Задание 1
Прочитать текст, выполнить упр.1.1 ПИСЬМЕННО В ТЕТРАДИ

FILE BASICS

A **computer file** – or simply a “file” – is defined as a named collection of data that exists on a storage medium, such as a disk, CD, DVD, or tape. A file can contain a group of records, a document, a photo, music, a video, an e-mail message, or a computer program. Computer files have several characteristics, such as a name, format, location, size, and date.

Every file has a name and might also have a ***file extension***. When you save a file, you must provide a ***valid*** file name that ***adheres to*** specific rules, referred to as **file-naming convention**s. Each operating system has a unique set of file-naming ***conventions.*** Figure 4 lists the file-naming conventions for the current versions of Windows.

Case sensitive	No
Maximum length of file name	File name and extension cannot exceed 255 characters
Spaces allowed	Yes
Numbers allowed	Yes
Characters not allowed	* \ : < > | " / ?
File names not allowed	Aux, Com1, Com2, Com3, Com4, Con, Lpt1, Lpt2, Lpt3, Prn, Nul

Fig. 4: Windows File-naming Conventions

DOS and Windows 3.1 limited file names to eight characters. With that limitation, it was often difficult to create ***descriptive*** file names As a result, files were sometimes difficult to ***locate*** and identify. Today, most operating systems allow you to use long file names.

Current versions of Windows support file names up to 255 characters long. That limitation includes the entire file path sometimes called a file specification—drive letter, folders, file name and extension.

C:\My Music\Reggae\Marley One Love.mp3

Drive letter	Primary folder	Secondary folder	File name	File extension

An operating system maintains a list of files called a directory for each storage disk, tape, CD, or DVD. The main directory of a disk is referred to as the **root directory**. A root directory can be subdivided into smaller lists. Each list is called a **subdirectory**. When you use Windows, Mac OS, or a Linux graphical file manager, these subdirectories are depicted as folders. Folders can be created within other folders. (See the example, mentioned above) A folder name is separated from a drive letter and other folder names by a special symbol. In

Microsoft Windows, this symbol is the backslash (\). By storing a file in a folder, you ***assign*** it a place in an organized hierarchy of folders and files.

If an operating system attaches special ***significance*** to a symbol, you might not be able to use it in a file name. For example, Windows uses the colon (:) character to separate the device letter from a file name or folder, as in *C:Music.* When you use Windows applications, avoid using the symbols: * \ < > | " / and ? in file names.

Some operating systems also contain a list of reserved words that are used as commands or special identifiers. You cannot use these words alone as a file name. Windows users should avoid using the following reserved words as file names: *Nul, Aux, Com1, Com2, Com3, Com4, Con, Lpt1, Lpt2, Lpt3,* and *Prn.*

Some operating systems are case sensitive, but not those you typically work with on personal computers. Feel free to use uppercase and lowercase letters in file names that you create on PCs and Macs.

You can also use spaces in file names. That's a different rule than for e-mail addresses where spaces are not allowed. You've probably noticed that people often use underscores or periods instead of spaces in e-mail addresses such as Madi_Jones@msu.edu. That convention is not necessary in file names, so a file name such as Letter to Madi Jones is valid.

A file extension is an optional file identifier that is separated from the main file name by a period, as in *Paint.exe.* With some operating systems, such as Windows, file extensions work like tickets that admit people to different plays, movies, or concerts. If a file has the right extension for a ***particular*** application program, you'll see it in the list of files you can open with that software. A file extension is related to the file format, which is defined as the ***arrangement*** of data in a file and the coding scheme used to represent the data. Files containing graphics are usually stored using a different **file format** than files containing text. Most software have a **native file format** (.doc for MSWord, .pdf for AdobeAcrobat etc.)

To designate a file's location, you must first specify where the file is stored. Each of PC's storage devices is identified by a device letter (A:, C:, D:) – a convention that is specific to DOS and Windows. A device letter is usually followed by a colon, so drive A could be designated as A: or as 3.5" Floppy (A:).

The main hard disk drive is usually referred to as "drive C." Additional storage devices can be assigned letters D through Z. Although most PCs stick to the standard of drive A for the floppy disk drive and drive C for the hard disk drive, the device letters for CD, Zip, and DVD drives are not standardized.

