочим навчальним планом для засвоєння студентом у процесі самостійної роботи, виноситься на підсумковий контроль поряд із навчальним матеріалом, який опрацьовувався при проведенні навчальних занять. Самостійна робота студента може проходити в бібліотеці вищого навчального закладу, навчальних кабінетах, комп'ютерних класах (лабораторіях), а також удома. Самостійна робота студента повинна бути спланована, організаційно й методично спрямована як особиста творча праця без безпосередньої взаємодії з викладачем. Навчальний час, відведений для самостійної роботи, регламентується робочим навчальним планом і повинен згідно з Болонською декларацією становити не менше 50 % загального обсягу навчального часу студента, відведеного для вивчення конкретної дисципліни. У необхідних випадках ця робота проводиться відповідно до заздалегідь складеного графіка, що гарантує можливість індивідуального доступу студента до потрібних дидактичних засобів. Графік доводиться до відома студентів на початку поточного семестру. При застосуванні складного обладнання чи устаткування, складних систем доступу до інформації (наприклад, комп'ютерних баз даних, систем автоматизованого проектування тощо) передбачається можливість отримати необхідні консультації або допомогу з боку фахівця.

Самостійне навчання може здійснюватись через:

- запам'ятовування певної інформації за рахунок уважного слухання й конспектування лекцій; активної роботи під час практичних занять;
- роботу над конспектами лекцій, планами практичних занять;
- опрацювання літературних джерел (конспектування самостійно вивченого матеріалу, рефератування);
- роботу з каталогами звичайних і електронних бібліотек, інформаційно-пошуковими сервісами Internet;
- вивчення навчального матеріалу за паперовими та електронними підручниками, навчальними посібниками, практикумами тощо;
- опрацювання матеріалу за першоджерелами, науковою і спеціальною літературою;

- підготовку доповідей, рефератів, написання курсових робіт; пошукову та науково-дослідну діяльність;
- самотестування.

Самостійна робота студента під час лекції. Лекційний матеріал призначається для спрямування студентів у найраціональнішому напрямі щодо вивчення навчальної дисципліни й акцентуванні уваги на складних, вузлових питаннях навчальної дисципліни. Належне ведення конспекту сприяє збереженню необхідної інформації та дає змогу в подальшому проаналізувати її. За умови подання лекційного матеріалу в усній формі одночасно засвоюється до 20% інформації. Викладання інформатики в комп'ютерних класах або в аудиторіях, обладнаних мультимедійним обладнанням (наприклад, мультимедійним проектором або сенсорним екраном), водночас із демонстрацією прийомів роботи з користувальницьким інтерфейсом програми дозволяє підвищити рівень засвоєння лекційного матеріалу до 50—60%.

Робота над конспектами лекцій, планами практичних занять. При підготовці до практичних занять студент має спиратися на складений ним конспект лекції. При опрацюванні матеріалу лекції слід зіставити законспектований матеріал із планом практичного заняття, що міститься в методичних матеріалах для практичних занять або в навчально-методичному комплексі. Якщо в конспекті бракує матеріалу з окремих питань лекції або недостатньо розкрито деякі питання практичного заняття, чи їх пропонується опрацювати самостійно, студент повинен звернутися до підручників, навчальних посібників і методичних матеріалів. Підготовку для практичного заняття краще за все здійснювати з використанням ПЕОМ зі встановленим на ньому відповідним програмним забезпеченням.

Працювати з підручниками, навчальними посібниками, методичними вказівками, практикумами, науковою й спеціальною літературою незалежно від типу їхнього носія (паперового чи електронного) необхідно таким чином, щоб отримати максимум теоретичних знань і навичок. При роботі із цими джерелами студент насамперед повинен ознайомитися з їхнім змістом, щоб визначити, чи необхідно опрацьовувати джерело й чи має воно відношення до навчального курсу, що вивчається, і тільки після цього визначити послідовність його опрацювання й відібрати необхідний для вивчення матеріал (глави, розділи тощо).

У разі роботи з інтерактивними електронними джерелами слід використовувати можливості навігації, що надаються сучасними програмами, призначеними для читання електронних документів відповідних форматів (MS Word, Adobe Reader, Adobe Acrobat та ін.), і, особливо, переваги гіпертекстової технології подання навчального матеріалу, а саме — за допомогою гіперпосилань знаходити відповіді на поставлені питання. При опрацюванні матеріалу необхідно з'ясувати суть питання, що вивчається, зокрема суть незрозумілих чи незнайомих слів, термінів. Саме інтерактивні гіпертекстові електронні джерела (довідки в складі програмних продуктів, електронні посібники та словники) дозволяють швидко конкретизувати терміни та визначення. При вивченні матеріалу необхідно аналізувати прочитане, порівнюючи із прослуханою та законспектованою лекцією, робити логічні висновки, позначати незрозумілі положення з метою їх подальшого з'ясування на практичному занятті. Бажано відпрацювати зручну для себе певну систему позначень (позначки на полях конспекту, підкреслення маркерами різних кольорів, доповнення конспекту альтернативними формулюваннями та посиланнями на інші джерела тощо) та фіксації опрацьованого матеріалу. Сучасні текстові редактори (в першу чергу MS Word) дають можливість створити електронний конспект із примітками, виносками, коментарями та зробити його роздруківку.

Для самостійного поглибленого вивчення навчального матеріалу студенту слід звертатися до наукової та спеціальної літератури, яка може бути й невказаною в навчально-методичному комплексі. Використання самостійно отриманих відомостей як у навчанні, так і на практиці є, безперечно, цінним здобутком у діяльності студента на шляху формування свого професійного потенціалу.

Робота з бібліотечними фондами та дистанційними джерелами з метою пошуку необхідної інформації. Знання з технологій захисту інформації належить до базової підготовки сучасної людини. З позицій випереджаючої освіти, навчання тільки за конспектом лекцій і основною літературою до програми є недостатнім. У більшості випадків належна підготовка потребує вмінь швидко знаходити та опрацьовувати необхідний матеріал за першоджерелами, науковою й спеціальною літературою та коректно його цитувати. Перелік такої літератури, як правило, наводиться в навчально-методичному комплексі навчальної дисципліни. Тому завдання студента зводиться до самостійного знаходження цих матеріалів шляхом перегляду паперових або електронних фондів бібліотек, а також різноманітних файлових архівів, баз даних та баз знань, доступ до яких здійснюється за

допомогою відповідних сервісів Internet (в основному — Word Wide Web, FTP та UseNet newsgroups).

Для пошуку документа використовуються різні його ознаки. Насамперед — реквізити (УДК. Автор(и). Заголовок опису. Основний заголовок: відомості, що належать до заголовку/Відомості про відповідальність. — Відомості про видання (в тому числі URL — адреса Web — документа або Ftp — файла). — Місце видання, дата видання. — Обсяг.).

УДК — це універсальна десяткова класифікація будь-яких офіційних видань у всьому світі. Відповідні довідники видаються багатьма мовами й постійно оновлюються. В Україні в 2006 р. Книжковою палатою України ім. І. Федорова видано "Універсальну десяткову класифікацію. Зміни та доповнення." Випуск 4" в паперовому варіанті. Довідкова база УДК постійно нарощується за рахунок електронних видань. Знання УДК дозволяє швидко знайти необхідне джерело за систематичним бібліотечним каталогом. Наприклад, УДК видань з інформаційних технологій починається з 004.

