МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

МЕТОДИЧНІ МАТЕРІАЛИ ЩОДО ЗАБЕЗПЕЧЕННЯ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

з дисципліни

“КОМП’ЮТЕРНА ВІРУСОЛОГІЯ”

(для бакалаврів)

Київ
ДП «Видавничий дім «Персонал»
2014

Підготовлено доцентом кафедри прикладної математики та інформаційних технологій *В. М. Ахрамовичем*

Затверджено на засіданні кафедри прикладної математики та інформаційних технологій (протокол № 5 від 05.02.10)

Схвалено Вченою радою Міжрегіональної Академії управління персоналом

Ахрамович В. М. Методичні матеріали щодо забезпечення самостійної роботи студентів із дисципліни "Комп'ютерна вірусологія" (для бакалаврів). — К.: ДП «Вид. дім «Персонал», 2014. — 40 с.

Методичні матеріали містять пояснювальну записку, тематичний план, питання щодо самостійного вивчення студентами та самоконтролю, теми рефератів, тестові завдання, глосарій, а також список літератури.

ПОЯСНЮВАЛЬНА ЗАПИСКА

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

Щорічно промислові й фінансові підприємства піддаються серйозним погрозам у зв'язку з постійними атаками комп'ютерних вірусів — найбільшого класу дестабілізуючих програмних дій. Атаки призводять до переривання контролю над виробничими процесами з можливими катастрофічними наслідками. Це є ризиком для людських життів і навколишнього середовища. Вірусні атаки різко зростають через велику кількість підприємств, які зв'язують системами управління виробництвом із внутрішніми комп'ютерними мережами й глобальною мережею Інтернет.

Приведемо лише декілька фактів. У серпні 2005 р. 13 заводів промислової компанії Chrysler в США зупинилися через комп'ютерний вірус Zotob. Також Zotob атакував комп'ютери близько 100 компаній, серед них General Electric, Caterpillar, CNN. У лютому 2006 р. внаслідок атаки комп'ютерного вірусу на цілу годину було припинено роботу всіх ринків Російської торгівельної системи.

Проблема безпеки інформації в період загальної інформатизації, широкого впровадження електронних технологій — одне з найгостріших питань сьогодення. Комплексне вирішення проблеми безпеки інформації як складової національної безпеки держави в цілому ґрунтується на розробці загальної стратегії. Головною властивістю комп'ютерних вірусів є саморозмноження. Тому процедура, здійснення цієї функції посідає в алгоритмі вірусу центральне місце, усі інші функції (прояв, засоби маскування тощо) мають другорядне значення. Комп'ютерний вірус — це невелика програма, що написана програмістом відповідної кваліфікації, здатна до саморозмноження й виконання різних деструктивних дій.

Бурхливий розвиток сучасних інформаційних технологій, комп'ютерних систем та обчислювальної техніки поряд із безперечними перевагами та позитивними результатами діяльності у сфері обробки найрізноманітнішої інформації спричинив також появу небажаних

негативних і навіть шкідливих наслідків. Насамперед це стосується масовомого поширення та "проникнення" в інформаційні системи 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 руйнування даних. Користувачі часто мимоволі розповсюджують віруси щоденним переписуванням дискет із різних машин. На сьогодні найсприятливішим середовищем існування та розмноження вірусів є загальновідома і найпопулярніша мережа Інтернет.

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 принципів побудови та функціонування обчислювальних машин, організацію обчислювальних процесів на персональних комп'ютерах (ПК) та їх алгоритмізацію, програмне забезпечення ПК і комп'ютерних мереж, захист інформації, а також ефективне використання сучасних інформаційно-комунікаційних технологій у професійній діяльності.

До самостійної роботи належить також вивчення та освоєння методичних вказівок до лабораторних робіт і вивчення додаткової літератури, пов'язаної з виконанням цих робіт.

Значну частину самостійної роботи студентів складає вивчення нормативних документів сфери предметної області з організації робіт.

Лише постійне самостійне навчання дає можливість якомога ближче підійти до вершини знань певної галузі і, оволодіти сумою знань і вмінь, які б дали змогу заявити про себе як про професіонала. Студент, який хоче якомога краще оволодіти професією, має добре розуміти: на занятті викладач подає основи знань, навчає, як учити, виділяє ті ключові істини дисципліни, які пробуджують у молодої людини потяг до поглиблення й удосконалення всіх знань. Збагачення загальною сумою знань, накопичених людством, розширен-

ня загального світогляду, усвідомлення наявної перспективи щодо реалізації певних знань є основним мотивом до сумлінного ставлення до навчання. Самостійна навчальна діяльність студента буде лише тоді результативною, коли вона ґрунтуватиметься на внутрішній потребі. Виховання відповідної здатності у студента потребує чіткого узгодження процесу самоосвіти із цілями навчання та виховання.

Згідно з державними стандартами навчальний матеріал навчальної дисципліни, передбачений робочим навчальним планом для засвоєння студентом у процесі самостійної роботи, виноситься на підсумковий контроль поряд із навчальним матеріалом. Самостійна робота студента над засвоєнням навчального матеріалу з конкретної дисципліни може виконуватися у бібліотеці вищого навчального закладу, навчальних кабінетах, комп'ютерних класах (лабораторіях), а також у домашніх умовах. Самостійна робота студента повинна бути спланована, організаційно й методично спрямована як особиста творча праця без прямої 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. За необхідності ця робота проводиться за заздалегідь складеним графіком, що гарантує можливість індивідуального доступу студента до потрібних дидактичних засобів. Графік доводиться до відома студентів на початку поточного семестру. При організації самостійної роботи студентів із використанням складного обладнання чи устаткування, складних систем доступу до інформації (наприклад, комп'ютерних баз даних, систем автоматизованого проектування тощо) передбачається можливість отримання необхідної консультації або допомоги з боку фахівця.