A file contains data, stored as a group of bits. The more bits, the larger the file. **File size** is usually measured in bytes, kilobytes, or megabytes. ***Compared to*** small files, large files fill up storage space more quickly, require longer transmission times, and are more likely to ***be stripped off*** e-mail ***attachments*** by a mail server.

Your computer keeps track of the date that a file was created or last ***modified***. The **file date** is useful if you have created several versions of a file and want to make sure you know which version is the most ***recent***.

УПРАЖНЕНИЕ 1.1

Comprehension check. *Mark the following statements as True or False.*

1. When you create a file, you should give it a proper name according to file-naming conventions.
2. Windows limits the length of file names up to 265 characters.
3. Users must store a file in a folder to appoint it a place in a hierarchical structure of folders and files.
4. Operating systems add special significance to certain symbols that you should avoid in file names.
5. A file extension is a compulsory file identifier separated from the file name by a period.
6. The device letters for the floppy and hard disks are standardized.

Задание 1.2 Перевод слов

Vocabulary practice

1. Match up the words that are similar in meaning.

1. stick; 2. particular; 3. contain;	a) attach significance; b) symbol;
4. conventions; 5. add importance;	c) layout; d)appoint; e) be defined as;
6. be referred to as; 7. retrieve;	f) modify; g) valid; h) adhere; i) rules;
8. whole; 9. character; 10. assign;	j) certain; k) include; l) strip off;
11. proper; 12. arrangement; 13. alter.	m) entire.

УПРАЖНЕНИЕ 1.3
Найти подходящее по смыслу определение

1. A valid file requires adhering to specific rules called file-naming … .
a) conditions b) conventions c) conversions d) contents

2. Drive letter, folders, file name and extension restrict the whole file path which is referred to as a file … .
a) location b) identification c) specification d) format

3. A list of files for each storage medium is defined as a … .
a) scheme b) directory c) modification d) application

4. … e-mail addresses, a valid file name may contain spaces.
a) instead of b) compared to c) like d) unlike

5. A native file format is supported by most …, e. g. .doc for MSWord.
a) processors b) hardware c) software d) servers

6. A character generally following a device letter is a … .
a) backslash b) period c) asterisk d) colon

7. If a user wants to find the most recent version of a created file, the file … will be useful.

a) name b) size c) date d) extension

8. The file format means the … of data and a coding scheme representing the data.

a) management b) attachment c) appointment d) arrangement

9. To pad storage space, files of a bigger size require … time than small file

a) more b) less c) higher d) lower

3. Make two -word combinations using the words in columns and then fill in the gaps in the following sentences.

A:	B:
root	words
maximum	sensitive
application	attachments
file	directory
e-mail	formats
reserved	program
case	length

1. Some operating systems which allow you to use uppercase and lowercase letters in file names are not … .

2. Large files can be easily stripped off … by mail server.

3. Graphical files and files containing text are saved in different … .

4. A … of file names is restricted in file-naming conventions.

5. The … is the main directory of a disk.

6. A file with the relevant extension for a particular … will be seen in the list of files of that software.

7. There are … that represent commands or special identifiers and can't be used alone as a file name.

1.4. Fill in the gaps in the text.

A computer ___ is a named collection of data that exists on a storage medium, such as a hard disk, floppy disk, CD, DVD, or tape. Every file has a name and might also have a file extension. The rules that specify valid file names are called ___. These rules do not allow you to use certain characters or ___ words in a file name. A file ___ is usually related to a file format - the arrangement of data in a file and the coding scheme used to represent the data. A software program's ___ file format is the default format for storing files created with that program.

A file's location is defined by a file ___ sometimes called a "path", which includes the storage device, folder(s), file name and extension. In Windows, storage devices are identified by a ___ letter, followed by a colon. An operating system maintains a list of files called a ___ for each storage disk, tape, CD, or DVD. The main directory of a disk is sometimes referred to as the ___ directory, which can be subdivided into several smaller lists called subdirectories that are depicted as ___.

Задание 2 Ответить ПИСЬМЕННО на вопросы

Speaking. *Discuss the following questions.*

1. What is a computer file?
2. What are the rules for naming files?
3. Is there a maximum length for file names?
4. What is the purpose of folders?
5. Why are certain characters not allowed in a file name?
6. What are reserved words?
7. What is the difference between e-mail addresses and file names?
8. Are file extensions important?
9. How can you designate a file's location?
10. What is the significance of a file's size?
11. Why is the file date useful?