Коли код УДК невідомий, то необхідно звернутися до алфавітного каталогу й за назвою джерела або за прізвищем та ініціалами автора знайти бібліотечний шифр джерела.

Якщо ж студент здійснює наукове дослідження вибраної проблеми, готує наукову доповідь або виступ на конференції, однак йому не відомі реквізити джерела чи саме джерело, то слід вдатися до пошуку у систематичному бібліотечному каталозі. Завдання студента полягає в пошуку необхідної галузі (підгалузі), що поглинає потрібну інформацію, а потім у її межах — необхідні картки з бібліотечним шифром. Студент повинен оформити на літературу бібліотечне замовлення встановленого зразка, вказавши всі необхідні реквізити. Робота з електронними фондами за такої ситуації значно ефективніша, оскільки в розвинутих бібліотеках облік літератури ведеться в середовищах систем управління базами даних, за допомогою яких пошук потрібної інформації здійснюється найефективніше.

Сервіси мережі Internet надають унікальні можливості знаходити літературні джерела у географічно віддалених фондах та архівах, а також шляхом участі в мережних конференціях, саме там можна отримати відповіді та поради з питань пошуку необхідної інформації. Для доступу до Internet-ресурсів необхідно знати їх мережну адресу. Оскільки Internet постійно оновлюється й розвивається, у ньому немає єдиного каталогу, змісту або наочного покажчика ресурсів.

Проте в Internet існують різні інформаційно-пошукові системи, що допомагають користувачам знайти те, що їм потрібно. Це передусім тематичні каталоги й так звані пошукові машини. Тематичні (наочні) каталоги — це інформаційно-довідкові системи, підготовлені вручну редакторами цих систем на основі інформації, зібраної на серверах Internet. Інформація в них розподіляється за тематичними розділами відповідно до певної ієрархії. На верхньому рівні розміщено зібрані загальні категорії (наприклад, "Інтернет", "Бізнес", "Мистецтво", "Освіта" тощо), а на нижньому зроблено посилання на конкретні Web-сторінки або інші інформаційні ресурси. Для швидкого переходу до потрібного розділу тематичного каталогу можна скористатися вбудованою системою автоматичного пошуку за ключовими словами. Для цього в рядку запиту слід ввести ключове слово (поєднання слів), клацнути "Пошук", і система повідомить, чи є відповідний розділ у її каталозі й запропонує в нього перейти через усі проміжні розділи. Рекомендовано використовувати каталоги: http: // www. yahoo. com, http: // www. portal. edu. ru, http: // www. ipl. org.

Пошукові системи — це складні інформаційно-довідкові структури, що автоматично генеруються на основі даних, які збираються мережними програмами-роботами з усього Internet, і дають відповідь на запит користувача посиланнями на різні Internet-ресурси. Запит здійснюється за певною процедурою (певною мовою), яка може різнитися в різних системах, проте в спрощеному вигляді зводиться до того, що пошук інформації здійснюється за ключовими словами або словосполученнями, що найточніше відображають суть проблеми.

До загальних положень мов запитів належать:

- Ключові слова можна вводити у відповідне поле пошукової системи поодинці, послідовно звужуючи пошук, або ж уводити відразу декілька слів, розділяючи їх пробілами чи комами. Регістр не має значення.
- Режим пошуку "AND" ("І") означає, що буде знайдено тільки ті дані, де зустрічається кожне із ключових слів.
- При використанні режиму "OR" ("АБО") результатом пошуку будуть усі дані, де зустрічається хоча б одне ключове слово.
- Використовуйте знаки "+" і "–" перед ключовим словом. Щоб уникнути документа, де зустрічається певне слово, поставте перед ним мінус. І навпаки, щоб певне слово обов'язково було присутнє в документі, поставте перед ним плюс. Зверніть увагу на те, що між знаком і словом не повинно бути пробілу.

- Якщо Ви хочете виключити яке-небудь слово з пошуку, поставте перед ним знак "–". Наприклад: "+захист -Excell".
- За замовчуванням програма шукає всі дані, де зустрічається введене вами слово. Наприклад, при запиті "редактор" буде знайдено слова "редактор", "текстовий", "графічний", "газети", "головний" і багато інших. Знак оклику перед або після ключового слова означає, що будуть знайдені тільки слова точно відповідні запиту (наприклад, "текстовий! редактор!").

Також корисно запам'ятати й використовувати при пошуку такі прийоми.

- Якщо для пошуку потрібно ввести словосполучення, візьміть його в лапки.
- Якщо Ви пишете все слово буквами в рядок, буде знайдено всі варіанти його написання; якщо ж хоча б одна буква буде прописною, то система шукатиме тільки такі варіанти.
- Якщо Ви хочете знайти не текст, а яке-небудь зображення, то можна користуватися словом image. Наприклад, image: sea дасть список сторінок із зображенням моря.
- Якщо слово, яке Ви шукаєте, зустрічається в різних контекстах, можна виключити слова, які зустрічаються в непотрібному контексті. Наприклад, вказати аргумент пошуку +Celeron +Price +UA -USA.
- Перевіряйте орфографію. Якщо пошук не дав результату, можливо, при введенні Ви припустилися помилки.
- Використовуйте синоніми. Якщо список дуже малий або не містить корисних сторінок, спробуйте змінити слово. Наприклад, "реферати" можна замінити на "курсові роботи" або "твори".
- Якщо один із знайдених документів ближче до теми від інших, клацніть "Знайти схожі документи". Це посилання розташоване під короткими описами знайдених документів. Система їх проаналізує й знайде саме ті, що Ви вказали.

Подібних систем в Internet значно більше, ніж тематичних каталогів. Серед пошукових систем існують як широкі за тематикою, так і вузькоспеціалізовані. Найвідоміші з них: http: // www. google. com, http: // www. altavista. com, http: // www. askjeeves. com, http: // www. lycos. com, http: // www. sciseek. com, http: // www. msn. com, http: // meta. ua http: // www. rambler. ru, http: // www. yandex. ru, http: // www. aport. ru, http: // www. metabot. ru, http: // newsgroups. langenberg. com, uk. wikipedia. org, www. bukinist. agava. ru. Матеріали щодо методів підвищення ефективності пошуку інформації в Internet містяться в статях: http: // www. yandex. ru/info/search. html, http: // www. searchengines. ru/,

http: // www. zodchiy. ru/links/search/, http: // www. citforum. ru/internet/search/index. shtml, http: // websearch. report. ru/, http: // www. kokoc. com/search-engines/index. shtml, http: // www. zhurnal. ru/search-r. shtml.

Самостійна робота має такі складові та форми її оцінювання:

- підготовка та власне аудиторна робота під час практичних і лабораторних занять. Результати її оцінюються під час поточного контролю;
- виконання самостійних робіт у формі есе, рефератів із конкретних проблем та складання письмових звітів на електронних чи паперових носіях або шляхом виголошення усних доповідей;
- опрацювання програмного матеріалу зі змістового модуля та оцінка його результатів під час проміжного контролю;
- виконання письмової контрольної роботи або тестування;
- звіт про проходження практики;
- звіт про науково-дослідну роботу, результати якої можуть бути використані при написані випускної роботи, за рішенням кафедри опубліковані.

Метою дисципліни "Комп'ютерна вірусологія" є ознайомлення з основними поняттями про комп'ютерні віруси, історією їх виникнення, основними принципами функціонування та поширення, класифікацією та набуття необхідних знань і навичок щодо захисту інформаційних ресурсів від вірусів.

