Краснодарский университет МВД России

АНГЛИЙСКИЙ ЯЗЫК ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ, ИСПОЛЬЗУЮЩИХ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

ENGLISH FOR THE FUTURE INFORMATION TECHNOLOGY SPECIALISTS IN THEIR PROFESSIONAL ACTIVITIES

Учебное пособие
по английскому языку

Краснодар
2023

УДК 811.111
ББК 81.2Англ-9
А647

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Составители: *С. В. Борисова, В. А. Гончарова*

Рецензенты:
В. В. Посиделова, кандидат филологических наук (Ростовский юридический институт МВД России);
Б. Н. Селин, кандидат педагогических наук (Белгородский юридический институт МВД России имени И.Д. Путилина).

А647 **Английский язык** для подготовки специалистов, использующих информационные технологии в профессиональной деятельности = English for the Future Information Technology Specialists in Their Professional Activities : учебное пособие по английскому языку / сост.: С. В. Борисова, В. А. Гончарова. – Краснодар : Краснодарский университет МВД России, 2023. – 220 с.

ISBN 978-5-9266-1947-5

Содержащиеся в пособии современные аутентичные профессионально ориентированные материалы способствуют углублению знаний обучающихся по темам: «Компьютер и компьютерные технологии обработки информации», «Программное обеспечение. Интернет-технологии», «Средства и системы связи. Компьютерные сети», «Программирование: языки, методы и технологии. Особое внимание уделяется профессиональной лексике, необходимой для деятельности будущих сотрудников органов внутренних дел.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 811.111
ББК 81.2Англ-9

ISBN 978-5-9266-1947-5

Contents

Introduction

Введение

Методическая организация учебного пособия, предусматривает выполнение целевых установок программы – научить будущих профессионалов – сотрудников полиции понимать и обсуждать литературу, связанную с аспектами информационных технологий, воспринимать на слух иноязычную речь и объясняться в определенных ситуациях профессионального характера на изучаемом языке по данной теме.

Методическая система учебного пособия предоставляет возможность освоить учебный материал поэтапно – от простого к сложному. Изучаются тематические лексические единицы, которые находят отражение в базовых текстах. После работы над текстом даются грамматические правила, освоение и закрепление которых осуществляется посредством упражнений для обучающихся разного уровня. В пособие включен краткий тематический англо-русский словарь, новый англо-английский технический словарь, англо-английский аудио-словарь основных понятий и терминов, тексты для дополнительного чтения с вопросами для самоконтроля, приложение с грамматическими таблицами и рекомендациями по реферированию статей. Учебное пособие «Английский язык для подготовки специалистов, использующих информационные технологии в профессиональной деятельности» предполагает взаимосвязанное прохождение лексического и грамматического материала и развитие речевых умений и навыков. Каждый раздел пособия включает как аутентичные, так и адаптированные учебные, профессионально ориентированные тексты, лексико-грамматические комментарии и упражнения. Для будущих сотрудников ОВД в сфере безопасности информационных технологий представляется необходимым овладение всеми видами чтения литературы по специальности на английском языке с

целью получения профессионально значимой информации, т. к. при решении ряда профессиональных задач как вид речевой деятельности чтение широко востребовано.

Особое внимание уделено разделам, которые содержат лексико-грамматические единицы, введённые в предыдущих разделах, что снимает сложности в активизации новых единиц. Упражнения и различные задания стимулируют освоение навыков речевой коммуникации, как в устной, так и письменной речи.

Каждый тематический раздел снабжён QR-кодом  , который позволяет перейти на Яндекс-диск для просмотра и, при необходимости, для скачивания видео-материала по теме. Данный видеоматериал на усмотрении преподавателя и обучающегося может быть использован как для ознакомления и закрепления материала, так и для контроля или самоконтроля полученных знаний по теме.

Изучение каждого раздела предваряет краткий англо-русский словарь и QR-код  на аудио-словарь основных понятий.

Представленные в пособии аутентичные тексты на английском языке углубляют знания обучающихся специальности Безопасность информационных технологий в правоохранительной сфере, знакомят их с современным английским языком, расширяют представления о компьютерных технологиях прошлого, настоящего и планируемого будущего, а также информируют об имеющихся методах и технологиях обработки информации, программировании и могут быть использованы профессорско-преподавательским составом, адъюнктами, курсантами и слушателями образовательных организаций МВД России как для работы в аудитории, так и для самоконтроля.

UNIT I. COMPUTER AND INFORMATION TECHNOLOGY.

PART 1. COMPUTERS TODAY

Study the vocabulary and learn the words

Tool	инструмент;
Peripheral devices (peripherals)	периферийные устройства;
Instruction	команда, инструкция, указание;
enable	разрешать, позволять, делать возможным;
fraction of the time	за короткое время;
to lurk	скрываться, оставаться незамеченным;
transaction	сделка, группа операций;
to monitor	наблюдать, контролировать, следить;
to process	обрабатывать;
solution	решение
application	применение, использование
to interact	взаимодействовать;
to control	управлять, регулировать;
to reduce costs	сокращать затраты;
otherwise	иначе, иным образом;
to affect	влиять, воздействовать.

Read and translate the text

Modern computers

«Modern computers are found everywhere: homes, offices, businesses, hospitals, and schools, to name a few. Contemporary society has become so dependent on computers that many people become frustrated and unable to function when computers are "down." Because of this dependence, computers are regarded as essential tools for everything from navigation to entertainment.