Самостійна навчальна діяльність студента 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 Інтернет;

- вивчення навчального матеріалу за паперовими та електронними підручниками, навчальними посібниками, практикумами тощо;
- опрацювання матеріалу за першоджерелами, науковою й спеціальною літературою;
- підготовку доповідей, рефератів, написання курсових робіт; пошукову й науково-дослідну діяльність;
- самотестування.

Самостійна робота студента під час лекції. Лекційний матеріал призначений для студентів у найбільш раціональному напрямі щодо вивчення навчальної дисципліни й акцентуванні уваги на найбільш складних, вузлових питаннях навчальної дисципліни. Належне ведення конспекту під час лекції сприяє збереженню необхідної інформації та дає студенту 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 студентам прийомів роботи з користувальницьким інтерфейсом програми дає можливість 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 розкриті деякі питання практичного заняття, або вони винесені на самостійне опрацювання, студент повинен звернутися до рекомендованих підручників, навчальних посібників і відповідних методичних матеріалів. Підготовку для практичного заняття краще здійснювати з використанням ПЕОМ зі встановленим на ньому відповідним програмним забезпеченням.

Вивчення навчального матеріалу за підручниками, навчальними посібниками, методичними вказівками, опрацювання матеріалу за першоджерелами, науковою й спеціальною літературою. Працювати з підручниками, навчальними посібниками, методичними вказівками, практикумами, науковою й спеціальною літературою незалежно

від типу їх носія (паперового чи електронного) необхідно, таким чином, щоб отримати максимум теоретичних знань і навичок. Для визначення необхідності опрацювання цих джерел, студент має ознайомитись з їх змістом, і тільки після цього визначити послідовність його опрацювання й відібрати необхідний для вивчення матеріал із цього джерела (глави, розділи тощо). Під час роботи з інтерактивними електронними джерелами слід використовувати можливості навігації за документом, що надаються сучасними програмами, призначеними для читання електронних документів відповідних форматів (MS Word, Adobe Reader, Adobe Acrobat та ін.) і, особливо, переваги гіпертекстової технології подачі навчального матеріалу, а саме — за допомогою гіперпосилань знаходити відповіді на поставлені питання. При опрацюванні матеріалу необхідно з'ясувати суть питання, що вивчається, не уникаючи при цьому визначення суті незрозумілих чи незнайомих слів, термінів. Саме інтерактивні гіпертекстові електронні джерела (довідки у складі програмних продуктів, електронні посібники та словники) надають можливості конкретизувати терміни і визначення як найшвидше. 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) надають можливість створення електронного конспекту із примітками, виносками, коментарями та його роздруківки. Для самостійного поглибленого вивчення навчального матеріалу студенту слід звертатися до наукової та спеціальної літератури, яка може бути й не зазначеною в навчально-методичному комплексі. Використання самостійно отриманих відомостей як у навчанні, так і на практиці є, безперечно, цінним здобутком 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 належать до базової підготовки сучасної людини. З позицій випереджаючої освіти навчання тільки за конспектом лекцій і основною літературою, зазначеного в навчальній про-

грамі, є недостатнім. У більшості випадків належна підготовка вимагає вмінь швидко знаходити та опрацювати необхідний матеріал за першоджерелами, науковою й спеціальною літературою та коректно цитувати знайдене. Перелік такої літератури, як правило, наводиться в навчально-методичному комплексі навчальної дисципліни. Тому завдання студента зводиться до самостійного знаходження цих матеріалів шляхом пошуку в паперових або електронних фондах бібліотек, а також у різноманітних файлових архівах, базах даних та базах знань, доступ до яких здійснюється за допомогою відповідних сервісів Інтернет (в основному — Word Wide Web, FTP та UseNet newsgroups).

Для пошуку документа використовуються різні його ознаки. У першу чергу це — реквізити документа (УДК. Автор(и). Заголовок опису. Основний заголовок: відомості, щодо 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 по всьому світу. Відповідні довідники видаються багатьма мовами й постійно оновлюються. В Україні в 2006 р. Книжковою палатою України імені Івана Федорова видано "Універсальну десяткову класифікацію. Зміни та доповнення." Вип. 4" в паперовому варіанті. Довідкова база УДК постійно нарощується за рахунок електронних видань. Знання УДК дає змогу 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 бібліотеки й за назвою джерела або прізвищем та ініціалами автора знайти відповідний бібліотечний шифр джерела.

Якщо ж студент здійснює наукове дослідження вибраної проблеми, готує наукову доповідь або виступ на конференції і йому не відомі реквізити джерела або саме джерело, то слід зробити пошук у систематичному бібліотечному каталозі. Завдання студента полягає в пошуку необхідної галузі (підгалузі), що охоплює розшукувану інформацію, а потім у межах цієї галузі (підгалузі) — картки з необхідним джерелом і бібліотечним шифром. У подальшому студент повинен оформити бібліотечне замовлення на літературу встановленого зразка, до якого внести шифр знайденого джерела та всі необхідні реквізити. Робота з електронними фондами в цьому варіанті значно ефективніша, оскільки в розвинених бібліотеках облік літератури ве-

деться в середовищах систем управління базами даних, за допомогою яких пошук потрібної інформації здійснюється найефективніше.