ЗАДАНИЕ 4 Письменно перевести текст «Компьютерные вирусы», соотнести перевод терминов

Text C

Задание 4.1 Pre-reading. *Match the meaning of the following English words with their Russian equivalents.*

computer virus	вирусная подпись
malicious code	бот
boot sector virus	компьютерный вирус
macro virus	«Троянский конь»
trigger event	переключающее (триггерное) событие
Trojan horse	контрольная сумма
Keylogger	клавиатурный шпион
Bot	макровирус
antivirus software	вирус сектора загрузки
Checksum	вредоносный код
virus signature	антивирусное программное обеспечение

Reading. *Read the text and try to guess the meaning of the words in bold. Check your variants in the dictionary.*

COMPUTER VIRUSES

Viruses are one of the biggest ***threats*** to the security of your computer files. In 1981, there was one known computer virus. Today, the count exceeds 100,000. Between 900 and 1,300 new viruses appear every month.

A **computer virus** is a set of program instructions that attaches itself to a file, ***reproduces*** itself, and ***spreads*** to other files. The term “computer virus” is often used to refer to any ***malicious*** code or software that ***invades*** a computer system. The term malicious code (sometimes called “malware”) refers to a program or set of program instructions designed to surreptitiously enter a computer and disrupt its normal work. Many types of malicious code, including viruses, worms, and Trojan horses, are created and ***unleashed*** by individuals referred to as “hackers” or “crackers”.

Viruses spread when people distribute ***infected*** files by exchanging disks and CDs, sending e-mail attachments, exchanging music on file-sharing networks, and downloading software from the Web. Many computer viruses infect files ***executed*** by your computer – files with extensions such as .exe, .com. or .vbs. When your computer executes an infected program, it also executes the attached virus instructions.

A virus can be classified as a file virus, ***boot*** sector virus, or macro virus. A file virus infects application programs, such as games. A boot sector virus infects the system files your computer uses every time you turn it on. These viruses can cause widespread ***damage*** to your computer files and recurring problems. A **macro virus** infects a set of instructions called a “macro” – a miniature program that usually contains ***legitimate*** instructions to automate document and worksheet production. When you view a document containing an infected macro, the macro virus duplicates itself into the general macro pool, where it is picked up by other documents. In addition to replicating itself, a virus might deliver a **payload**, which could be as harmless as displaying an annoying message or as devastating as ***corrupting*** the data on your computer’s hard disk. A trigger event, such as a specific date, can unleash some viruses. For example, the Michelangelo virus triggers on March 6, the birthday of artist Michelangelo.

A Trojan horse (sometimes simply called a “Trojan”) is a computer program that seems to perform one function while actually doing something else. Trojan horses are notorious for stealing passwords using a **keylogger** – a type of program that records your key-stroke.

Any software that can automate a task or autonomously execute a task when commanded to do so is called an intelligent agent. Because an intelligent agent behaves somewhat like a robot, it is often called a bot. Like a spider in its web, the person who controls many bot-infested computers can link them together into a network called a **botnet**. Botnets as large as 400,000 computers have been discovered by security experts.

Malicious Code Trends

Date	**Threats**	**Trends**

1981	Cloner	The first known virus begins to spread. Cloner infects files on disks formatted for Apple II computers. The prevalence of disk-borne viruses continues well into the1990s with Jerusalem (1987), Michelangelo (1992), and others.
1988	Internet Worm	The first major worm attack over the Internet sets the stage for today's prolific crop of mass-mailing worms.
1998	Back Orifice	First Trojan horse designed to allow a remote hacker to gain unauthorized access to a computer.
1999	Melissa	Macro viruses, such as Melissa and l.aroux, are ***prevalent*** for several years and cause trouble by infecting Microsoft Word and Excel files.
2000	Love Letter	One of the fastest spreading mass-mailing worms. Followed by Sobig, Blaster, and MyDoom (2004).
2001	Code Red	Worms designed for Denial of Service attacks gather steam. Code Red, which ***targeted*** the White House, is followed by Blaster (2001) and Slammer (2003).
2002	Klez	Klez is a mass-mailing worm that is particularly difficult to eradicate. Because the “From” address is spoofed, it is almost impossible to locate infected computers.
20Most notebook computers are equipped with several USB ports. 03	Mimail	Social engineering takes center stage and users are confused by fake e-mails from seemingly legitimate companies, such as PayPal, Microsoft, and Wells Fargo.
2004	Sasser Netsky Xombe MyDoom, Zafi Bagle	Worms, such as Sasser, begin to emerge that infect computers without user interaction, such as opening an infected e-mail attachment. Mass-mailing worms are still most prevalent. Worms that spread over instant messaging and handheld devices begin to emerge.
2005	Mytob	Bots become one of the biggest security