Today's computers are smaller, faster, and cheaper than their predecessors. Some computers are the size of a deck of cards. Hand-held Personal Data Assistants and notebook computers or "ultra-lights" make users portable and give them the opportunity to work in a variety of places. These systems provide a wide range of connectivity and access to information on local, wide, and wireless networks. This gives users more convenience and more control over their time.

Future computers promise to be even faster than today's computers and smaller than a deck of cards. Perhaps they will become the size of coins and offer "smart" or **artificial intelligence** features like expert intelligence, neural network **pattern recognition** features, or natural language capabilities. These capabilities will allow users to more conveniently interact with systems and efficiently process large amounts of information from a variety of sources: fax, e-mail, Internet, and telephone. Already evident are some evolving cutting-edge applications for computer technology: wearable computers, DNA computers, virtual reality devices, quantum computers, and optical computers.

Wearable Computers

Is a wearable computer in your future? With hardware shrinking and becoming more powerful and more able to execute instructions and perform computations in shorter timeframes, it is very possible that there will be widespread use of wearable systems in the future. A wearable is defined as a

handless system with a data processor supported by a user's body rather than an external surface. The unit may have several components (camera, touch panel, screen, wrist-mounted keyboard, head-worn display, and so forth) that work together to bring technology to situational and environmental problems.

Assembly and repair environments are ideally suited for wearable technology because they deploy users with technical expertise to problem areas. Wearable computers allow users to keep their hands free at all times while providing access to technical specifications and detailed instructions for problem-solving and troubleshooting.

In the future, wearables may even be built into the fabric of clothing. Garments can be made using **conductive** and nonconductive textiles like organza and yarn, gripper snaps, and embroidered elements. Ordinary fabric can be connected to electronic components to add functionality and usability.

DNA-Based Computers

Can small molecules such as DNA be used as the basis for new computing devices? A biologist and mathematician named Leonard Adelman first linked genetics and computer technology in the mid-1990s. Adelman coded a problem using the four **nucleotides** that combine to form DNA and discovered that the DNA solution was accurate.

A DNA-based computer would be radically different from a conventional computer. Instead of storing data on silicon chips, converting data to binary notation (0s and 1s), and performing computations on the binary digits, DNA computing would rely on data found in patterns of molecules in a synthetic DNA strand. Each strand represents one possible answer to the problem. A set of strands is manufactured so that all conceivable answers are included. To winnow out a solution, the DNA computer subjects all the strands simultaneously to a series of chemical reactions that imitate mathematical computations.

The advantage of DNA computing is that it works in parallel, processing all possible answers simultaneously. An electronic computer can analyze only one potential answer at a time. The future holds great possibilities as DNA-based computers could be used to perform **parallel processing** applications, **DNA fingerprinting** , and the decoding of strategic information such as banking, military, and communications data.

Virtual Reality Devices

Virtual reality (VR) immerses its user in a simulated world of possibilities and actions. In the virtual world, the user has the ability (through head-mounted displays, gloves, and body suits) to respond to **tactile** stimulation. Users manipulate objects, examine architectural renderings, and interact in an environment before it becomes a physical reality. This is often very cost-effective, and it supports decision-making tasks. VR is often used in modeling situations, but its future holds promise in other areas: education, government, medicine, and personal uses.

In education, students and teachers may have the ability to interact inside virtual classrooms to explore ideas, construct knowledge structures, and conduct experiments without risk, fear of failure, or alienation. Government offices may use VR technology to improve services, provide better delivery of health care (model symptoms, progression, and prevention), and monitor environmental changes in air quality, wetlands, ozone layers, and other ecological areas (animal populations and forestry).

Medical areas could use VR to train interns and practicing physicians on new procedures and equipment; observe internal tissue production in three dimensions (3-D); collect and better analyze medical images; simulate surgical and invasive procedures; and empower therapists to use exposure therapy along with realistic models. VR technology could also be used to augment instructional games, 3-D movies, and real-time conferencing and communication efforts.

Quantum Computers

The first application of **quantum theory** and computers occurred in 1981 at Argonne National Laboratory. Quantum computers, like conventional computing systems, were proposed before supportive hardware existed. In 1985, a quantum parallel computer was proposed. Today, physicists and computer scientists still hope that the imprecision of subatomic particles can be used to solve problems that thus far remain unsolved.

The quantum computer would overcome some of the problems that have plagued conventional computers: namely, sequentially following rules and representing data as a series of switches corresponding to 0 or 1. By using subatomic particles, quantum computers will have the ability to represent a number of different states simultaneously. These particles will be manipulated by the rules of probability rather than absolute states or logic gates. Manipulating these small subatomic particles will allow researchers to solve larger, more complex problems, such as determining drug properties, performing complex computations, precisely predicting weather conditions, and helping chip designers create circuits that are presently impossibly complex.

Optical Computers

As microprocessor chip designers reach physical limitations that prevent them from making chips faster, they are searching for other materials to conduct data through the electrical circuits of computer systems. If designers could harness photons to transmit data, faster microprocessor chips could become a reality.