У результаті вивчення дисципліни студенти повинні

знати:

- основні принципи й правила побудови, структуру комп'ютерних вірусів, їх класифікацію, способи розповсюдження;
- класифікацію загроз безпеці комп'ютерних систем, а також методи боротьби з ними;

уміти:

- застосовувати теоретичні засади й принципи побудови сучасних і перспективних електронних обчислювальних машин, локальних, корпоративних, глобальних комп'ютерних мереж при вирішенні питань їх захисту від вірусів;
- демонструвати розуміння сучасних проблем вірусології, опанування певних прийомів низькорівневого програмування для де-

тальнішого засвоєння властивостей і характеристик основних об'єктів файлової системи;

- визначати критерії ефективності використання комп'ютерних антивірусних програмних засобів для створення умов безпеки інформації;
- використовувати методи аналізу для розробки методів захисту інформації;
- розробляти пропозиції (проекти) з питань захисту інформації та комп'ютерних систем від вірусів;
- здійснювати прогнози з питань розробки та використання обчислювальної техніки, мереж, програмного забезпечення від можливих вірусних атак;
- оцінювати можливі наслідки застосування елементів обчислювальної техніки, програмного забезпечення та їх систем при вірусних атаках;
- застосовувати у власній професійній діяльності набуті знання та навички.

володіти:

- системним аналізом методів розпізнавання комп'ютерних вірусів і їх впливом на обчислювально-управлінські комплекси підприємств, фірм, методів їх роботи та взаємодії з обчислювальним середовищем, використання системи інструментів для боротьби з ними, створенням систем захисту від вірусних атак.

ТЕМИ ДЛЯ САМОСТІЙНОЇ РОБОТИ

№ пор.	Назва розділу, теми курсу	Зміст завдання	Форми контролю
1	2	3	4
Змістовий модуль І. Основні поняття з теорії вірусів			
1	Тема 1. Загальні поняття про комп'ютерні віруси, історія їх виникнення та розвитку	1. Феномен комп'ютерних вірусів. Передісторія та хронологія їх виникнення 2. Перші випадки масового зараження комп'ютерними вірусами 3. Етичні проблеми, пов'язані з розповсюдженням комп'ютерних вірусів 4. Хто й для чого пише віруси? 5. Умови первісного зараження комп'ютера вірусом 6. Умови неможливості зараження комп'ютера вірусом	Конспект
2	Тема 2. Основні принципи функціонування комп'ютерних вірусів	1. Ознаки присутності вірусних програм 2. Загальні принципи функціонування комп'ютерних вірусів, їх розмноження Структура ("анатомія") комп'ютерного вірусу 3. Деструктивні можливості вірусів	Конспект
3	Тема 3. Класифікація комп'ютерних вірусів та принципи її побудови	1. Файлові, завантажувальні (бутові) та файлово-завантажувальні віруси 2. Макровіруси та мережні віруси 3. Класифікаційний код вірусу 4. Дескриптор вірусу 5. Сигнатура вірусу	Конспект

1	2	3	4
4	Тема 4. Алгоритми роботи вірусів	1. Резидентність 2. Використання стелс-алгоритмів 3. Самошифрування та поліморфізм 4. Використання нестандартних прийомів	Конспект
Реферат за модулем І			

Теми рефератів за модулем І

1. Історія, сучасна ситуація та перспективи в сфері вірусології.
   Література [1–4; 7; 9; 10; 15; 19]
2. Класифікаційний код вірусу. Дескриптор вірусу. Сигнатура вірусу.
   Література [1–4; 7; 9; 10; 15; 19]
3. Файлові віруси. Бутові віруси.
   Література [1–4; 7; 9; 10; 15; 19]
4. Мережні віруси.
   Література [1–4; 7; 9; 10; 15; 19]
5. Структура (“анатомія”) комп’ютерного вірусу.
   Література [1–4; 7; 9; 10; 15; 19]
6. Принципи та алгоритми роботи Word/Excel/Access-макровірусів.
   Література [1–4; 7; 9; 10; 15; 19]

Питання для самоконтролю та співбесіди за модулем І:

1. Предмет, структура та зміст дисципліни.
2. Визначення поняття “комп’ютерний вірус”.
3. Перші випадки масового зараження комп’ютерними вірусами.
4. Умови первісного зараження комп’ютера вірусом.
5. Ознаки наявності вірусних програм.
6. Етичні проблеми, пов’язані з розповсюдженням комп’ютерних вірусів.
7. Хто й для чого пише віруси?
8. Сучасна ситуація та перспективи.
9. Поведінка комп’ютерних вірусів.
10. “Невидимі” віруси.
11. Самомодифікуючі віруси.
12. Класифікація вірусів.
13. Цикл функціонування вірусів.
14. Деструктивні можливості вірусів.
15. Завантажувальні віруси й боротьба з ними.
16. Макровіруси.
17. Поштові віруси.
18. Файлові віруси.
19. Бутові віруси.
20. Мережні віруси.
21. Класифікаційний код вірусу.
22. Дескриптор вірусу.
23. Сигнатура вірусу.
24. Алгоритми роботи вірусу.
25. Принципи та алгоритми роботи Word/Excel/Access-макровірусів.
26. Роль комп’ютерних мереж при заражені вірусами.
27. “Небезпечний” Інтернет — міфи та реалії.
28. Небезпечні програми — троянські коні, приховане адміністрування.
29. Поняття вірусних атак.
30. Пошкоджені й заражені файли.

Тестові завдання за модулем І:

1. Історично виникнення вірусів пов’язане з ідеєю створення програм, що:
   - самовідтворюються;
   - самопошкоджуються;
   - переносяться.

2. Концепція створення програм, що самовідтворюються, виникла в:
   - шістдесяті роки;
   - п’ятдесяті роки;
   - сорокові роки.

3. Перший етап розробки вірусоподібних програм мав:
   - характер протистояння користувачів безвідповідальним або навіть кримінальним “елементам”;
   - дослідницький характер.

4. Другий етап розробки вірусоподібних програм мав:
   - характер протистояння користувачів безвідповідальним або навіть кримінальним “елементам”;
   - дослідницький характер.

5. На сьогодні можна вказати точну кількість вірусоподібних програм:

- так;
- ні.

6. Віруси можна розділити на класи за основними ознаками:

- місцем існування;
- операційною системою (ОС);
- величиною;
- особливостями алгоритму роботи;
- деструктивними можливостями.

7. За місцем існування віруси можна розділяти на:

- дискові;
- файлові;
- завантажувальні;
- макро;
- мережні;
- флешкові.

8. Файлові віруси:

- різними способами упроваджуються у виконавчі файли (найпоширеніший тип вірусів): або створюють файли-двійники (віруси компаньйона), або використовують особливості організації файлової системи (link-віруси);
- записують себе або в завантажувальний сектор диска (boot-сектор), або в сектор — системний завантажувач вінчестера (Master Boot Record), що містить, або міняють покажчик на активний boot-сектор;
- заражають файли-документи й електронні таблиці декількох популярних редакторів;
- використовують для свого розповсюдження протоколи або команди комп'ютерних мереж і електронної пошти.

9. Макро-віруси:

- різними способами упроваджуються у виконавчі файли (найпоширеніший тип вірусів): або створюють файли-двійники (віруси компаньйона), або використовують особливості організації файлової системи (link-віруси);
- записують себе або в завантажувальний сектор диска (boot-сектор), або в сектор — системний завантажувач вінчестера (Master Boot Record), що містить, або міняють покажчик на активний boot-сектор;

- заражають файли-документи й електронні таблиці декількох популярних редакторів;
- використовують для свого розповсюдження протоколи або команди комп'ютерних мереж і електронної пошти.