Сервіси мережі Інтернет надають унікальні можливості знаходження літературних джерел у географічно віддалених фондах та архівах, а також шляхом участі в мережевих конференціях, де можна отримати відповіді та поради щодо питань із розшукуваної інформації. Для доступу до Інтернет-ресурсів необхідно знати їх мережеву адресу. Оскільки Інтернет постійно оновлюється і розвивається, у ньому немає єдиного каталога, змісту, або наочного покажчика ресурсів, існують різні інформаційно-пошукові системи, що допомагають користувачам знайти те, що їм потрібно. Це насамперед 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 Інтернет. Інформація в цих системах розподіляється за тематичними розділами відповідно до певної ієрархії. На верхньому рівні розділів зібрані загальні категорії (наприклад, "Інтернет", "Бізнес", "Мистецтво", "Освіта" тощо), а нижній рівень складають 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 увести ключове слово (поєднання слів), клацнути Пошук, і система повідомить, чи є відповідний розділ у її каталозі й запропонує в нього перейти, минувши всі проміжні розділи. Рекомендуємо використовувати каталоги: http://www.yahoo.com, http://www.portal.edu.ru, http://www.ipl.org

Пошукові системи є складними інформаційно-довідковими системами, що автоматично генеруються на основі даних, які збираються мережевими програмами-роботами по всій системі Інтернет, і надаються у відповідь на запит користувача посиланнями на різні Інтернет-ресурси. Запит здійснюється за певною процедурою (на певній мові), яка може відрізнятися в різних системах, проте у спрощеному вигляді вона зводиться до того, що користувач уводить в спеціальному полі (або в кількох полях) ключові слова, та/або словосполучення, які найточніше відображають суть проблеми.

Загальні положення мов запитів:

- ключові слова, які можна вводити у відповідне поле пошукової системи поодинці, послідовно звужуючи пошук, або ж уводити

одразу кілька слів, розділяючи їх пробілами або комами. Регістр не має значення;

- режим пошуку "AND" ("І") означає, що будуть знайдені тільки ті дані, де зустрічається кожне з ключових слів;
- при використанні режиму "OR" ("АБО") результатом пошуку будуть усі дані, де зустрічається хоч би одне ключове слово;
- використовуйте знаки "+" і "–" перед ключовим словом. Щоб виключити документи, 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 пропуску;
- 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" будуть знайдені 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, укладіть його в лапки;
- якщо Ви пишете все слово рядковими буквами, будуть знайдені всі варіанти його написання; якщо Ви вказали хоч би одну букву в шуканому слові 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 приніс результатів, можливо, при введенні Ви припустилися помилки;
- використовуйте синоніми. Якщо список знайдених сторінок дуже малий або не містить корисних сторінок, спробуйте зміни-

ти слово. Наприклад, замість "реферати", можливо, більше підійде "курсові роботи" або "твори";
- якщо один зі знайдених документів ближче до шуканої теми, ніж інші, клацніть Знайти схожі документи. Це посилання розташовано під короткими описами знайдених документів. Система проаналізує сторінку й знайде документи, схожі на ту, що Ви зазначили.

Подібних систем в Інтернет значно більше, ніж тематичних каталогів. Серед пошукових систем існують як обширні з тематики метапошукові системи, так і вузькоспеціалізовані. Найбільш відомі 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 Інтернет 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 й форми їх оцінювання:
- підготовка та власне аудиторна робота під час практичних і лабораторних занять. Результати оцінюються під час поточного контролю;
- виконання самостійних робіт у формі есе, рефератів з конкретної проблеми та складання письмових звітів на електронних або паперових носіях або усних доповідей;
- опрацювання програмного матеріалу змістового модуля;
- виконання письмової контрольної роботи або тестування;
- звіт про проходження практики;
- звіт про науково-дослідну роботу, результати якої можуть бути використані при написанні випускної роботи й за рішенням кафедри опубліковані.

Мета курсу

Мета дисципліни "Комп'ютерна вірусологія" — ознайомити студентів з основними поняттями про комп'ютерні віруси, історією

їх виникнення, основними принципами функціонування та поширення, класифікацією та надати необхідних знань і навичок щодо захисту інформаційних ресурсів від вірусів.

Результати навчання

У результаті вивчення дисципліни студенти повинні

знати:

- основні принципи й правила побудови, класифікацію, способи розповсюдження та структури комп'ютерних вірусів;
- 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 з захисту вказаних систем від вірусів;
- демонструвати розуміння сучасних проблем вірусології, володіти певними прийомами низькорівневого програмування для детальнішого засвоєння властивостей та 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-управляючі комплекси підприємств, фірм, методів їх роботи й взаємодії з обчислюваль-

ним середовищем; використанням системи інструментів для боротьби з ними; створенням систем захисту від вірусних атак.

ЗМІСТ САМОСТІЙНОЇ РОБОТИ
з дисципліни
“КОМП’ЮТЕРНА ВІРУСОЛОГІЯ”

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

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

Теми рефератів за модулем І

1. Історія, сучасна ситуація та перспективи в області вірусології.
   Література [1–4; 7; 9; 10; 14; 18]
2. Класифікаційний код вірусу. Дескриптор вірусу. Сигнатура вірусу.
   Література [1–4; 7; 9; 10; 14; 18]
3. Файлові віруси. Бутові віруси.
   Література [1–4; 7; 9; 10; 14; 18]
4. Мережеві віруси.
   Література [1–4; 7; 9; 10; 14; 18]
5. Структура (“анатомія”) комп’ютерного вірусу.
6. Принципи та алгоритми роботи Word/Excel/Access-макровірусів.
   Література [1–4; 7; 9; 10; 14; 18]

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 присутності 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. Мережеві 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 зараженні 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:

а) самовідтворюються;
б) самопошкоджуються;
в) переносяться.

2. Концепція створення програм, що самовідтворюються виникла:

а) у 60-ті роки;
б) 50-ті роки;
в) 40-ві роки;

3. Перший етап, розробки вірусоподібних програм носив:

а) характер протистояння користувачів безвідповідальним або навіть кримінальним "елементам";
б) дослідницький характер.

4. Другий етап, розробки вірусоподібних програм носив:

а) характер протистояння користувачів безвідповідальним або навіть кримінальним “елементам”;
б) дослідницький характер.

5. Зазначте, чи можливо вказати точну кількість вірусоподібних програм:

а) так;
б) ні.

6. Віруси можна розділити на класи за такими основними ознаками:

а) місцем існування;
б) операційною системою (ОС);
в) величиною;
г) особливостями алгоритму роботи;
д) деструктивними можливостями.

7. За місцем існування віруси можна розділити на:

а) дискові;
б) файлові;
в) завантажувальні;
г) макро;
д) мережеві;
е) флешкові.