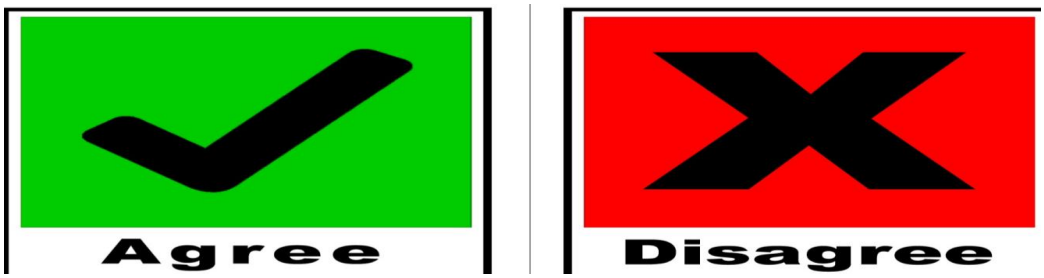
This new frontier—optical computing—could allow computers to perform parallel processing tasks more efficiently and increase the speed and complexity of computers by allowing them to process billions of **bits** simultaneously. Optical computers might use **fiber-optic** cable, optical chips, or wireless optical networks to process and transmit data.

Fiber-optic cable is currently used in many establishments. It uses a laser to transmit billions of data bits through cables made of thin strands of glass coated in layers of plastic. Signals can be carried over a distance of 40 to 60 miles. A more recent development—optical chips—could cut the cost of optical communication by using Dense Wave Division Multiplexing technology to carry more information over a fiber. This would give users increased **bandwidth** for connecting to the Internet. Optical networks could be used to improve free-space optics, video delivery, and voice communications»

I. Answer the following questions:

1. Who interacted with yesterday's computers?
2. What service do computers in business provide?
3. How do ecologists use computers?
4. How do engineers use them?
5. How do educators use them?
6. Where can we find computes in our life?
7. What computer manufacturers do you know?

II. Agree or disagree with the statements.



1. Today computers are operated only by scientists, mathematicians and engineers.
2. Businesses and organizations own and use only personnel computers.
3. All computers are produced of the same size and power.
4. In offices computers are used only as typewriters.
5. Any kind of job can be performed with the help of the computer.
6. Our lives are affected by computers every day.
7. All country schools have computer classes.

III. Translate from Russian into English.

1. В настоящее время нельзя обойтись без компьютера.
2. Каждый день мы ходим в банк, пользуемся кредитной картой, оплачиваем счёт, а компьютер остается незамеченным.
3. Компьютеры могут за короткое время обработать информацию.
4. Нет предела применению компьютера.
5. Экологи используют компьютеры, чтобы наблюдать за проблемами окружающей среды.
6. Учёные строят компьютерные модели самолётов.
7. Компьютеры используются в разных целях.

IV. Read the text

Without my computer I would not have the pleasure of the getting to my favourite sites, I would have difficulty in communication with my friends, and I would not be able to do my work for college. I often wonder how we all managed before computers were a common place in the home. I just don't have the time to be always running to the post box to send letters. E – mail is very important when you have a tough schedule. Most of my relaxed time is spent at the computer as by the time I finish doing homework. I am too tired and it is often too late to go out. It is reference aid and educational tool. If all else fails, you can play cards on it, although I am for action games!

V. Write an essay giving your opinion on the following topic:

"Imagine that you could only use one of the following: a computer, a mobile phone or a car. Which one would you use and why?"

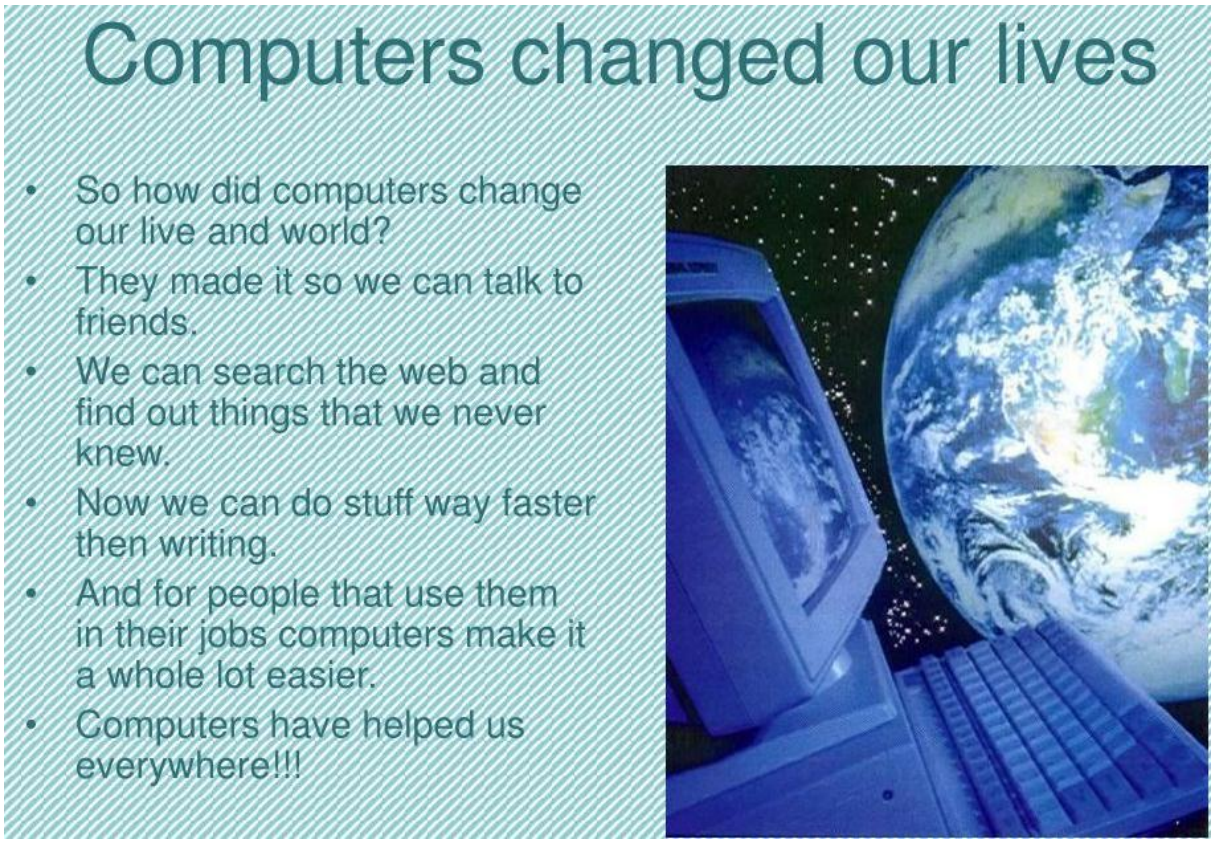
(see Appendix 7)