Zotob Rbot	problems. Arriving as e-mail attachments, links embedded in e-mail messages, or from infected banner ads, bots install themselves on unprotected computers, which can then be controlled by unauthorized hackers and commandeered into botnets that launch spam and Denial of Service attacks.

These are the top three steps you can take to prevent your computer from becoming infected:

- Use antivirus software on every computing device you own.
- Keep software patches and operating system service packs up to date.
- Do not open ***suspicious*** e-mail attachments.

Antivirus software is a type of utility software that can look for and eradicate viruses, Trojan horses, bots, and worms. This essential software is available for handheld computers, personal computers, and servers. Popular antivirus software for personal computers includes McAfee VirusScan, Norton AntiVirus, and F-Secure Anti-Virus.

Antivirus software uses several techniques to find viruses. As you know, some viruses attach themselves to an existing program. The presence of such a virus often ***increases*** the length of the original program. The earliest antivirus software simply ***examined*** the programs on a computer and recorded their length. A change in the length of a program from one computing session to the next indicated the possible presence of a virus.

To counter early antivirus software, hackers became more cunning. They created viruses that insert themselves into unused portions of a program file without changing its length. Antivirus software developers fought back. They designed software that examines the bytes in an uninfected application program and calculates a checksum. A **checksum** is a number calculated by combining the binary values of all bytes in a file. Each time you run an application program, antivirus software calculates the checksum and compares it with the previous checksum. If any byte in the application program has changed, the checksum will be different, and the antivirus software ***assumes*** that a virus is present.

Today's viruses, Trojan horses, bots, and worms are not limited to infecting program files, so modern antivirus software attempts to locate them by searching your computer's files and memory for virus signatures. A **virus signature** is a section of program code, such as a unique series of instructions, that can be used to identify a known malicious program, much as a fingerprint is used to identify an individual.

Comprehension check. *Choose the ending for each sentence from the two versions given.*

1. Worm named Code Red was targeted a) White House;
b) Bank of Scotland.

2. Any program designed to enter a computer and disrupt its normal operations is called	a) malicious code; b) utility.
3. Many types of malicious codes are created by	a) the computer itself; b) individuals referred to as “hackers”.
4. A boot sector virus infects the system files your computer uses	a) every time you turn it on; b) when you are connected to the Internet.
5. A change in the length of a program from one computing session to the next	a) indicated the possible presence of a virus; b) is a result of operation system work.
6. A checksum is	a) a number calculated by combining the binary values of all bytes in a file; b) the cost of an antivirus program.

Vocabulary practice

1. Which word does not belong to the group?

a) virus, worm, Trojan horse, bot, file, botnet;
b) distribute, download, automate, infect, view, execute;
c) duplicates, instructions, infects, invades, behaves, spreads;
d) spider, programmer, hacker, user, server, developer;
e) individual, general, normal, personal, analytical, digital.

2. Fill in the blanks choosing from the variants given.

1. Does the term computer virus refer to any malicious code that … (*makes up/invades*) a computer system?

2. When your computer executes an infected program it … (*executes/deletes*) the attached virus instructions.

3. A trigger event, such as a specific date, can … (*kill/destroy/unleash*) some viruses.

4. Love letter is one of the … (*slowest/fastest*) spreading mass-mailing worms of all time.

5. Hackers created viruses that insert themselves into … (*used/unused*) portions of a program file without changing its length.