8. Файлові віруси:

а) різними способами упроваджуються у виконавчі файли (найбільш поширений тип вірусів), або створюють файли-двійники (віруси компаньйона), або використовують особливості організації файлової системи (link-віруси);
б) 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;
в) заражають файли-документи й електронні таблиці кількох популярних редакторів;
г) використовують для свого розповсюдження протоколи або команди комп’ютерних мереж і електронної пошти.

9. Макро-віруси:

а) різними способами упроваджуються у виконавчі файли (найбільш поширений тип вірусів), або створюють файли-двійники (віруси компаньйона), або використовують особливості організації файлової системи (link-віруси);

б) 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;

в) заражають файли-документи й електронні таблиці кількох популярних редакторів;

г) використовують для свого розповсюдження протоколи або команди комп'ютерних мереж і електронної пошти.

10. Серед особливостей алгоритму роботи вірусів виділяються такі:

а) резидентність;

б) паразитність;

в) використання стелс-алгоритмів;

г) самошифрування й поліморфізм;

д) використання нестандартних прийомів.

11. Резидентний вірус при інфікуванні комп'ютера:

а) не заражає пам'ять комп'ютера й зберігає активність обмежений час;

б) залишає в оперативній пам'яті свою резидентну частину.

12. Макровіруси — це:

а) резидентний вірус;

б) нерезидентний вірус.

13. Вірус "Frodo" — це:

а) завантажувальний вірус;

б) стелс-вірус.

14. За деструктивними можливостями віруси можна розділити на такі :

а) нешкідливі;

б) безпечні;

в) небезпечні віруси;

г) дуже небезпечні віруси.

15. Зазначте кількість етапів, які розрізняють у циклі функціонування вірусів:

а) 6;
б) 10;
в) 3.

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

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

17. KakWorm, Stages і ILOVEYOU — це:

а) завантажувальні віруси;
б) макро-віруси;
в) поштові віруси-хропаки.

18. Сигнатура вірусів — це:

а) семафор вірусу;
б) біти, які не належать до основного "тіла" вірусу;
в) унікальний програмний код вірусу.

19. За місцезнаходженням віруси поділяються:

а) на файлові;
б) бутові;
в) файлово-бутові;
г) пакетні;
д) мережеві;
е) WinWord-віруси;
є) Windows-віруси;
ж) OS/2-віруси;
з) Novell NetWare-віруси;
і) BIOS- віруси;
ї) CD-ROM-віруси.

20. За наслідками деструктивних дій віруси поділяються:

а) не нешкідливі;
б) не уразливі;
в) уразливі;
г) дуже уразливі.

21. За особливостями алгоритму віруси вони поділяються на:

а) stealth-віруси;
б) worm-віруси;
в) companion-віруси;
г) MtE-віруси;
д) DIR-віруси;
е) driver-віруси;
є) віруси-паразити;
ж) віруси-привиди;
з) "троянські" програми;
і) Логічні бомби;
ї) комбіновані віруси та ін.

22. За способом створення вірусів вони поділяються:

а) на створені ручними засобами розробки (Н-віруси);
б) створені автоматизованими засобами розробки (А-віруси).

23. Код вірусу може бути скопійований:

а) у таблицю налагодження адрес (для EXE-файлів);
б) в область стека;
в) поверх коду або даних програми (при цьому программа безповоротно пошкоджується).

24. Завантажувально-файлові віруси — це віруси, які:

а) спроможні вражати, як код завантажувальних секторів, так і код файла;
б) фальсифікують інформацію, читаючи з диска так, що активна програма отримує невірні дані;
в) заражають антивірусні програми, знищують їх або роблять їх непрацездатними;
г) вражають одночасно EXE, COM, boot-сектор, MBR, FAT і директорії.

25. STEALTH-віруси — це віруси, які:

а) спроможні вражати, як код завантажувальних секторів, так і код файла;
б) фальсифікують інформацію, читаючи з диску так, що активна програма отримує невірні дані;

в) заражають антивірусні програми, знищують їх або роблять їх непрацездатними;
г) вражають одночасно EXE, COM, boot-сектор, MBR, FAT і директорії.

26. Multipartition — це віруси:

а) які спроможні вражати, як код завантажувальних секторів, так і код файла;
б) які фальсифікують інформацію, читаючи з диску так, що активна програма отримує невірні дані;
в) які заражають антивірусні програми, знищують їх або роблять їх непрацездатними;
г) які вражають одночасно EXE, COM, boot-сектор, MBR, FAT і директорії.

27. Ознаками зараження вірусом є:

а) збільшення розміру пам'яті;
б) уповільнення роботи комп'ютера;
в) затримки при виконанні програм;
г) незрозумілі зміни у файлах;
д) зміна дати модифікації файлів без причини;
е) незрозумілі помилки Write-protection;
є) помилки при інсталяції й запуску WINDOWS;
ж) відключення 32-розрядного допуску до диска;
з) неспроможність зберігати документи Word в інші каталоги, крім TEMPLATE;
і) некоректна робота дисків.

28. При переході вірусу в активну фазу, легко помітити такі зміни:

а) зникнення файлів;
б) форматування HDD;
в) неспроможність завантажити комп'ютер;
г) неспроможність завантажити файли;
д) незрозумілі системні повідомлення, музикальні ефекти тощо.

29. Основними джерелами вірусів є:

а) дискета, флешка, CD-ROM на яких знаходяться заражені вірусом файли;
б) комп'ютерна мережа, у тому числі система електронної пошти та Інтернет;

в) жорсткий диск, на який потрапив вірус у результаті роботи із зараженими програмами;
г) вірус, що залишився в оперативній пам'яті після попереднього користувача;
д) віруси можуть записувати своє тіло;
е) у кінець файла-жертви;
є) у середину;
і) окремими "плямами".