10. Серед особливостей алгоритму роботи вірусів виокремлюють такі:

- резидентність;
- паразитність;
- використання стелс-алгоритмів;
- самошифрування та поліморфізм;
- використання нестандартних прийомів.

11. Резидентний вірус при інфікуванні комп'ютера:

- не заражає пам'ять комп'ютера й зберігає активність обмежений час;
- залишає в оперативній пам'яті свою резидентну частину.

12. Макровіруси — це:

- резидентний вірус;
- нерезидентний вірус.

13. Вірус "Frodo" — це:

- завантажувальний вірус;
- стелс-вірус.

14. За деструктивними можливостями віруси можна розділити на:

- нешкідливі;
- безпечні;
- небезпечні;
- дуже небезпечні.

15. У циклі функціонування вірусів вирізняють кілька етапів, а саме:

- шість;
- десять;
- три.

16. Укажіть умови існування макро-вірусів у конкретній системі:

- прив'язки програми на макромові до конкретного файла;
- копіювання макропрограм з одного файла в інший;
- отримання управління макропрограмою без втручання користувача (автоматичні або стандартні макроси).

17. KakWorm, Stages і ILOVEYOU — це:

- завантажувальні віруси;
- макро-віруси;

- поштові віруси-хробаки.

18. Сигнатура вірусів — це:
- семафор вірусу;
- біти, які не мають відношення до основного “тіла” вірусу;
- унікальний програмний код вірусу.

19. За місцезнаходженням віруси можна розділити на:
- файлові;
- бутові;
- файлово-бутові;
- пакетні;
- мережні;
- WinWord-віруси;
- Windows-віруси;
- OS/2-віруси;
- Novell NetWare-віруси;
- BIOS- віруси;
- CD-ROM-віруси.

20. За наслідками деструктивних дій віруси поділяють на:
- нешкідливі;
- невразливі;
- уразливі;
- дуже уразливі.

21. За особливостями алгоритму віруси поділяють на:
- stealth-віруси;
- worm-віруси;
- companion-віруси;
- MtE-віруси;
- DIR-віруси;
- driver-віруси;
- віруси-паразити;
- віруси-привиди;
- “троянські” програми;
- логічні бомби;
- комбіновані віруси та ін.

22. За способом створення віруси поділяють на:
- створені ручними засобами розробки (Н-віруси);
- створені автоматизованими засобами розробки (А-віруси).

23. Код вірусу можна скопіювати:
- у таблицю налагодження адрес (для EXE-файлів);
- в область стека;
- поверх коду або даних програми (при цьому програма безповоротно пошкоджується).

24. Завантажувально-файлові віруси — це такі, що:
- спроможні вражати як код завантажувальних секторів, так і код файла;
- фальсифікують інформацію, читаючи з диску так, що активна програма отримує не правильні дані;
- заражають антивірусні програми, знищують або роблять їх непрацездатними;
- вражають одночасно EXE, COM, boot-сектор, MBR, FAT і директорії.

25. STEALTH-віруси — це такі, що:
- спроможні вражати як код завантажувальних секторів, так і код файла;
- фальсифікують інформацію, читаючи з диску так, що активна програма отримує не правильні дані;
- заражають антивірусні програми, знищують або роблять їх непрацездатними;
- вражають одночасно EXE, COM, boot-сектор, MBR, FAT і директорії.

26. Multipartition — це віруси, що:
- спроможні вражати, як код завантажувальних секторів, так і код файла;
- фальсифікують інформацію, читаючи з диску так, що активна програма отримує не правильні дані;
- заражають антивірусні програми, знищують або роблять їх непрацездатними;
- вражають одночасно EXE, COM, boot-сектор, MBR, FAT і директорії.

27. Ознаки зараження вірусом:
- зростання обсягу пам’яті;
- уповільнення роботи комп’ютера;
- затримки при виконанні програм;
- незрозумілі зміни у файлах;
- зміна дати модифікації файлів без причини;
- незрозумілі помилки Write-protection;
- помилки при інсталяції та запуску WINDOWS;
- відключення 32-розрядного допуску до диску;

- неспроможність зберігати документи Word в інших каталогах, крім TEMPLATE;
- некоректна робота дисків.

28. При переході вірусу в активну фазу легко помітити такі зміни:
- зникнення файлів;
- форматування HDD;
- неспроможність завантажити комп'ютер;
- неспроможність завантажити файли;
- незрозумілі системні повідомлення, музикальні ефекти тощо.

29. Основними джерелами вірусів є:
- дискети, флешки, CD-ROM з зараженими вірусом файлами;
- комп'ютерна мережа, зокрема система електронної пошти та Internet;
- жорсткий диск, на який перейщов вірус із заражених програм;
- вірус, що залишився в оперативній пам'яті після попереднього користувача.

30. Віруси можуть записувати своє тіло:
- у кінець файла-жертви;
- у середину;
- окремими "плямами".

31. Специфічними функціями для вірусу "черв'як" є:
- знаходити нові цілі для атаки;
- проникати в них;
- передавати свій код на видалену машину;
- запускати її (отримувати управління);
- перевіряти на зараженість локальну або видалену машину для запобігання повторного зараження.

32. Такі файли комп'ютерний вірус не тільки псує, а й заражає:
- графічні;
- програмні;
- інформаційні файли без даних;
- медіа-файли.

33. Такі різновиди вірусів перехоплюють звернення операційної системи до уражених файлів:
- "троянські" віруси;
- "паразитичні" віруси;
- віруси "черв'яки";
- віруси-невидимки (стелс-віруси).

34. Найнебезпечніші віруси, що руйнують завантажувальний сектор, — це:
- "троянські" віруси;
- "паразитичні" віруси;
- віруси "черв'яки";
- віруси-невидимки (стелс-віруси).

35. Резидентні віруси:
- активні до вимкнення комп'ютера;
- активні обмежений час;
- активізуються після натиснення на певну комбінацію клавіш.

№ пор.	Назва розділу, теми курсу	Зміст завдання	Форми контролю
1	2	3	4
Змістовий модуль II. Створення вірусів та захист			
1	Тема 5. Основи низькорівневого програмування	1. Прості приклади асемблерних програм 2. Основні типи даних 3. Контроль за зміною регістрів і прапорів 4. Основні арифметичні операції 5. Основні логічні операції. Операції зі стеком. 6. Безумовні та умовні переходи. Цикли 7. Базова техніка використання переривань	Конспект
2	Тема 6. Антивірусне програмне забезпечення	1. Принципи роботи антивірусних програм та їх класифікація 2. Методика використання антивірусних програм	Конспект
Реферат за модулем II			

Теми рефератів за модулем II

1. Створення простих типів вірусів.

Література [1–7]

2. Створення мережних типів вірусів.

Література [1–7]

3. Створення макровірусів.

Література [1–7]

4. Антивірусне програмне забезпечення.

Література [1–7]

5. Налаштування та робота в антивірусній програмі Dr. Web (Doctor Web)

Література [1–4; 8–20]

6. Налаштування пакета та робота в антивірусній програмі AVP (AntiViral Toolkit Pro).