3. Transform the given sentences using the word(s) in brackets without any change in meaning.

1. A computer virus is a set of programs that attaches itself to a file (*connecting*).

2. If a document contains an infected macro, the macro virus duplicates itself into the general macro pool, where it is picked up by other documents (*doubles, selected*).

3. A virus might deliver a payload which could be both harmless and devastating (*do no harm, corrupt*).

4. Software that can automate a task when commanded to do so is called an intelligent agent (*is able, is instructed*).

5. A trigger event, such as a specific date, can unleash some viruses (*particular, release*).

6. Trojan horses are notorious for stealing passwords using a keylogger – a type of program that records your key-strokes (*known, a sort*).

4. Fill in the gaps in the text.

A computer virus is a set of program instructions that attaches itself to a file, reproduces itself, and spreads to the other files. You might encounter several types of viruses. A virus that attaches itself to an application program, such as a game utility, is known as a ___ virus. A boot ___ virus infects the system files your computer uses every time you turn it on. A ___ virus infects a set of instructions that automates document and worksheet production.

A Trojan horse is a computer program that seems to perform one function while actually doing something else. Such programs are notorious for stealing ___, although some delete files and cause other problems.

___ software can help prevent viruses from invading your computer system and can root out viruses that that take up residence. This software typically scans for a virus ___ and is sometimes referred to as virus scanning software.

Speaking. *Discuss the following questions.*

1. What is a computer virus?
2. How do viruses spread?
3. Are there different kinds of viruses?
4. What is a Trojan horse? What is a bot?
5. What is a botnet?
6. How can you avoid viruses and worms?
7. What is antivirus software? How does it work?

Text D

Reading. *Read the text and try to guess the meaning of the words in bold. Check your variants in the dictionary.*

DATA BACKUP

Backup and restore procedures

Have you ever mistakenly copied an old version of a document over a new version? Has your computer's hard disk drive gone on the fritz? Did a virus wipe out your files? Has lightning “fried” your computer system? These kinds of data disasters are not rare; they happen to everyone. You can’t always prevent them, so you need a backup plan that helps you recover data that's been wiped out by operator error, viruses, or hardware failures.

A backup is a copy of one or more files that has been made in case the original files become ***damaged***. A backup is usually stored on a different storage medium from the original files. For example, you can back up files from your hard disk to a different hard disk, a writable CD or DVD; tape, floppy disk, or Web site.

A good backup plan allows you to ***restore*** your computing ***environment*** to its pre-disaster state with a minimum of fuss. Unfortunately, no single backup plan ***fits*** everyone’s computing style or budget. You must ***devise*** your own backup plan that’s tailored to your particular computing needs.

A **full-system backup** contains a copy of every program, data, and system file on a computer. The advantage of a full-system backup is that you can easily restore your computer to its pre-disaster state simply by copying the backup files to a new hard disk. A full-system backup takes a lot of time, however, and automating the process requires a large-capacity tape backup device or a second hard disk drive.

A workable alternative to a full system backup is a “selective” backup that contains only your most important data files. The ***disadvantage*** of this backup strategy is that because you backed up only data files, you must manually reinstall all your software before restoring your data files.

If your strategy is to back up your important data files, the procedure can be simplified if you’ve stored all these files in one folder or its subfolders.

In addition to data files you create, a few other types of data files might be important to you. Consider making backups of these-files:

- Internet connection information
- E-mail folders
- E-mail address book
- Favorite URLs
- Downloads

Windows users often hear a ***variety*** of rumors about backing up the Windows Registry. The Registry, as it is usually called, is an important group of files the Windows operating system uses to store configuration information about all the devices and software installed on a computer system.

As simple as it sounds, backing up the Registry can present a bit of a problem because the Registry is always open while your computer is on. Windows users whose backup plans encompass all files on the hard disk must ***make sure*** their backup software provides an option for including the Windows Registry.

Your backup ***schedule*** depends on how much data you can ***afford*** to lose. If you’re working on an important project, you might want to back up the project files several times a day. ***Under normal use***, however, most people schedule a once-a-week backup. If you work with a To Do list, use it to remind yourself when it is time to make a backup.

Store your backups in a safe place. Don't keep them at your computer desk because a fire or flood that damages your computer could also wipe out your backups. Storing your backups at a different location is the best idea, but at least store them in a room apart from your computer.