30. Специфічними функціями для вірусу черв'як є:

а) знаходити нові цілі для атаки;
б) проникати в них;
в) передавати свій код на видалену машину;
г) запускати її (отримувати управління);
д) перевіряти на зараженість локальну або видалену машину для запобігання повторному зараженню.

31. Зазначте, які типи файлів комп'ютерний вірус не тільки псує, але й заражає:

а) графічні файли;
б) програмні файли;
в) інформаційні файли без даних;
г) медіа-файли.

32. Зазначте, які різновиди вірусів перехоплюють звернення операційної системи до уражених файлів:

а) троянські віруси;
б) паразитичні віруси;
в) віруси черв'яки;
г) віруси невидимки (стелс-вируси).

33. Найнебезпечнішими вірусами, що руйнують завантажувальний сектор, є:

а) троянські віруси;
б) паразитичні віруси;
в) віруси черв'яки;
г) віруси-невидимки (стелс-вируси).

34. Резидентними вірусами є:

а) активні до виключення комп'ютера;

б) активні якийсь обмежений час;
в) активізуються після натиснення на визначену комбінацію клавіш.

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

Теми рефератів за модулем ІІ

1. Створення простих типів вірусів.
Література [1–7]
2. Створення мережевих 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; 8–19]
6. Налаштування пакета та робота в антивірусній програмі AVP (AntiViral Toolkit Pro).
Література [1–4; 8–19]

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 й погрози безпеки.

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:

а) з сигнатуру;
б) даних;
в) таблиці для налагодження адрес.

2. Дізасемблер запускається командою:

а) sr test-com;
б) call sub_1;
в) sub_1: pop si;
г) sub si,3.

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

а) mov AH, 3dh;
б) mov AL, 0;
в) mov Dx, offset frame;
г) int 21h;
д) jnc ok.

4. Спробою відкрити файл є:

а) mov ah,0;
б) int 21h;
в) mov day, dl;
г) mov month, dh;
д) add cx,1980;
е) mov year, cx.

5. Використання вільного вектора переривань користувача:

а) mov ah,0;
б) intlah;
в) mov oldcount, dx;
г) mov ah,0;
д) movbx, oldcount;
е) cmp bx, dx;
є) jc adjust;
ж) sub dx, bx;
з) jmp short;
і) adjust:;
к) mov cx,0fiffh;
л) sub cx, bx;
м)add cx, dx;
н) mov dx, cx.

6. Призначення й характеристика індексних регістрів. Команди двійкової арифметики (команди множення й ділення):

а) mov AH, 4ch;
б) mov AL, errcode;
в) int 21h.

7. Для визначиння сегментної адреси вільної ділянки пам'яті, розмір якої достатній для розміщення EXE-програми:

а) створюється й заповнюється блок пам'яті для змінних середовища;
б) створюється блок пам'яті для PSP і програм (сегмент ЮОООЬ
в) PSP сегмент+ООЮЬЮОООЬ — програма.

8. Програма захисту від вірусів BIOS записана у файлі:

а) Setup;
б) Bat;
в) int 13h.

9. Евристична маска — це:

а) набір дій, виявлених при перевірці файла;
б) порядковий номер першої з евристичних масок, що співпали;

10. Евристичне число — це:

а) набір дій, виявлених при перевірці файла;
б) порядковий номер першої з евристичних масок, що співпали.

11. Правила профілактики від зараження вірусами:

а) необхідно регулярно робити резервні копії файлів, з якими ведеться робота;
б) слід купувати дистрибутивні копії програмного забезпечення тільки в офіційних продавців;
в) не слід запускати неперевірені антивірусні програми, отримані із сумнівних джерел;
г) при лікуванні дисків слід використовувати свідомо "чисту" операційну систему.

12. Зазначте, основні типи антивірусних програм:

а) сканери;
б) перфоратори;
в) монітори;
г) ревізори змін;
д) суперматори;
е) імунізатори;
є) поведінкові, які блокують.

13. Сканери — це антивірусні програми, які:

а) шукають у файлах, пам'яті, завантажувальних секторах сигнатур вірусів;
б) знімають оригінальні контрольні суми з можливих об'єктів зараження;
в) перехоплюють різні події й у разі підозрілих дій.

14. Поведінкові, які блокують , — це антивірусні програми, що:

а) шукають у файлах, пам'яті, завантажувальних секторах сигнатур вірусів;
б) знімають оригінальні контрольні суми з можливих об'єктів зараження;
в) перехоплюють різні події й у разі підозрілих дій.

15. Ревізори змін — це антивірусні програми, які:

а) шукають у файлах, пам'яті, завантажувальних секторах сигнатур вірусів;
б) знімають оригінальні контрольні суми з можливих об'єктів зараження;
в) перехоплюють різні події й у разі підозрілих дій.

16. Зазначте характерні ознаки вияву наявності вірусу в роботі на ПК:

а) деякі програми припиняють працювати або починають працювати неправильно;
б) на екран виводяться сторонні повідомлення, символи й т. д.;
в) робота на комп'ютері істотно сповільнюється;
г) деякі файли виявляються зіпсованими й т. д.

17. Методами захисту інформації є:

а) програмні;
б) віртуальні;
в) апаратні;
г) програмно-апаратні;
д) демократичні;
е) фізичні;
є) правові;
ж) централізовані;
з) організаційні.

18. Детектори (сканери) призначені:

а) для постановки діагнозу, лікуванням буде займатися інша антивірусна програма або професійний програміст-"вірусолог";
б) для пошуку й видалення вірусів (фаги) або кількох вірусів (поліфаги);
в) для контролю всіх (відомих на момент випуску програми) можливих способів зараження комп'ютерів, контролю всіх операцій які постійно знаходяться в пам'яті комп'ютера;
г) для обробки файлів і завантажувальних секторів з метою попередження зараження відомими вірусами.