Література [1–4; 8–20]

Питання для самоконтролю та співбесіди за модулем II:

1. Прості приклади асемблерних програм.
2. Основні типи даних.
3. Контроль за зміною регістрів і прапорів.
4. Основні арифметичні операції.
5. Основні логічні операції.
6. Операції зі стеком.
7. Безумовні та умовні переходи.
8. Цикли.
9. Базова техніка використання переривань.
10. Використання засобів захисту від вірусів операційної системи Windows.
11. Вірусофобія. Вірусні містифікації.
12. Які ви знаєте джерела зараження комп'ютерним вірусом?
13. За якими ознаками можна виявити факт зараження комп'ютерним вірусом?
14. Які заходи рекомендується вживати, щоб запобігти зараженню комп'ютерним вірусом?
15. Що таке антивірус? Які типи антивірусів ви знаєте?
16. Що таке евристичний аналізатор? Які функції він виконує?
17. Наведіть приклади антивірусних програм. Коротко охарактеризуйте їх.
18. Принципи роботи антивірусних програм та їх класифікація.
19. Методика використання антивірусних програм.
20. Призначення, основні можливості, налаштування та робота в антивірусній програмі AVP (AntiViral Toolkit Pro).

21. Призначення, основні можливості, налаштування та робота в антивірусній програмі Dr. Web (Doctor Web).
22. Призначення, основні можливості, налаштування та робота в антивірусній програмі Ad-aware 6.0.
23. Варіанти типового сканування.
24. Головне меню програми.
25. Початок сканування.
26. Дії над списком карантин.
27. Результати сканування.
28. Додавання елементів до списку ігнорування.
29. Призначення, основні можливості, налаштування та робота в антивірусній програмі Symantec AntiVirus.
30. Налагодження захисту від змін.
31. Налагодження повідомлень про віруси, загрози безпеці.
32. Категорія "Журнали".
33. Відбір записів за датою.
34. Відбір записів за категорією подій.
35. Видалення записів із журналу подій.
36. Експорт даних у файл. csv.
37. Категорія "Огляди при запуску".
38. Категорія "Призначені для користувача огляди".
39. Категорія "Планові огляди".
40. Застосування Symantec AntiVirus разом з Windows Security Center.
41. Зміна й видалення оглядів.
42. Оновлення баз даних програми вручну.

Тестові завдання за модулем II:

1. Заголовок EXE-файла складається з:
- сигнатури;
- даних;
- таблиці для налагодження адрес.

2. Запускається дізасемблер командою:
- sr test-com
- call sub_1
- sub_1: pop si
- sub si,3

3. Синтаксичні особливості мови Асемблер. Команди двійкової арифметики (команди складання):

- mov AH, 3dh
- mov AL, 0
- mov Dx, offset frame
- int 21h
- jnc ok

4. Спроба відкрити файл:
- mov ah,0
- int 21h
- mov day, dl
- mov month, dh
- add cx,1980
- mov year, cx

5. Використання вільного вектора переривань користувача:
- mov ah,0
- intlah
- mov oldcount, dx
- mov ah,0
- movbx, oldcount
- cmp bx, dx
- jc adjust
- sub dx, bx
- jmp short
- adjust:
- mov cx,0fiffh
- sub cx, bx
- add cx, dx
- mov dx, cx

6. Призначення та характеристика індексних регістрів. Команди двійкової арифметики (команди множення й ділення).
- mov AH, 4ch
- mov AL, errcode
- int 21h

7. Визначається сегментна адреса вільної ділянки пам'яті, розмір якої достатній для розміщення EXE-програми:
- створюється й заповнюється блок пам'яті для змінних середовищ;
- створюється блок пам'яті для PSP і програм (сегмент ЮООООЬ — PSP;
- сегмент+ООЮЬЮОООЬ — програма.

8. У такому файлі записано програму захисту BIOS від вірусів:
- Setup;
- Bat;
- int 13h.

9. Евристична маска — це:
- набір дій, виявлених при перевірці файла;
- порядковий номер першої з евристичних масок, що збіглися.

10. Евристичне число — це:
- набір дій, виявлених при перевірці файла;
- порядковий номер першої з евристичних масок, що збіглися.

11. Правила профілактики від зараження вірусами:
- з файлів, які постійно перебувають у роботі, необхідно робити резервні копії;
- слід купувати дистрибутивні копії програмного забезпечення тільки в офіційних продавців;
- не слід запускати неперевірені антивірусні програми, отримані із сумнівних джерел;
- при лікуванні дисків слід використовувати свідомо "чисту" операційну систему.

12. Укажіть основні типи антивірусних програм:
- сканери;
- перфоратори;
- монітори;
- ревізори змін;
- суперматори;
- імунізатори;
- поведінкові, які блокують.

13. Сканери — це антивірусні програми, які:
- шукають у файлах, пам'яті, завантажувальних секторах сигнатур вірусів;
- знімають оригінальні контрольні суми з можливих об'єктів зараження;
- перехоплюють різні події й у разі підозрілих дій.

14. Поведінкові, які блокують, — це антивірусні програми, що:
- шукають у файлах, пам'яті, завантажувальних секторах сигнатур вірусів;
- знімають оригінальні контрольні суми з можливих об'єктів зараження;
- перехоплюють різні події й у разі підозрілих дій.

15. Ревізори змін — це антивірусні програми, що:
- шукають у файлах, пам'яті, завантажувальних секторах сигнатур вірусів;
- знімають оригінальні контрольні суми з можливих об'єктів зараження;
- перехоплюють різні події й у разі підозрілих дій.

16. Укажіть харктерні ознаки прояву наявності вірусу в ПК:
- деякі програми відмовляються працювати або починають працювати неправильно;
- на екран виводяться сторонні повідомлення, символи тощо;
- робота на комп'ютері істотно сповільнюється;
- деякі файли виявляються зіпсованими.

17. Методи захисту інформації:
- програмні;
- віртуальні;
- апаратні;
- програмно-апаратні;
- демократичні;
- фізичні;
- правові;
- централізовані;
- організаційні.

18. Детектори (сканери)призначені для:
- діагностування (для лікування призначена інша антивірусна програма або це робитиме професійний програміст — "вірусолог");
- знаходження й видалення вірусів (фаги) або декількох вірусів (поліфаги);
- контролю за всіма (відомими на момент випуску програми) можливими способами зараження комп'ютерів, за всіма операціями, що є в пам'яті комп'ютера;
- обробки файлів і завантажувальних секторів із метою попередження зараження відомими вірусами.

19. Охоронці призначені для:
- встановлення діагнозу (для лікування призначена інша антивірусна програма або це робитиме професійний програміст — "вірусолог");
- знаходження й видалення вірусів (фаги) або декількох вірусів (поліфаги);

- контролю за всіми (відомими на момент випуску програми) можливими способами зараження комп'ютерів, за всіма операціями, що є в пам'яті комп'ютера;
- обробки файлів і завантажувальних секторів із метою попередження зараження відомими вірусами.

20. Фаги (поліфаги) призначені для:
- встановлення діагнозу (для лікування призначена інша антивірусна програма або це робитиме професійний програміст — "вірусолог");
- знаходження й видалення вірусів (фаги) або декількох вірусів (поліфаги);
- контролю за всіма (відомими на момент випуску програми) можливими способами зараження комп'ютерів, за всіма операціями, що є в пам'яті комп'ютера;
- обробки файлів і завантажувальних секторів із метою попередження зараження відомими вірусами.