Backup devices

The backup device you select depends on the value of your data, your current equipment, and your budget. Most computer owners use what they have — a writable CD drive, Zip drive, or floppy disk drive.

The major disadvantage of backing up your data on CDs and DVDs is that the writing process is slow — slower than writing data to tape or a removable hard disk. Further, although it is ***feasible*** to back up your entire system on a series of CDs or DVDs, you would have to use special backup software, monitor the backup process, and switch disks occasionally. CDs and DVDs are more practical for backing up a select group of important data files.

Zip disks with 100 MB or 250 MB capacity are sufficient for backups of documents and most digital graphics files. Several 750 MB Zip disks might be enough for backing up all your data files and could be feasible for a full-system backup if you have not installed lots of application software.

A second hard disk drive is a good backup option — especially if it has equivalent capacity to your main hard disk. This capacity allows the backup process to proceed unattended because you won't have to swap disks or CDs. Speed-wise, a hard disk is faster than tape, CD, or DVD drives. Unfortunately, like your computer's main hard disk, a backup hard disk is susceptible to head ***crashes***, making it one of the least reliable storage options.

Network and internet backup

If your computer is connected to a local area network, you might be able to use the network server as a backup device. Before ***entrusting*** your data to a server, check with the network administrator to make sure you are allowed to store a large amount of data on the server. Because you might not want strangers to access your data, you should store it in a password-protected, non-shared folder. You also should make sure the server will be backed up on a regular basis so that your backup data won't be wiped out by a server crash.

Several Web sites offer fee-based backup storage space. When needed, you can simply download backup files from the Web site to your hard disk. These sites are practical for backups of your data files, but space limitations and download times make them impractical for a full-system backup. Experts suggest that you should not rely on a Web site as your only method of backup. If a site goes out of business or is the ***target*** of a Denial of Service attack, your backup data might not be accessible.

Backup software

To make a backup, you can use **backup software** — a set of utility programs designed to back up and restore files. Backup software usually includes options that make it easy to schedule periodic backups, define a set of files that you want to regularly back up, and automate the restoration process.

Backup software differs from most copy routines because it typically compresses all the files for a backup and places them in one large file. Under the direction of backup software, this file can spread across multiple tapes if necessary. The file is indexed so that individual files can be located, uncompressed, and restored.

Boot disks

A ***boot*** disk is a floppy disk or CD containing the operating system files needed to boot your computer without accessing the hard disk. A barebones boot disk simply loads the operating system kernel. It is needed, if your hard disk fails or a virus wipes out the boot sector files on your hard disk, you will not be able to use your normal boot procedure.

To create an MS-DOS boot disk, insert a blank floppy disk in drive A. Open My Computer or Windows Explorer, and then right-click the Drive A icon. Select Format and check the box labeled Create an MS-DOS startup disk.

Упр. 1.1 Comprehension check. *Match the beginnings of the sentences in the first column with the endings in the second one.*

1. A backup is a copy of one or more files
2. A good backup plan allows you
3. You must devise your own backup plan
4. A full-system backup takes a lot of time
5. Your backup schedule depends on how much data
6 The backup device you select depends on the
7. If your computer is connected to a local area network

a) to restore your computing environment to its pre-disaster state with a minimum of fuss.
b) and automating the process requires a large capacity tape backup device or a second hard disk drive.
c) that is tailored to your particular computing needs.
d) that has been made in case the original files become damaged.
e) value of your data, your current equipment, and your budget.
f) you can afford to lose.
g) you might be able to use the network server as a backup device.

Vocabulary practice

1. Put the appropriate unscrambled words into the sentences on the right.

1. Because you backed up only data files you must manually ___ all

covreer
evitartalen
lailtsner
emagad
mumide

your software before restoring your data files.

2. You need a backup plan that helps you ___ data that's been wiped out by operator error, viruses or hardware ___.

3. Store your backups in a safe place or a fire or flood that ___ your computer could also wipe out your backup.

4. A workable ___ to a full system backup is a selective backup that contains only your most important data files.

5. A backup is usually stored on a different storage ___ from the original files.

2. Fill in the blanks choosing from the variants given.

1. A backup is usually … (*detected/stored*) on a different storage medium from the original files.

2. A workable alternative to a full system backup is a … (*selective/overall*) backup that contains only your most important data files.