19. Охоронці призначені:

а) для постановки діагнозу, лікуванням буде займатися інша антивірусна програма або професійний програміст-"вірусолог";
б) для пошуку й видалення вірусів (фаги) або кількох вірусів (поліфаги);
в) для контролю всіх (відомих на момент випуску програми) можливих способів зараження комп'ютерів, контролю всіх операцій які постійно знаходяться в пам'яті комп'ютера;
г) для обробки файлів і завантажувальних секторів з метою попередження зараження відомими вірусами.

20. Фаги (поліфаги) призначені:

а) для постановки діагнозу, лікуванням буде займатися інша антивірусна програма або професійний програміст-“вірусолог”;
б) для пошуку й видалення вірусів (фаги) або кількох вірусів (поліфаги);
в) для контролю всіх (відомих на момент випуску програми) можливих способів зараження комп’ютерів, контролю всіх операцій які постійно знаходяться в пам’яті комп’ютера;
г) для обробки файлів і завантажувальних секторів з метою попередження зараження відомими вірусами.

21. Ревізори призначені:

а) для постановки діагнозу, лікуванням буде займатися інша антивірусна програма або професійний програміст-“вірусолог”;
б) для пошуку й видалення вірусів (фаги) або кількох вірусів (поліфаги);
в) для контролю всіх (відомих на момент випуску програми) можливих способів зараження комп’ютерів, контролю всіх операцій які постійно знаходяться в пам’яті комп’ютера;
г) для обробки файлів і завантажувальних секторів з метою попередження зараження відомими вірусами.

22. Вакцини призначені:

а) для постановки діагнозу, лікуванням буде займатися інша антивірусна програма або професійний програміст-“вірусолог”;
б) для пошуку й видалення вірусів (фаги) або кількох вірусів (поліфаги);
в) для контролю всіх (відомих на момент випуску програми) можливих способів зараження комп’ютерів, контролю всіх операцій які постійно знаходяться в пам’яті комп’ютера;
г) для обробки файлів і завантажувальних секторів з метою попередження зараження відомими вірусами.

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

а) резервне копіювання інформації (створення копій файлів і системних областей жорстких дисків);
б) уникнення користування випадковими й невідомими програмами. Найчастіше віруси розповсюджуються разом із комп’ютерними вірусами;

в) перезавантаження комп'ютера перед початком роботи, зокрема, у випадку, якщо за цим комп'ютером працювали інші користувачі;
г) обмеження доступу до інформації, зокрема, фізичний захист дискети під час копіювання файлів з неї.

24. Розрізняють такі типи антивірусних програм:

а) програми-детектори: призначені для знаходження заражених файлів одним із відомих вірусів;
б) програми-лікарі: призначені для лікування заражених дисків і програм;
в) програми-ревізори: призначені для виявлення зараження вірусом файлів, а також пошуку ушкоджених файлів;
г) лікарі-ревізори: призначені для виявлення змін у файлах і системних областях дисків й у разі змін повертають їх у початковий стан;
д) програми-фільтри: призначені для перехоплення звернень до операційної системи, що використовуються вірусами для розмноження й повідомляють про це користувача;
е) програми-вакцини: використовуються для обробки файлів і boot-секторів з метою попередження зараження.

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

а) віймейкарами;
б) позитронами;
в) хакерами;
г) крекерами.

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

а) якість евристичного аналізу;
б) швидкість реакції при виявленні вірусів;
в) якість сигнатурного аналізу:
г) якість поведінкового блокиратора:
д) здібність до лікування активних заражень:
е) якість самозахисту:
є) можливість підтримки упаковщиків:
ж) частота помилкових спрацьовувань.

27. Зазначте типи антивірусних програм, які здатні виявляти й лікувати заражені файли:

а) вартуючі;
б) детектори;
в) ревізори;
г) доктори.

28. Зазначте тип антивірусних програм, які здатні ідентифікувати тільки відомі їм віруси й вимагають оновлення антивірусної бази:

а) вартуючі;
б) детектори;
в) ревізори;
г) доктори.

29. Зазначте тип антивірусних програм, які подають сигнал тривоги, але лікувати не здібні:

а) вартуючі;
б) детектори;
в) ревізори;
г) доктори.

30. Антивірусна програма Dr. Web — це:

а) програма-сторож;
б) програма-детектор;
в) програма-ревізор;
г) програма-доктор.

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

а) запустили заражений виконуваний файл;
б) вставили в дисковод заражену дискету;
в) встановили заражений драйвер;
г) відкрили для редагування заражений документ MS Word/.

МЕТОДИЧНІ ВКАЗІВКИ ДО ПІДГОТОВКИ, НАПИСАННЯ ТА ЗАХИСТУ КОНТРОЛЬНОЇ РОБОТИ (РЕФЕРАТУ)

Реферат є складовою вивчення дисципліни.

Завдання підготовлені відповідно до курсу "Комп'ютерна вірусологія" для бакалаврів.

Мета написання реферату — допомогти студентам засвоїти теоретичні знання, розвинути й удосконалити навички захисту інформації, використання сучасних нових інформаційних технологій захисту від вірусних атак (пакетів прикладних програм) і засобів обчислювальної техніки. Оформлення й захист рефератів повинні сприяти активному засвоєнню нового матеріалу, виробленню у студентів уміння комплексного використання суміжних дисциплін при вирішенні практичних питань.

Орієнтовна структура і обсяги реферату наведені у таблиці.

План (розділи)	Обсяг у сторінках (приблизно)	Короткий зміст (що потрібно висвітлити)
Вступ	До однієї	Мета, загальна характеристика, визначення номера варіанта завдання
Назва кожного питання відповідно до реферату	1–2, загальний обсяг роботи в межах 20–30	Викладення суті питання з наведенням прикладів та посилань 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, надрукованого через 2 інтервали, рукописне викладення тексту не повинно перевищувати 18–24 сторінок шкільного зошита.

Виконання та оформлення реферату

Під час написання реферату студент має розкрити історичні посилки цієї проблеми, відповідаючи на всі питання як теоретичного плану, так і описати технологію розв'язання практичної задачі, якщо такі передбачені рефератом.

