ЗАТВЕРДЖУЮ

Завідувач кафедрою
інформатики та кінезіології
Назва кафедри

професор Заневський І.П.
Підпис, ініціали, прізвище

ЛАБОРАТОРНЕ ЗАНЯТТЯ № 9
З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«КОМП'ЮТЕРНІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ»

найменування навчальної дисципліни

Тема: **Сервісні програми. Захист інформації. Антивірусні програми. Архівація.**

(повне найменування теми)

Навчальний потік 5-й курс факультету здоров'я людини (магістр)
курс, спеціальності, спеціалізація підготовки

Навчально-матеріальне забезпечення

персональні комп'ютери, мультимедійний проектор,
програмне забезпечення Windows 8, Microsoft Office
(лабораторні макети та контрольно-вимірювальні прилади, електрона обчислювальна техніка, технічні засоби навчання і контролю знань, та інші навчальні матеріали)

Методичну розробку для проведення лабораторного заняття
Розробила к.п.н., доц. _____О.С. Ільків
(посада, вчений ступінь, вчене звання, підпис, ПІБ)

Методична розробка обговорена та схвалена на засіданні кафедри
економіки, інформатики та кінезіології

Протокол № ___ від _____20 р.

Мета: навчитися працювати з сервісними програмами

ПЛАН

1. Основні положення.

2. Захист інформації від пошкоджень.

2.1. Антивірусні програми.

2.2. Резервування інформації. Архіватор WinZip

2.3. Технічні заходи.

2.4. Адміністративні заходи.

3. Запитання. Завдання.

1. Основні положення

Проблема безпеки інформації в період загальної інформатизації, широкого впровадження електронних технологій є однією з найактуальніших у суспільстві. Комплексне вирішення проблем безпеки інформації як складової частини національної безпеки держави в цілому ґрунтується на розробленні загальної стратегії. Необхідно створити єдину правову, організаційну та матеріально-технічну базу з урахуванням міжнародних норм і правил безпеки інформації, а також оптимізувати чинні в країні нормативні, організаційні та регламентуючі документи.

Серед способів захисту інформації виокремлюють способи її захисту від пошкоджень і способи захисту від несанкціонованого доступу.

2. Захист інформації від пошкоджень

Захистити інформацію від пошкоджень можна за допомогою антивірусних програм, резервування інформації, технічних і адміністративних заходів.

Антивірусні програми. Ці програми призначені для захисту від спеціально створених програм пошкодження інформації — вірусів, які класифікують за такими характеристиками.

1. Середовище перебування. Виокремлюють:
   - *файлові* — ті, що додаються до файлів з розширенням exe, com;
   - *завантажувальні* — ті, які додаються до Ьoot-сектора;
   - *мережні* — ті, що поширюються по комп'ютерній мережі;
   - *макровіруси* — ті, які заражають файли Microsoft Office. Вони пошкоджують копію шаблону Normal.dot який завантажується в оперативну пам'ять комп'ютера під час роботи, внаслідок чого всі файли, з якими проводиться робота, стають ураженими.
2. Способи зараження комп'ютера. У цій групі існують такі віруси:
   - *резидентні* — ті, що вміщуються в оперативну пам'ять і додаються до всіх об'єктів (файлів, дисків), до яких звертається ОС;
   - *нерезидентні* — ті, що додаються до оперативної пам'яті і є активними лише короткий час.
3. Функціональні можливості. Виділяють такі гру пи вірусів:
   - *нешкідливі* — ті, що не впливають на роботу комп'ютера (наприклад, збільшують розмір файла);
   - *безпечні* — ті, що заважають роботі, але не пошкоджують інформацію (наприклад, дають якісь повідомлення, перезавантажують комп'ютер тощо);
   - *небезпечні* — ті, що пошкоджують інформацію файлів, зумовлюючи «зависання» комп'ютера;

- *дуже небезпечні* — ті, що зумовлюють утрату програм, знищення інформації із системних областей, форматування жорсткого диска.

4. Особливості алгоритму. За цією ознакою віруси поділяють на такі групи:
   - *віруси-супутники* — віруси, які не змінюють файлів, але створюють однойменні файли з розширенням сот, що завантажуються першими;
   - *віруси-черв'яки* — віруси, що поширюються автоматично в комп'ютерній мережі за знайденою адресою в адресній книзі;
   - *віруси-паразити* — віруси, які розпізнаються за зміненим змістом дискових секторів і файлів;
   - *Stealth-віруси* — ті, що фальсифікують інформацію, яка читається з диска. Вірус перехоплює вектор переривання int13h і видає активній програмі хибну інформацію, яка показує, що на диску все гаразд. Цей принцип використовується як у файлових, так і в завантажувальних вірусах;
   - *віруси-мутанти* — віруси, що мають зашифрований програмний код;
   - *ретровіруси* — звичайні файлові віруси, які намагаються заразити антивірусні програми, щоб знищити їх або зробити недієздатними.

Антивірусні програми, що дають змогу виявити вірус, відкоригувати або вилучити пошкоджені файли, поділяють на детектори, фаги (лікарі), ревізори, сторожі, вакцини.

Детектори (сканери) перевіряють оперативну або зовнішню пам'ять на наявність вірусу за допомогою розрахованої контрольної суми або сигнатури (частина коду, що повторюється) і складають список ушкоджених програм. Якщо детектор — резидентний, то програма перевіряється, і тільки в разі відсутності вірусів вона активізується. Детектором є, наприклад, програма MS AntiVirus.