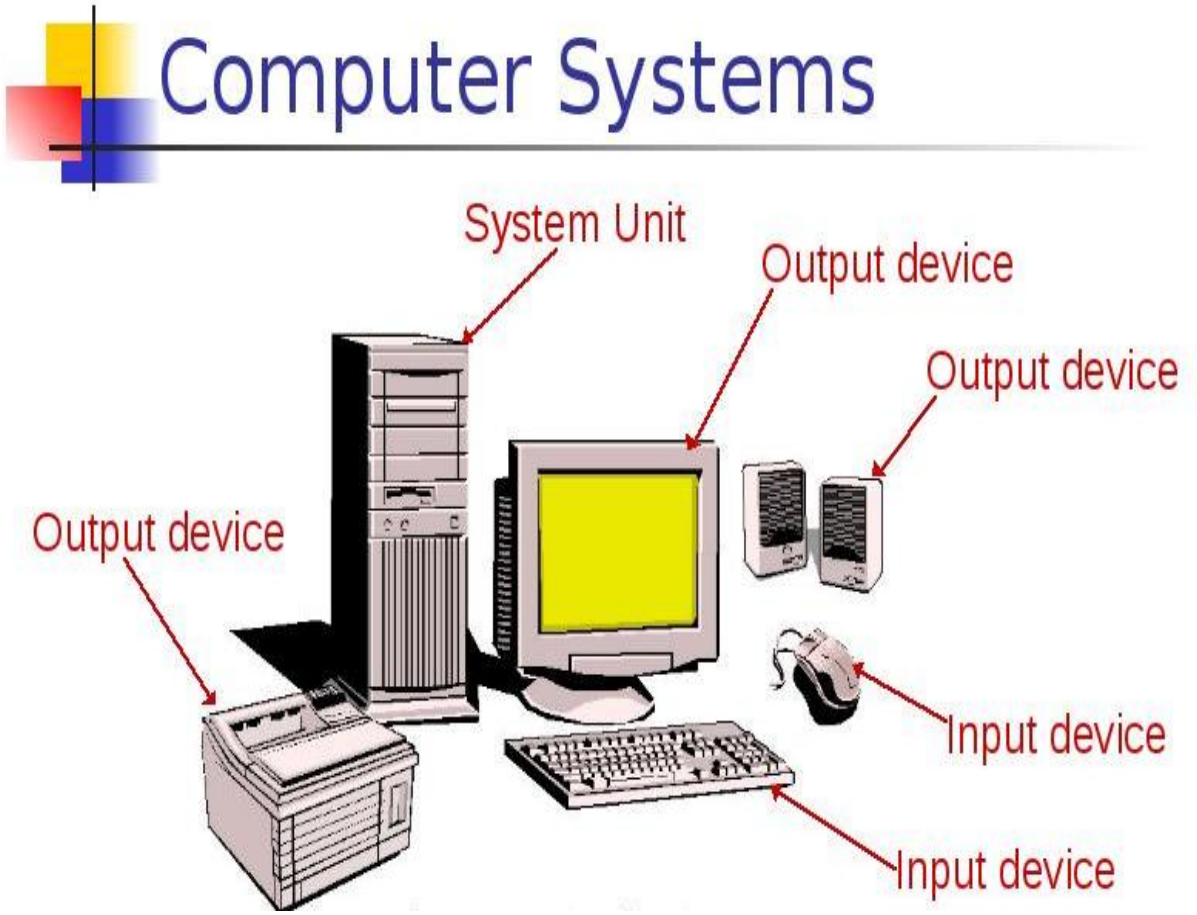
VI. Speak on the following:

„Computers change our life“

Use questions:

1. Do you have your own computer?
2. What purposes do you use it for?
3. How long have you had PC?
4. What devices is it supplied with?