21. Ревізори призначені для:
- встановлення діагнозу (для лікування призначена інша антивірусна програма або це робитиме професійний програміст — "вірусолог");
- знаходження й видалення вірусів (фаги) або декількох вірусів (поліфаги);
- контролю за всіма (відомими на момент випуску програми) можливими способами зараження комп'ютерів, за всіма операціями, що є в пам'яті комп'ютера;
- обробки файлів і завантажувальних секторів із метою попередження зараження відомими вірусами;

22. Вакцини призначені для:
- встановлення діагнозу (для лікування призначена інша антивірусна програма або це робитиме професійний програміст — "вірусолог");
- знаходження й видалення вірусів (фаги) або декількох вірусів (поліфаги);
- контролю за всіма (відомими на момент випуску програми) можливими способами зараження комп'ютерів, за всіми операціями, що є в пам'яті комп'ютера;
- обробки файлів і завантажувальних секторів із метою попередження зараження відомими вірусами.

23. До загальних засобів, що допомагають запобігти зараженню та його руйнівних наслідків, належать:

- резервне копіювання інформації (створення копій файлів і системних областей жорстких дисків);
- уникнення користування випадковими й невідомими програмами (найчастіше віруси розповсюджуються разом із комп'ютерними вірусами);
- перезавантаження комп'ютера перед початком роботи, насамперед тоді, коли за ним працювали інші користувачі;
- обмеження доступу до інформації, зокрема, фізичний захист дискети під час копіювання файлів із неї.

24. Розрізняють такі типи антивірусних програм:

- програми-детектори: призначені для знаходження заражених файлів одним із відомих вірусів;
- програми-лікарі: призначені для лікування заражених дисків і програм;
- програми-ревізори: призначені для виявлення заражених вірусом файлів, а також знаходження ушкоджених файлів;
- лікарі-ревізори: призначені для виявлення змін у файлах і системних областях дисків та їх відновлення;
- програми-фільтри: призначені для перехоплення звернень до операційної системи, що використовуються вірусами для розмноження, та повідомляють про це користувача;
- програми-вакцини: використовуються для обробки файлів і boot-секторів із метою попередження зараження.

25. Групу людей, які займаються написанням вірусів, називають:

- віймейкарами.
- позитронами.
- хакерами.
- крекерами.

26. Для оцінювання головного критерію тестованих антивірусних програм — якості захисту, враховуються такі параметри:

- якість евристичного аналізу;
- швидкість реакції при виявленні вірусів;
- якість сигнатурного аналізу;
- якість поведінкового блокиратора;
- здатність до лікування активних заражень;
- якість самозахисту;
- можливість підтримки упаковників;

- частота помилкових спрацьовувань.

27. Такі типи антивірусних програм здатні виявляти і лікувати заражені файли:

- вартуючі;
- детектори;
- ревізори;
- доктори.

28. Такі типи антивірусних програм здатні ідентифікувати тільки відомі їм віруси та потребуть оновлення антивірусної бази:

- вартуючі;
- детектори;
- ревізори;
- доктори.

29. Такі типи антивірусних програм подають сигнал тривоги, але лікувати не можуть:

- вартуючі;
- детектори;
- ревізори;
- доктори.

30. Антивірусна програма Dr. Web — це:

- програма-сторож;
- програма-детектор;
- програма-ревізор;
- програма-доктор.

31. Комп'ютер не може зазнати зараження вірусом, якщо Ви:

- запустили заражений виконуваний файл;
- вставили в дисковод заражену дискету;
- установили заражений драйвер;
- відкрили для редагування заражений документ MS Word.

МЕТОДИЧНІ ВКАЗІВКИ ДО ПІДГОТОВКИ, НАПИСАННЯ ТА ЗАХИСТУ РЕФЕРАТУ

Реферат є складовою вивчення дисципліни.

Завдання підготовлено відповідно до курсу: **"***Комп'ютерна вірусологія***"** (для бакалаврів).

Мета — допомогти студентам засвоїти теоретичні знання й удосконалити навички захисту інформації, використання сучасних нових інформаційних технологій у сфері захисту від вірусних атак (пакетів

прикладних програм) і засобів обчислювальної техніки. Оформлення й захист рефератів повинні сприяти активному засвоєнню нового матеріалу, виробленню в студентів уміння комплексно використовувати суміжні дисципліни для вирішення практичних питань.

Орієнтовна структура і обсяги реферату мають бути такими.

План (розділи)	Обсяг у сторінках (приблизно)	Короткий зміст (що потрібно висвітлити)
Вступ	До однієї	Мета, загальна характеристика, визначення номера варіанта завдання
Назва кожного питання реферату	1 — 2, загальний обсяг роботи в межах 20–30	Викладення суті питання з наведенням прикладів та посиланнями на літературні джерела
Висновки	До однієї	Прикладне значення
Список літератури	До однієї	
Додатки	До трьох	Якщо є

Загальний обсяг роботи не повинен перевищувати 20–30 сторінок машинописного тексту через 2 інтервали, рукописне викладення тексту не повинно перевищувати 18–24 сторінок шкільного зошита.

Студент повинен розкрити як питання теоретичного плану, так і описати технологію розв'язання практичної задачі, якщо таке передбачено рефератом.

Відповіді на теоретичні питання потребують ретельної роботи з літературою. Крім виписок і конспектування з літературних джерел, наприклад, з Internet, студент має зробити висновки. Робота повинна бути виконана самостійно з посиланнями на використану літературу. У висновках у цілому до реферату розглядають питання економічної доцільності та практичного застосування сучасних інформаційних технологій, обчислювальної техніки в сфері захисту.

Реферат слід оформляти на стандартних аркушах паперу, зброшурованих у папку. Усі аркуші мають бути пронумеровані. На титульній сторінці вказується назва вищого навчального закладу, факультет, спеціальність, дисципліна, курс, група, а також прізвище, ініціали та номер залікової книжки.

На першій сторінці наводяться розрахунки варіанта контрольної роботи та питання до нього і проставлено відповідні номери сторінок. На останній сторінці ставиться підпис виконавця і дата. У кінці роботи вміщується список використаної літератури. Зшита папка повинна

бути вкладена в поліетиленовий файл та містити дискету з повним текстом, графікою та іншими матеріалами, що стосуються реферату.

Кожен студент отримує окреме завдання для виконання КР згідно з варіантом Z, котрий обчислюється за формулою:

$Z = \mathrm{mod}_{10}(NZK + PR - 2000) + 1$,

де NZK — номер залікової книжки (студентського білета);

PR — рік отримання завдання.

Наприклад, NZK = 398, PR =2001, тоді

$Z = \mathrm{mod}_{6}(398+2008 - 2000)+1 = \mathrm{mod}_{6}(406) + 1 = 4+1=5.$

Отже, тут Z=5.

Для довідки: $\mathrm{mod}_a b$ дорівнює залишку від ділення b на a.

Увага! Неправильно оформлена робота без перевірки повертається на дооформлення та виконана не за своїм варіантом — підлягає переробці.

Індивідуально-консультативна робота з дисципліни здійснюється у формі консультацій за графіком (одна консультація на два тижні). На консультаціях студенти отримують пояснення з виконання самостійної роботи, вказівки щодо підготовки до практичних занять, здійснюється перевірка та захист завдань, винесених на поточний контроль тощо.

СПИСОК ЛІТЕРАТУРИ

Основна

1. *Безруков Н. Н.* Компьютерная вирусология. — К., 1991. — 414 с.
2. *Гульев И.* Компьютерные вирусы, взгляд изнутри. — ДМК, 1998.
3. *Касперский Е. В.* Компьютерные вирусы: что это такое и как с ними бороться. — СК Пресс, 1998.
4. *Коваленко М. М.* Комп'ютерні віруси і захист інформації. — К.: Наук. думка, 1999. — 268 с.
5. *Рудаков П. И., Финогенов К. Г.* Язык ассемблера: уроки программирования. — М.: ДИАЛОГ-МИФИ, 2001. — 640 с.