3. Storing your backups at a different locations is … (*not a good/the best*) idea.

4. The backup device you select depends on … (*how much data you can afford to lose/the value of your data/your current equipment and your budget*).

5. A full-system backup … (*can be done in no time/takes a lot of time*).

6. Under normal use most people schedule … (*an everyday backup/once-a-week backup*).

3. Match the beginnings and the endings of the instructions/steps given and put them into correct order.

1. Your backup schedule depends on	a) that is tailored to your particular computing needs.
2. No single backup plan fits	b) most people schedule a once-a-week backup.
3. You can't always prevent data disasters	c) how much data you can afford to use.
4. You must devise your own backup plan	d) everyone's computing style or budget.
5. Under normal use	e) but at least store them in a room apart from your computer.
6. The best idea is storing your backups at a different location	f) so you need a backup plan that helps you recover data that's been wiped out.

4. Fill in the gaps in the text.

A backup is a copy of one or more files that has been made in case the original files become damaged. For safety, a backup is usually stored on a different storage medium from the original files. A good backup plan allows you to ___ your computing environment to its pre-disaster state with a minimum of fuss.

No single backup plan fits everyone’s computing style or budget. Your personal backup plan depends on the files you need to back up, the hardware you have available to make backups, and your backup software. In any case, it is a good idea to back up the Windows ___ and make sure your files are free of ___. Backups should be stored in a safe place, away from the computer.

Backups can be recorded on floppy disks, writable CDs and DVDs, networks, Web sites, a second hard disk, or tapes. Many computer owners depend on writable CDs for backups, and use My Computer or Windows ___ to simply select files and copy files to the backup. ___ drives and backup software are typically used in business situations when a full-system backup is desirable. Backup software differs from most copy routines because it ___ all the files for a backup into one large file.

In addition to file backups, you should have a ___ disk containing the operating system files and settings needed to start your computer without accessing the hard disk.

Speaking. *Discuss the following questions.*

1. Why do you need to make backups?
2. What are the major strategies and plans of backup? What does their choice depend on?
3. What are the advantages and disadvantages of different backup devices?
4. What can you say about network and internet backup?
5. What can you say about backup software?
6. What is a boot disk? How can it be created?

Critical thinking. *Read the article and express you opinion on the problem.*

Computer Crime

It doesn’t take any special digital expertise to mastermind some computer crimes. Setting fire to a computer doesn’t require the same finesse as writing a stealthy virus, but both can have the same disastrous effect on data. “Old-fashioned” crimes, such as arson, that take a high-tech twist because they involve a computer can be prosecuted under traditional laws.

Traditional laws do not, however, cover the range of possibilities for computer crimes. Suppose a person unlawfully enters a computer facility and steals backup tapes. That person might be prosecuted for breaking and entering. But would common breaking and entering laws apply to a person who uses an off-site terminal to “enter” a computer system without authorization? And what if a person copies a data file without authorization? Has that file really been “stolen” if the original remains on the computer?

Many countries have computer crime laws that specifically define computer data and software as personal property. These laws also define as crimes the unauthorized access, use, modification, or disabling of a computer system or data. But laws don’t necessarily stop criminals. If they did, we wouldn’t have to deal with malicious code and intrusions.

A 1995 high-profile case involved a computer hacker named Kevin Mitnick, who was accused of breaking into dozens of corporate, university, government, and personal computers. Although vilified in the media, Mitnick had the support of many hackers and other people who believed that the prosecution grossly exaggerated the extent of his crimes. Nonetheless, Mitnick was sentenced to 46 months in prison and ordered to pay restitution in the amount of $4,125 during his three-year period of supervised release. The prosecution was horrified by such a paltry sum – an amount that was much less than its request for $1,5 million in restitution.

Forbes reporter Adam L. Penenberg took issue with the 46-month sentence imposed by Judge Marianne Pfaelzer and wrote, “This in a country where the average prison term for manslaughter is three years. Mitnick’s crimes were curiously innocuous. He broke into corporate computers, but no evidence indicates that he destroyed data. Or sold anything he copied. Yes, he pilfered software — but in doing so left it behind. This world of bits is a strange one, in which you can take something and still leave it for its rightful owner. The theft laws designed for payroll sacks and motor vehicles just don’t apply to a hacker.”