Фаги (поліфаги) виявляють і знешкоджують вірус (фаг) або кілька вірусів. Сучасні версії поліфагів, як правило, можуть здійснювати евристичний аналіз файла, досліджуючи його на наявність коду, характерного для вірусу (додавання частини цієї програми в іншу, шифрування коду тощо). Фагами є, наприклад, програми Aidstest, DrWeb.

Ревізори — програми, що контролюють можливі засоби зараження комп'ютера, тобто можуть виявити вірус, не відомий програмі. Ці програми перевіряють стан BOOT-сектора, FAT-таблиці, атрибути файлів (обсяг, час створення тощо). При виявленні будь-яких змін користувачеві видається повідомлення (навіть у разі відсутності вірусів, але за наявності змін). Ревізором є, наприклад, програма Adinf.

Сторожі — резидентні програми, які постійно зберігаються у пам'яті й у визначений користувачем час перевіряють оперативну пам'ять комп'ютера (включаючи додаткову та розширену), файли, завантажувальний сектор, FAT-таблицю. Сторожем є, наприклад, програма AVP, що може виявити понад ЗО тис. вірусів.

Вакцини — програми, які використовуються для оброблення файлів та завантажувальних секторів з метою завчасного виявлення вірусів.

Резервування інформації. Архіватор WinZip. Основними способами резервування інформації є:

- її зберігання в захищених місцях (спеціальних приміщеннях, сейфах та ін.);
- зберігання інформації в територіально розподілених місцях.

Архіватор WinZip призначений для ущільнення інформації при її резервуванні. Він забезпечує:

- створення нового архіву;

- перегляд і відкривання існуючого архіву;
- додавання (вилучення) файлів до архіву;
- підтримку інтерфейсу WINDOWS 98/2000;
- Internet-підтримку для форматів Internet-файлів — gzip стиснення — Uunix, UUEncode, XXencode, BinHex, ARJ, LZH;
- створення саморозпаковувальних архівів;
- вірусну перевірку.

Для відкривання існуючого архіву його активізують, клацаючи правою клавішею миші (команда **Открыть**). Меню **File** містить команди для виконання таких дій, як відкривання та закривання архіву, створення нового, перегляд усіх архівів диска, вилучення, копіювання, переміщення, друкування архіву.

Меню **ACTIONS** містить команди для роботи з одним вибраним із архіву файлом (додавання, копіювання, вилучення, перейменування, створення саморозпаковувального файла). Для розпакування архівного файла вигористовується команда **Extract** або відповідна кнопка панелі інструментів.

Меню **ACTIONS** містить також команду **Make.Exe File**, яка використовується для створення саморозпаковувальних архівів. Робота з таким архівом не потребує програми-архіватора.

Для створення архіву файл виділяють, клацають правою клавішею миші та активізують команду **Add to**.

Технічні заходи. Один із технічних заходів захисту інформації — використання безперебійних джерел живлення (UPS), які дають змогу коректно завершити роботу і вийти з програми в разі перебою електропостачання. Ці пристрої залежно від складності задачі та потужності встановленого комп'ютерного обладнання можуть підтримувати роботу системи від 20 хв. до кількох годин. Більш надійна робота забезпечується при підключенні до запасної енергопідстанції. На підприємствах, що мають неперервний робочий цикл перероблення інформації (наприклад, головні банки), слід використовувати власні енергогенератори.

Адміністративні заходи. Керівники інформаційних відділів повинні:
чітко визначити функції всіх учасників інформаційного процесу;

- досліджувати й аналізувати ризики безпеки інформації;
- створити інструкції щодо дій персоналу в разі виникнення загроз безпеці інформації;
- мінімізувати ризик для тих, хто працює з важливою інформацією, та їх родин із метою запобігання їх викраденню та вимаганню інформації;
- визначити стратегію резервування, створити окрему інструкцію з резервування (наприклад, «Цю інформацію копіювати кожен день о 12 год.»). При цьому слід ураховувати *фізичне* руйнування магнітних носіїв з часом. Копій має бути як мінімум дві, одна з яких зберігається у вогнетривкому сейфі біля комп'ютера, інша — якнайдалі від офісу (на випадок вибуху, пожежі, землетрусу).

3. Запитання. Завдання.

1. За якими ознаками виокремлюють основні групи вірусів?
2. Охарактеризуйте роботу антивірусних програм.
3. Вкажіть адміністративні дії, що використовуються для захисту інформації від пошкоджень.
4. Назвіть основні функції програми-архіватора WinZip.

Вимоги до оформлення звіту

Звіт містить такі розділи:

- Титульний аркуш (дивитись додаток №1).
- Завдання роботи.
- Письмовий опис дій по виконанню завдань.
- Результати виконання зазначених завдань.

Мова написання – *українська*.

Внизу сторінки, праворуч проставляються **номери сторінок**.

У роздрукованому матеріалі застосовують такі **верхні та нижні колонтитули**:

верхній – назва роботи, прізвище студента, спеціальність, група.

нижній – дата створення документу, номер поточної сторінки та загальна кількість сторінок.

Здача та захист проводиться на практичних заняттях.

Оцінювання. Робота оцінюється в 4, 3 або 0 балів. Якщо студент оформив роботу згідно вищеописаних правил, здав та захистив її вчасно, та під час захисту продемонстрував вільне володіння викладеним матеріалом, тоді він отримує оцінку 4; якщо студент оформив роботу згідно вищеописаних правил, але здав та захистив її із незначним запізненням або під час захисту продемонстрував поверхневе володіння викладеним матеріалом, тоді він отримує оцінку 3; в усіх інших випадках здачі роботи студент отримує оцінку 0; після визначеного часу робота не приймається.