Додаткова

6. *Косарёв В. П.* Компьютерные сети и системы. — М., 2000.
7. *"Хакер"*. — 2001. — № 32 & № 35.
8. *Домарев В. В.* Безопасность информационных технологий. — СПб.: DiaSoft, 2002. — 688 с.
9. *История* вирусологии — http: // comp/comp — anv. php
10. *Компьютерные* вирусы — http: // www. virusnyaki. ru/

11. *Способы* проверки от вирусов — http: / ru. wikipedia. org/ wiki4/
12. *Антивирусные* программы — http/www. allware. info/doc/viruses/avp 6/
13. *Галатенко В. А., Гагин А. В.* Информационная безопасность — обзор основных положений (часть 1,2,3), Jet INFO, # 1,2,3, 1996.
14. *Защита* компьютерных систем от разрушающих программных воздействий: Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 128 с.
15. *Зегжда Д. П., Калинин М. О., Степанов П. Г.* Теоретические основы информационной безопасности. Защищенные операционные системы. Руководство к практическим занятиям / Под ред. проф. П. Д. Зегжды. — СПб., 1998. — 69 с.
16. *Компьютеры*: Справочное руководство: В 3 т. / Под ред. Г. Хелмса. — М.: Мир, 1986.
17. *Конев И., Беляев А.* Информационная безопасность предприятия. — СПб.: БХВ Петербург, 2003. — 752 с.
18. *Методы* и средства защиты информации / Под ред. Ю. С. Ковтанюка. — К.: ЮНИОР, 2003. — 501 с.
19. *Олецький О. В.* Принципи роботи комп'ютерних систем: Навч. посіб. — К.: Академія, 2003. — 144 с.

ГЛОСАРІЙ

ACESS CONTROL (управління доступом, контроль за доступом) — попередження несанкціонованого використання ресурсу.

Alias (Альтернативне/додаткове ім'я): хоча кожен вірус має спеціальне ім'я, проте дуже часто він більш відомий під своїм псевдонімом (описується відміність або характерне для цього вірусу). У таких випадках ми говоримо про вірусний 'alias'. Наприклад, вірус CIH також відомий під псевдонімом Chernobyl.

Anti-Debug / Anti-debugger (Анти-налагодження/анти-налагоджувач): методи використовуються вірусами для того, щоб приховати свою присутність.

Antivirus / Antivirus Program (Антивірус/антивірусна програма): сканують пам'ять, дисководи та інші частини комп'ютера на наявність вірусів.

Armouring (Бронювання): метод використовується для того, щоб вірус приховав свою присутність і уникнув виявлення антивірусом.

Autoencryption (Автокодування): спосіб, у рамках якого вірус кодує (шифрує) себе частково або повністю, що значно утруднює аналіз або виявлення.

Backup (Резервне копіювання, резервна копія) — це копія окремих файлів, груп файлів або всього диска, збережених на окремому носієві.

Boot virus (Завантажувальний вірус): вражає конкретно завантажувальний сектор як жорсткого диска, так і дискет.

Category / Type (of virus) (Категорія/Тип (вірусу): оскільки існує багато різних типів вірусів, то для зручності вони згруповані відповідно до певних типових характеристик.

Cavity (Вільні осередки): метод, що використовується певними вірусами й черв'яками з метою утруднення їх виявлення, при його застосуванні розмір файла не змінюється (заповнюються тільки вільні осередки в зараженому файлі).

Code (Код): вірусний код, написаний певною мовою програмування.

Companion / Companion virus / Spawning (Компаньйон/вірус-компаньйон): тип вирусів, які не вставляють себе в програми, а приєднуються до них.

CVP — Content Vectoring Protocol (Протокол перенаправлення контента): протокол розроблено 1996 Check Point Software, дозволяє антивірусному захисту бути інтегрованим у сервер брандмауера (файервола).

Damage level (Рівень пошкодження): показує рівень негативної дії вірусу на заражений комп'ютер, один із чинників, що використовується для визначення рівня загрози.

Detection updated on (Оновлення виявленого шкідливого ПЗ): останні дані про те, коли проводилося оновлення виявленого шкідливого ПЗ у сигнатурному файлі вірусів.

Disinfection (Дезинфекція): дія, коли антивірус виявляє й видаляє вірус.

Distribution level (Рівень розподілу): це значення, яке показує, як швидко і як далеко розповсюджується вірус. Один із чинників визначення рівня загроз.

DOS / Denial of Service< (Відмова в обслуговуванні): це викликаний діями вірусів тип атак, які перешкоджають доступу користувачів до певних служб (у ОС, веб-серверах).

Dropper (Інсталятор шкідливої програми): файл, який містить різні типи вірусу.

Encryption / Self-encryption (Шифрування/Самошифрування): техніка, що використовується деякими вірусами для того, щоб приховати свою присутність і уникнути виявлення антивірусними програмами.

PO (Entry Point Obscuring), Утаєння точки входу: технологія зараження програм, коли вірус намагається приховати свою точку входу для того, щоб не виявити свою присутність. Замість того, щоб почати свою дію одразу, вірус дозволяє зараженій програмі певний час працювати безпомилково, а вже потім відбувається його активація.

Exceptions (Виключення): технологія використовується антивірусними програмами для виявлення вірусів.

Firewall, Brandmauer (Міжмережний екран, брандмауер).

First detected on (Вперше виявлений...): дата, коли виявлене шкідливе ПЗ було вперше включено в сигнатурний файл вірусів.

Heuristic scan (Евристичне сканування): термін, пов'язаний із проблемою, яка вирішується методом проб і помилок у комп'ютерному світі, належить до технології виявлення невідомих вірусів.

Hoax (Розіграш): помилкове повідомлення, застереження про вірус, якого немає.

IDS – Intrusion Detection System (Система виявлення вторгнення): призначена для визначення ворожої активності в мережі.

In The Wild (У дії): офіційний список вірусів, випускається щомісяця, повідомлення про їхні дії.

Infection (Зараження): процес впровадження вірусу в комп'ютер, у його файли.

Link virus (Віруси-посилання): змінює адресу файла на адресу вірусу. У результаті при запуску комп'ютера і відкритті файла активується вірус, початковий файл стає непридатним для використання.

Macro (Макрос): це ряд інструкцій з приводу того, щоб програма, скажімо, Word, Excel, PowerPoint, Access виконувала позначені операції. Оскільки макроси є програмами, то можуть бути атаковані вірусом. Віруси, що використовують макрос для зараження, називаються макровірусами.

Macro virus (Макровірус): вірус, який вражає макрос у документах Word, таблицях Excel, презентаціями PowerPoint і т. д.

Malware (Шкідливе ПЗ): цей термін вживається стосовно всіх програм, що містять шкідливий код (MALicious softWARE): вірус, троян або черв'як.

Multipartite (Складений): це характеристика особливого типу складного вірусу, який заражає комп'ютери, використовуючи комбінацію технологій інших вірусів.

Overwrite (Перезаписувати): це дія, яку здійснюють певні програми або віруси, коли перезаписують файл, стираючи його вміст.