The U.S. Patriot Act and the Cyber-Security Enhancement Act carry even stiffer penalties – anywhere from 10 years to life in prison.

A CNET reporter questions the harshness of such penalties: “What bothers me most is that here in the United States, rapists serve, on average, 10 years in prison. Yet if, instead of assaulting another human being, that same person had released a virus on the Net, the criminal would get the same or an even harsher sentence.”

Law makers hope that stiff penalties will deter cyber criminals. U. S. Attorney John McKay is quoted as saying, “Let there be no mistake about it, cyber-hacking is a crime. It harms persons, it harms individuals, it harms businesses.

These cases illustrate our culture's ambivalent attitude toward computer hackers. On the one hand, they are viewed as evil cyberterrorists who are set on destroying the glue that binds together the Information Age. From this perspective, hackers are criminals who must be hunted down, forced to make restitution for damages, and prevented from creating further havoc.

From another perspective, hackers are viewed more as Casper the Friendly Ghost in cur complex cybermachines – as moderately bothersome entities whose pranks are tolerated by the computer community, along with software bugs. Seen from this perspective, a hacker's pranks are part of the normal course of study that leads to the highest echelons of computer expertise.

What do you think?

1. Should a computer virus distribution sentence carry the same penalty as manslaughter?
2. Should it be a crime to steal a copy of computer data while leaving the original data

in place and unaltered?

3. Should hackers be sent to jail if they cannot pay restitution to companies and
individuals who lost money as the result of a prank?

4. Do you think that a hacker would make a good consultant on computer security?

Final test. *Do the tasks in the following test.*

1. A (n) ___ is a copy of one or more files that has been made in case the original files become damaged.
2. The Windows ___ is an important group of files that the Windows operating system uses to store configuration information about all the devices and software installed on a computer system.
3. The main directory of a disk is referred to as the ___ directory.
4. The main hard disk drive on a PC is often referred to as “drive C”. (*True/False*)
5. A filename extension is usually related to a file ___, which is the arrangement of data in a file and the coding scheme used to represent the data.
6. Antivirus software is 100% reliable when it comes to protecting your computer from viruses. (*True/False*)
7. A file specification or path typically includes all of the following information EXCEPT ___.
a) the file author b) the file name c) the file extension d) the drive letter
8. ___ software is a set of utility programs that looks for and eradicates viruses, worms, and Trojan horses.
9. File-naming ___ are a set of rules for naming files.
10. The easiest way to convert a file from one format to another is to find an application program that works with both file formats. (*True/False*)
11. Deleting a file’s icon from a directory does not necessarily remove the data from the disk. (*True/False*)
12. A computer ___ is a set of program instructions that attaches itself to a file, reproduces itself, and spreads to other files.
13. A root directory typically contains smaller ___, often depicted as folders in graphical user interfaces.
14. A (n) ___ is a computer program that seems to perform one function while actually doing something else.
15. A virus can be spread if people distribute infected files by ___.
a) exchanging disks or CDs b) sending e-mail attachments
c) downloading software from the Web d) all of the above
16. You should update your antivirus software regularly. (*True/False*)
17. Bot-infected computers linked together into a network is called a(n) ___.
18. A virus ___ is a section of the virus program that can be used to identify a known virus.
19. Computer virus trigger events are often tied to a specific date. (*True/False*)
20. The file ___ helps you keep track of the most current version of your file when you have saved several versions.

Projects. *Choose and perform one of the projects given.*

1. Select one of the following statements and argue for or against it:

- People have the “right” to hone their computing skills by breaking into computers.
- A person who creates a virus is perfectly justified in releasing it if the purpose is to make everyone aware of these security breaches.
- Computer crimes are no different from other crimes, and computer criminals should be held responsible for the damage they cause.

2. Suppose you are a reporter for a local television station. Your assignment is to create a 90-second story about new emerged virus for your local TV news show. The basic objectives of the story are (1) to inform about the ways of spreading this virus and attributes that enable a person to find out presence of this particular virus and (2) to provide a set of concrete steps that a person could take to minimize the consequences for his computer and get rid of the virus. Of course, the network wants the story to be interesting, so you have to include a human-interest angle. Write the script for the story and include notes about the visuals that will appear.