Part 2. COMPUTER SYSTEMS

Vocabulary

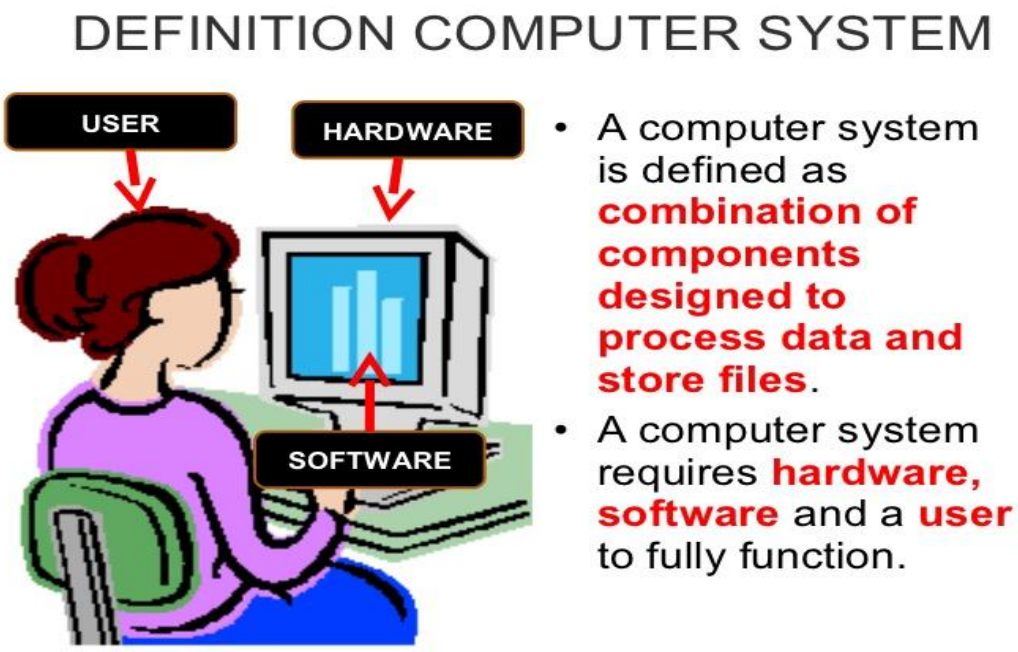
Study the vocabulary and learn the words

1. **authenticate** [C] подтвердить личность (подлинность) пользователя компьютера; E.g.: *Admittance was denied when the computer could not authenticate him*. C греч. authentikos (подлинный).

2. **boot** [D] запустить компьютер. *Сокращение от bootstrap*.
3. **browser** [A] браузер - Программное обеспечение, которое позволяет вам исследовать или просматривать Интернет. от фр. brouter (кормиться).
4. **compres** [A] сжимать; хранить данные в меньшем количестве места ; E.g.: *The manuscript was compressed on a single floppy disk*. Со старо-фр. compresser.
5. **cracker** [B] взломщик; Злоумышленник; кто-то, кто взломал компьютерные системы. С нем. krachen
6. **curso** [B] курсор; подвижный индикатор на экране компьютера; E.g.: *He put the cursor after the last typed word*. С лат. (бегать).
7. **download** [A] скачать; скопировать файл или программу на персональный компьютер; С др.англ. adune (с холма) and lad (несущий).
8. **emoticon** [D] смайлик; Иллюстрация, передающая настроение; Also called smiley. Derived from emotion and icon.
9. **gigabyte** [B] гигабайт; единица хранения; E.g.: *A gigabyte of work was saved on her home computer*. С греч. gigas (гигант) и варианта бита (сокращение от for binary digit- двоичной цифры).
10. **glitch** [C] глюк; Ошибка; неисправность; E.g.: *A telecommunications glitch nearly wiped out the stockbroker's on-line trading*.
11. **hit** [D] Посетить веб-сайт. С древнескандинавского hitta (встречаться с кем-либо).

12. **link** [C] ссылка; относящийся к сайту в интернете; E.g.: *One links anthem from Carusoto Pavarotti*. C нем. Gelenk (присоединённый).
13. **log on** [B] войти в систему; получить доступ к компьютерной сети; E.g.: *A user IDand password will help you log on*. Origin unknown.
14. **modem** [D] модем, Подключающее устройство между компьютерами по телефонной линии; E.g.: *The journalist submitted her article by modem*. Condensed form of modulator and demodulator.
15. **network** [C] сеть, Система электронно-объединенных компьютеров; E.g.: *A network offers many opportunities for sharing information*. C др.-англ. nett (узел) and weorc (действие).
16. **pixel** [A] пиксель, элемент изображения; основная единица экранного изображения. Сокращение от pix и element.
17. **scanner** [A] Machine that reproduces images onto a computer. Latin scandere (to climb).
18. **server** [A] сервер, Машина, которая воспроизводит изображения на компьютер Central computer sharing resources and data with other computers on a network. C лат.servire (быть в использовании).
19. **shareware** [D] Бесплатное пробное программное обеспечение, часто требующее более поздней оплаты. Combination of share and software.
20. **virus** [D] вирус, цифровая инфекция; as, *The virus wreaked havoc with the bank's accounting.*

Read and translate



COMPUTER SYSTEMS

Computers can be divided into 3 main types, depending on their size and power.

The largest and most powerful are Mainframe computers. They can handle large amounts of information very quickly and can be used by many people at the same time. They usually fill a whole room and are sometimes referred to as mainframes or computer installations. They are found in large institutions like universities and government departments.

Minicomputers, commonly known as minis, are smaller and less powerful than mainframes. They are about the size of an office desk and are usually found in banks and offices. They are becoming less popular as microcomputers improve.