Відповіді на теоретичні питання потребують ретельної роботи з літературою. Крім виписок і конспектування з літературних джерел, наприклад з Інтернет, студент повинен зробити висновки. Робота виконується самостійно. У тексті реферату потрібно давати посилання на використану літературу. У висновках у цілому з реферату розглядають питання економічної доцільності й практичного застосування сучасних інформаційних технологій та обчислювальної техніки у сфері захисту.

Реферат слід оформляти на стандартних аркушах паперу, зброшурованих у папку. Усі аркуші мають бути пронумеровані. На титульній сторінці необхідно вказати назву вищого навчального закладу, факультет, спеціальність, дисципліну, курс, групу, а також прізвище, ініціали та номер залікової книжки.

На першій сторінці мають бути представлені розрахунок варіанта контрольної роботи та питання варіанта й проставлені номери сторінок, на яких викладено цей матеріал. На останній сторінці студент підписує роботу й ставить дату. У кінці роботи необхідно подати використану літературу. Зшита папка має бути вкладена в поліетиленовий файл та містити дискету з повним текстом, графікою тощо набраного варіанта реферату.

Вибір варіанта реферату

Кожний студент отримує окреме завдання для виконання КР згідно з варіантом *Z*, який обчислюється за формулою:

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

де *NZK* — номер залікової книжки (студентського квитка) студента;

PR — поточний рік отримання завдання.

Наприклад, $NZK = 398$, $PR = 2001$, тоді

$$Z = mod_{6}(398 + 2008 - 2000) + 1 = mod_{6}(406) + 1 = 4 + 1 = 5.$$

Отже, тут $Z = 5$.

Зауваження. 1. Обчислення варіанта має бути у вступі до контрольної роботи.

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

Увага!

Неправильно оформлена робота повертається без перевірки на дооформлення. Робота, виконана не за своїм варіантом, підлягає переробці.

ІНДИВІДУАЛЬНО-КОНСУЛЬТАЦІЙНА РОБОТА

Індивідуально-консультативна робота з дисципліни здійснюється у формі консультацій за графіком (одна консультація на два тижні). На консультаціях студентам надаються пояснення з виконання само-

стійної роботи, підготовки до практичних занять, перевірка та захист завдань, винесених на поточний контроль тощо.

Глосарій

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

***Alias (Альтернативне/додаткове ім'я)*:** Хоча кожен вірус має спеціальне ім'я, дуже часто він відоміший під своїм псевдонімом, що описує відмінну рису або характеристику цього вірусу. У таких випадках ми говоримо про вірусний 'alias'. Наприклад, вірус CIH також відомий під псевдонімом Chernobyl.

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

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

***Armouring (Бронювання)*:** Цей метод використовується вірусами для того, щоб приховати свою присутність і запобігти виявленню антивірусом.

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

***Backup (Резервне копіювання, резервна копія)*:** Резервна копія це копія окремих файлів, груп файлів або всього диска, збережені на окремому носієві

Boot virus (Завантажувальний вірус): Вірус, який 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 за певними типовими характеристиками.

Cavity (Вільні осередки): Метод, використовуваний певними вірусами й черв'яками для створення утруднень у їх виявленні. При його застосуванні розмір файла не змінюється (вони заповнюють тільки вільні осередки в зараженому файлі).

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

Companion / Companion virus / Spawning, Компаньон/вірус-компаньон: Тип вирусів, які не вставляють себе у програмі, а приєднуються до них.

CVP — Content Vectoring Protocol (протокол перенаправлення контента): Протокол, розроблений в 1996 р. Check Point Software, який дає можливість антивірусному захисту бути інтегрованим у сервер брандмауера (файервола).

Damage level (Рівень пошкодження): Значення, яке показує рівень негативної дії вірусу на заражений комп'ютер. Один із чинників, який використовувується 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): Значення, яке показує, як швидко і як далеко розповсюджується вірус. Один із чинників визначення рівня погроз.

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

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

Encryption / Self-encryption, Шифрування/Самошифрування: Техніка, використовувана деякими вірусами для того, щоб приховати свою присутність і уникнути виявлення антивірусними програмами.

EPO (Entry Point Obscuring), Утаювання точки входу: Технологія зараження програм, коли вірус намагається приховати свою точку входу, для того, щоб не виявити свою присутність. Замість того, щоб узяти контроль і починати виконувати свої дії, як тільки використовується або запускається заражена програма, вірус дає можливість безпомилково працювати, перш ніж відбудеться його активація.

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

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

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

Hoax (Розиграш): Це не вірус, а помилкове повідомлення про вірус, якого немає.

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

In The Wild (У дії): Офіційний список вірусів, що випускається кожного місяця, й повідомлення про їх дії.

Infection (Зараження): Це належить до процесу впровадження вірусу в комп'ютер або в його певні області або файли.

Link virus (Віруси-посилання): Тип вірусу, який змінює адресу, де зберігається файл, замінюючи його адресою вірусу. У результаті, при запуску/відкритті файла активується вірус. Після зараження комп'ютера початковий файл стає непридатним для використання.

Macro (Макрос): Ряд інструкцій, визначених так, щоб програма, скажімо Word, Excel, PowerPoint, або Access, виконувала позначені операції. Оскільки макроси є програмами, то вони 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 використовується відносно до всіх програм, які містять шкідливий код (MALicious softWARE), будь це вірус, троян або черв'як.

Multipartite (Складений): Характеристика особливого типу складного вірусу, який заражає комп'ютери, використовують комбінацію технологій, уживаних також іншими вірусами.

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

Permanent protection (Постійний захист): Процес, який виконують деякі антивірусні програми, проводячи безперервне сканування файлів, використовуваних в інших операціях (навіть якщо це користувач або ОС.) Також відомі як охоронні або резидентні.