Permanent protection (Постійний захист): це процес, до якого вдаються деякі антивірусні програми під час безперервного сканування файлів, що використовуються в інших операціях (навіть якщо це користувач або ОС.) Також відомі як охоронні або резидентні.

Polymorphic / Polymorphism (Поліморфний/поліморфізм): техніка, до якої вдаються віруси для зашифровування своєї сигнатури кожного разу по-новому, або навіть інструкції для виконання шифрування.

Prepending (Приєднання спереду): це техніка, до якої вдаються віруси для зараження файлів шляхом приєднання своїх кодів на їх початок, забезпечуючи свою активацію уже при першому використанні зараженого файла.

Replica (Копіювання/Реплікація): дія, коли вірус копіює себе з метою подальшого свого розповсюдження.

Resident / Resident virus (Резидент/резидентний вірус): програми, що зберігаються в пам'яті комп'ютера і постійно відстежують операції, здійнювані на ньому.

Signature / Identifier (Сигнатура/Ідентифікатор): це схоже на паспорт вірусу, послідовність знаків (числа, букви тощо) визначають вірус.

Stealth (Прийом): техніка, коли віруси залишаються непоміченими для користувачів або антивірусних програм.

Tunneling (Тунелівання): технологія руйнування антивірусного захисту

Vacination (Вакцинація): технологія антивірусу, дозволяє інформації на файлі зберегтися, а можливі зараження виявити щойно зміни в файлі будуть помічені.

Variant (Варіант): це модифікована версія початкового вірусу, який може відрізнятися від останнього способами зараження і враженнями від нього.

Virus (Вірус): це програми, які можуть потрапляти в комп'ютери або IT системи різними способами, викликаючи ефекти від просто дратівливих до дуже руйнівних і непоправних.

Virus constructor (Конструктор вірусів): шкідлива програма, призначена для створення нових вірусів без навичок програмування, оскільки має інтерфейс, який дозволяє вибрати характеристики для створюваного шкідливого ПО: тип, зброя, файли поразки, шифрування, поліморфізм тощо.

Virus Signature File (Вірусний файл сигнатури): файл, який дозволяє антивірусу виявляти віруси.

WORM ("черв'як", різновид комп'ютерного вірусу) — анонімна програма, яка присутня в системі, загрожує файлам і може копіювати себе в інші частини системи.

XOR (OR-Exclusive), що Виключає АБО, нееквівалентність: операція, що використовується багатьма вірусами для зашифровування свого контенту.

Антивірус (anti-virus): клас програмного забезпечення для запобігання інфікуванню системи вірусами.

Антивірусний захист (у сфері захисту інформації) — комплекс організаційних, правових, технічних і технологічних заходів, що вживаються для забезпечення захисту засобів обчислювальної техніки й автоматизованих систем від дії програм-вірусів.

Безпека інформації — стан інформації, інформаційних ресурсів та інформаційних систем, при якому з необхідною вірогідністю забезпечується збереження даних від витоку, розкрадання, втрати, несанкціонованого знищення, спотворення, модифікації (підробки), копіювання, блокування тощо.

Бомба в повідомленні електронної пошти — частина повідомлення електронної пошти, що містить інтерактивні дані для виконання зловмисних дій на комп'ютері одержувача.

Брандмауер — комплекс апаратних і програмних засобів, що перешкоджає несанкціонованому переміщенню даних між мережами.

Вакцини — програми, які впроваджують себе у виконувану програму для перевірки ознак і попередження в разі виникнення змін.

Віруси, що вражають початкові коди — при попаданні на заражений ПК такий вірус шукає й записує себе в компоненти програми, що ще не відкомпілювалися. Після цього він може бути видалений.

Віруси-компаньйони. За своєю дією схожі на ті, що перезаписуються, однак цільовий файл не знищується, а переміщується в інше

місце. Таким чином, при запуску файла, інфікованого таким вірусом, спочатку відкриється код вірусу, а вже потім власний.

Віруси-ланки. Змінює адресу зараженого файла на свою, примушуючи ОС запускати себе замість цільового файла. Після виконання тіла вірусу управління, як правило, передається самій програмі.

Ефективність захисту інформації — ступінь відповідності результатів захисту інформації до поставленої мети.

Журнал аудиту (аудиторський слід) — хронологічний запис даних про використання системних ресурсів: зведення про входи користувачів, доступи до файлів та спроби або факти порушення захисту, як легальні, так і несанкціоновані.

Завантажувальні віруси — вражають сектор початкового завантажувача дискети BR або сектор головного завантажувача вінчестера MBR.

Збір інформації — це діяльність суб'єкта з метою отримати відомості про об'єкт, що його цікавить.

Неможливість обминути захисні засоби. Усі інформаційні потоки в мережу і з неї мають проходити через засоби захисту. Не повинно бути таємних модемних входів або тестових ліній, що йдуть в обхід захисту.

Неможливість переходу в небезпечний стан. Цей принцип означає, що за будь-яких обставин, зокрема нештатних, захисний засіб виконує свої функції або навіть блокує доступ.

Ознака проникнення. Опис ситуації або умови, коли може статися проникнення; опис системних подій, що свідчать про проникнення.

Пакет "Чорнобиль", називається також пакетом "Камікадзе". Мережний пакет, що викликає передачу незліченної кількості пакетів даних і перевантаження мережі.

Паразитуючі віруси — вид файлових вірусів, що змінюють цільовий файл, додаючи в нього свій код. При цьому сам заражений файл працездатність зберігає майже завжди.

Перезаписуючі віруси — записують своє тіло замість коду програми, не змінюючи назви початкового файла. Внаслідок при запуску зараженого файла розглядається код вірусу, а не сама програма.

Порушення безпеки: успішне подолання засобів захисту й проникнення в систему.

Резидентна програма — програма, яка після завантаження в ОЗУ та передачі їй управління ініціалізується таким чином, що постійно знаходиться в ОЗУ і виконується паралельно з іншими програмами.

Реплікатор — будь-яка програма, що копіює себе, наприклад черв'яки, логічні бомби, віруси.

Ретро-вірус — чекає зараження всіх можливих резервних носіїв, щоб не дати можливості системі повернутися до неінфікованого стану.

Різноманітність захисних засобів. Принцип, що рекомендує організовувати різні за своїм характером оборонні рубежі.

Троянський кінь: на перший погляд, корисна й нешкідлива програма, що містить додатковий прихований код, однак здійснює несанкціонований збір, використання, фальсифікацію або руйнування даних.

Фаг. Програма, що модифікує інші програми або бази даних несанкціонованими способами (за допомогою вірусів або "троянських коней").

Файлові черв'яки. Створюють на зараженому комп'ютері свої копії з назвами "game. exe", "instal. exe", сподіваючись, що користувач з необережності їх відкриває.

Шкідливий код — це устаткування, програмне забезпечення або програмно-апаратні засоби, зумисне включені в систему з метою здійснення несанкціонованих дій (наприклад, "троянський кінь").

ЗМІСТ

Відповідальний за випуск *А. Д. Вегеренко*
Редактор *О. М. Коваленко*
Комп'ютерне верстання *А. П. Нечипорук*

Зам. № ВКЦ-4470

Формат 60×84/16. Папір офсетний.
Друк ротаційний трафаретний.
Наклад 30 пр.
Міжрегіональна Академія управління персоналом (МАУП)
03039 Київ-39, вул. Фрометівська, 2, МАУП
ДП «Видавничий дім «Персонал»
03039 Київ-39, просп. Червонозоряний, 119, літ. ХХ
Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи ДК № 3262 від 26.08.2008