Microcomputers, commonly known as micros, are the smallest and least powerful. They are about the size of a typewriter. They can handle smaller amounts of information at a time and are slower than the other two types. They are ideal for use as home computers and are also used in education and business.

More powerful microcomputers are gradually being produced; therefore, they are becoming the most commonly used type of computers.

A computer can do very little until it is given some information. This is known as the input and usually consists of a program and some data.

A program is a set of instructions, written in a special computer language, telling the computer what operations and processes have to be carried out and in what order they should be done. Data, however, is the particular information that has to be processed by the computer, *e.g*. numbers, names, measurements. Data brought out of the computer is known as the output.

PROGRAM Add two numbers then display the result.

OUTPUT DATA 7

INPUT DATA 3, 4

EXAMPLE: A computer calculating 3 + 4 = 7 uses the following program and data:

«When a program is run, i.e. put into operation, the computer executes the program step by step to process the data. The same program can be used with different sets of data.

Information in the form of programs and data is called software, but the pieces of equipment making up the computer system are known as hardware.

The most important item of hardware is the CPU (Central Processing Unit). This is the electronic unit at the center of the computer system. It contains the processor and the main memory The processor is the brain of the computer. It does all the processing and controls all the other devices in the computer system The main memory is the part of the computer where programs and data being used by the processor can be stored. However, it only stores information while the computer is switched on and it has a limited capacity.

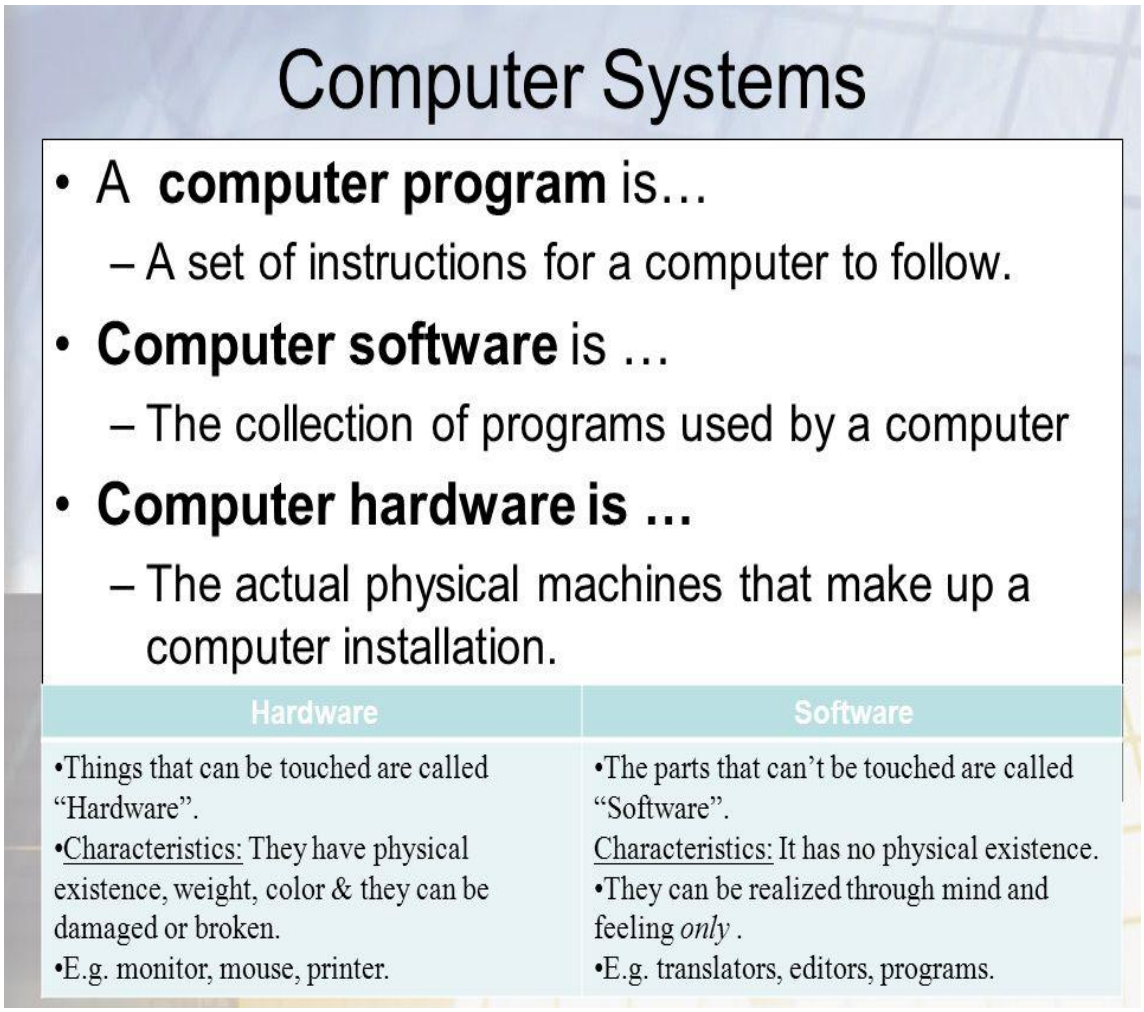
All the other devices in the computer system, which can be connected to the CPU, are known as peripherals. These include input devices, output devices and storage devices.

An input device is a peripheral, which enables information to be fed into the computer. The most commonly used input device is a keyboard, similar to a typewriter keyboard.