Polymorphic / Polymorphism, Поліморфний/поліморфізм: Техніка, використовувана вірусами для зашифровуваної своєї сигнатури кожного разу по-новому, або навіть інструкції для виконання шифрування.

Prepending (Приєднання спереду): Техніка, використовувана вірусами для зараження файлів шляхом приєднання своїх кодів на початок файла. Таким чином, віруси забезпечують свою активацію при першому використанні зараженого файла.

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

Resident / Resident virus, Резидент/резидентний вірус: Програми, які належать до резидентних, тобто зберігаються в пам'яті комп'ютера, і які постійно відстежують операції, що виконуються на комп'ютері.

Signature / Identifier, Сигнатура/Ідентифікатор: Це подібно до номера паспорта вірусу. Послідовність знаків (числа, букви і т. д.), які визначають вірус.

Stealth (Прийом): Техніка, використовувана деякими вірусами для зараження комп'ютерів, залишаючись непоміченими для користувачів або антивірусних програм.

Tunneling (Тунелірування): Технологія, використовувана деякими вірусами для руйнування антивірусного захисту.

Vacination (Вакцинація): Технологія антивіруса, яка дає змогу зберегтися інформації файла, а можливі зараження виявити, якщо деякі зміни в ньому будуть відмічені.

Variant (Варіант): Це модифікована версія початкового вірусу, який може відрізнятися від останнього способами зараження й справленими враженнями.

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

Virus constructor (Конструктор вірусів): Шкідлива програма, призначена для створення нових вірусів без наявності навичок програмування, оскільки має інтерфейс, який дає можливість вибрати характеристики створюваного шкідливого ПО: тип, зброя, файли поразки, шифрування, поліморфізм і тому подібне.

Virus Signature File (Вірусний файл сигнатури): Файл, який дає можливість 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, використовувана багатьма вірусами для зашифровування свого контента.

Антивірус (anti-virus): Клас програмного забезпечення, яке призначене для запобігання інфікуванню системи вірусами.

Антивірусний захист (в області захисту інформації): Комплекс організаційних, правових, технічних і технологічних заходів, вживаних для забезпечення захисту засобів обчислювальної техніки й автоматизованих систем від дії програм-вірусів.

Безпека інформації: Стан інформації, інформаційних ресурсів і інформаційних систем, при якому з необхідною вірогідністю забезпечується збереження даних від витоку, розкрадання, втрати, несанкціонованого знищення, спотворення, модифікації (підробки), копіювання, блокування й т. п.

***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 компіляції, вірус може бути видалений.

Віруси-компаньйони. По своїй дії схожі з тими, що перезаписують, за виключенням того, що цільовий файл не знищується, а переміщується в інше місце, таким чином, при запуску файла, інфікованого таким вірусом, виконується спочатку код вірусу і уже потім — код самого файла.

Віруси-ланки: Змінює адресу місцеположення зараженого файла на свій, таким чином, 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 і інших дій, про спроби порушення, або факти порушення захисту як легальні, так і несанкціоновані.

Завантажувальні віруси: Віруси, які вражають сектор початкового завантажувача дискети BR або сектор головного завантажувача вінчестера MBR.

Збір інформації: Діяльність суб'єкта, у ході якої він отримує відомості про об'єкт, що цікавить його.

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

Неможливість переходу в небезпечний стан: Принцип неможливості переходу в небезпечний стан означає, що за будь-яких обставин, зокрема, нештатних, захисний засіб або повністю виконує свої функції, або повністю блокує доступ.

Ознака проникнення: Опис ситуації або умови, за яких може відбутися проникнення; опис системних подій, що означають акт проникнення.

Пакет "Чорнобиль": Також називається пакетом "Камікадзе". Мережевий пакет, що викликає передачу незліченної кількості пакетів даних і перевантаження мережі.

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

Перезаписуючі віруси: Записують своє тіло замість коду програми, не змінюючи при цьому назви початкового файла. Унаслідок цих дій, при запуску зараженого файла виконується код вірусу, а не сама програма.

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

Резидентна програма: Програма, яка після завантаження в ОЗУ й передачі їй управління ініціалізувалася, так, що постійно знаходиться в ОЗУ й виконується паралельно з іншими програмами.

Реплікатор: Будь-яка програма, що створює копії самої себе. Прикладами є черв'яки, логічні бомби й віруси.

Ретро-вірус: Вірус, який очікує зараження всіх можливих резервних носіїв, щоб виключити повернення системи в неінфікований стан.

Різноманітність захисних засобів: Принцип різноманітності захисних засобів рекомендує організовувати різні за своїм характером оборонні рубежі.

"Троянський кінь". На вигляд корисна й нешкідлива програма, що містить додатковий прихований код, який 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 виду "game.exe", "instal.exe" сподіваючись на те, що користувач сплутає такий файл з чим-небудь іншим і за необережності запустить.

Шкідливий код: Устаткування, програмне забезпечення або програмно-апаратні засоби, умисне включені в систему в цілях здійснення несанкціонованих дій (наприклад, "троянський кінь").

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. *Косарев В. П.* Компьютерные сети и системы. — М., 2000.
7. *Журнал* "Хакер". — № 32, 35. — 2001.
8. *Домарев В. В.* Безопасность информационных технологий. — СПб., 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: В 3 ч. — 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 Санкт-Петербург, 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 / За ред. Ю. С. Ковтанюка. — К.: ЮНИОР, 2003. — 501 с.
19. *Олецький О. В.* Принципи роботи комп'ютерних систем: Навч. посіб. — К.: Вид. дім "КМ Академія", 2003. — 144 с.

ЗМІСТ

Відповідальний за випуск *А. Д. Вегеренко*
Редактор *А. А. Тютюнник*
Комп'ютерне верстання *С. А. Шередега*

Зам. № ВКЦ-4944

Формат 60 $84/_{16}$. Папір офсетний.
Друк ротаційний трафаретний. Ум. друк. арк. 2,38. Обл.-вид. арк. 1,8
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 р.