An output device is a peripheral, which enables information to be brought out of the computer, usually to display the processed data. The most commonly used output device is a specially adapted television known as a monitor or VDU (Visual Display Unit). Another common output device is a printer. This prints the output of the CPU onto paper.

A storage device is a peripheral used for the permanent storage of information. It has a much greater capacity than the main memory and commonly uses magnetic tape or magnetic disks as the storage medium.

These are the main pieces of hardware of any computer system whether a small "micro" or a large mainframe system.



EXERCISES

I. Answer the following questions:

1. What type of computer is most suitable for home use?
2. What is a program?
3. What are the functions of main memory, input device, storage device?
4. What is data?
5. What are the functions of processor, output device, monitor?

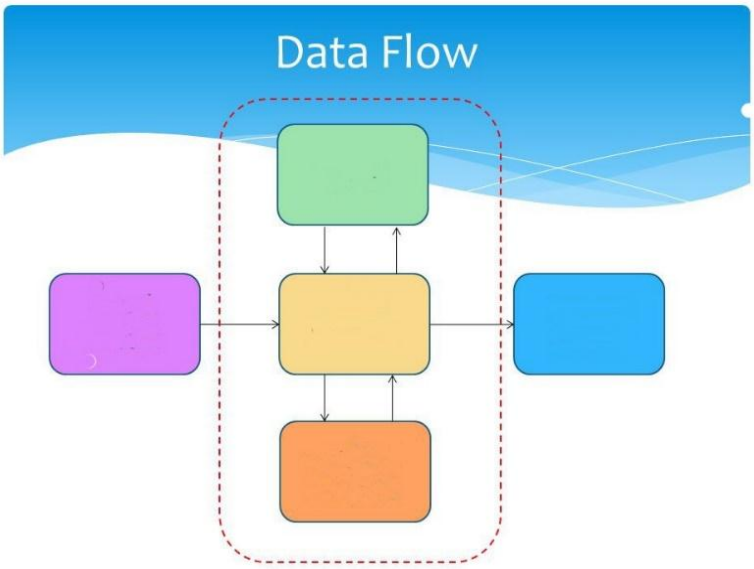
II. Match each component in column A with its function in column B:

A	B
1. Storage device 2. Input device 3. Output device 4. Main memory 5. Processor	a. It displays the processed data b. It holds the programs and data being used by the processor c. It does all the processing and controls the peripherals d. It allows data to be entered e. It provides permanent storage for programs and data

III. Complete the table:

	Mainframe	Minicomputer	Microcomputer
Size			
Power			
Use			

IV. Label the diagram of a computer system using these terms:



1.Storage device

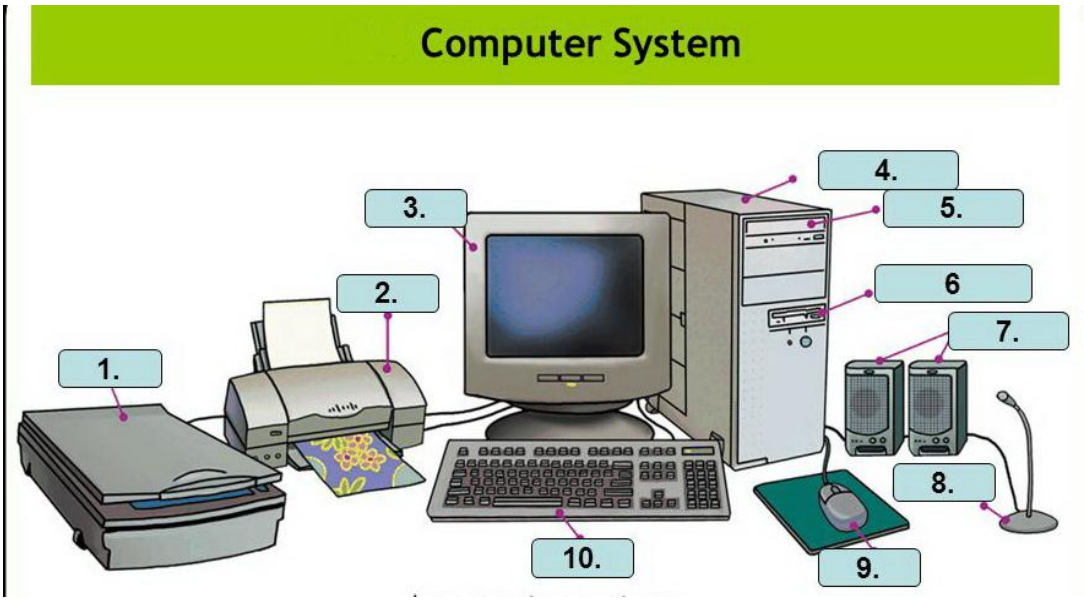
2.Processor

3.Output device

4.Input device

5.Main memory

V. Name each component and write down its function



1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

10._____

Choose the right variant

authenticate, *v* O A: to fade. B: complicate. C: confirm. D: test.

emoticon, *n* O A: robot. B: radiation. C: trick. D: illustration.

download, *v* O A: to copy. B: scramble. C: erase.D: belittle.

cursor, *n* O A: coarse speaker. B: indicator. C: moneychanger. D: technician.

cracker, *n* O A: fanatic. B: intruder. C: burglar. D: expert.

compress, *v* O A: to shrink. B: understand. C: fix. D: soften.

browser, *n* O software that allows you to A: explore the Internet. B: eavesdrop. C: send a fax. D: save a file.

boot, *v* OA: to fail gradually. B: enlarge. C: adjust. D: start up.

gigabyte, *n* O A: sudden shutdown. B: unit of storage. C: wide gap. D: high pressure.

glitch, *n* O A: flash. B: excitement. C: error. D: stroke of luck.

pixel, *n* O A: picture element. B: programming oddity. C: brief blur. D: long delay.

network, *n* O A: TV channel. B: digital design. C: system of computers. D: filter.

modem, *n* O A: digital code. B: keyboard. C: visual display. D: connecting device.

log on, *v* O A: to pile. B: gain access. C: waste time.

link, *n* O A: missing piece. B: space station. C: related site. D: warning signal.

hit, *n* O A: accident. B: stumbling block. C: unit of measurement. D: visit.

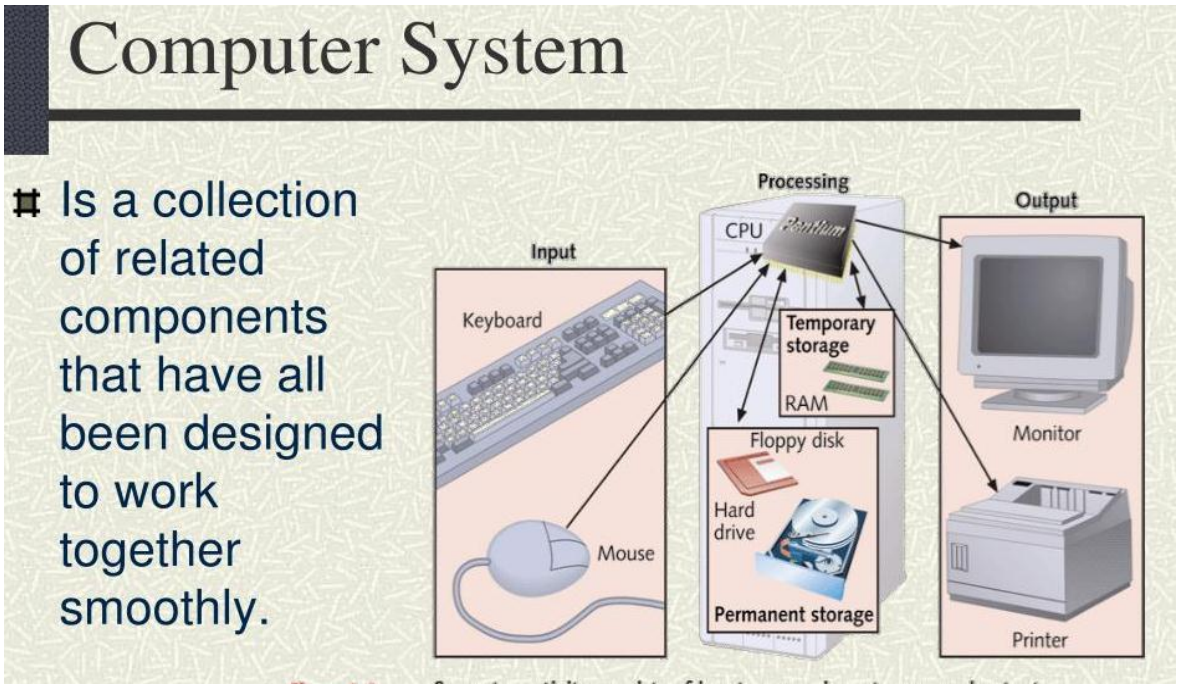
scanner, *n* O machine that A: reproduces images. B: translates files. C: searches a document. D: adds color.

virus, *n* O A: flaw. B: poison. C: fatigue. D: infection.

shareware, *n* O A: hand-me-down clothing. B: free hardware. C: relic. D: trial software.

server, *n* O A: central computer. B: speed control. C: power supply. D: trouble-shooter.

PART 3. COMPUTER HARDWARE



Study the vocabulary and learn the words

Keyboard клавиатура

Mouse мышь

to load загружать

Instructionкоманда

Error message сообщение об ошибки

Input ввод

Output	вывод информации
Button	кнопка
Memory	память
To create	создавать
Softcopy	мягкая копия, изображение на экране
Hardcopy	твердая копия, машинная (печатная)
to attach	подсоединяться, подключать

Read and translate the text 2

What is the hardware?

The devices composing a computer system is called the hardware.

It can be divided into 4 categories:

- storage hardware.
- processing hardware.

- output hardware.
- input hardware.

- ***Storage hardware***
- The purpose of storage hardware is to store computer instructions and date hardware.
- There are two types of output; soft copy and hard copy. Soft copy is information that is seen on a television-like screen, of monitor, attached to most computers. It is temporary; as soon as the monitor is turned off or new information is required, the old information vanishes. Hard copy is output printed in a tangible form such as on paper. It can be read without using the computer and can be conveniently carried around, written on, or passed to other readers.

Processing hardware

Processing hardware directs the execution of software instructions in the computer. The most common components of processing hardware are the central processing unit and main memory.

The central processing unit (CPU) is the brain of the computer. It reads and interprets software instructions and coordinates the processing.

Memory is the component of the computer in which information is stored. There are two types of computer memory: RAM and ROM.

RAM (random access memory) is the memory, used for creating, loading and running programs.

ROM (read only memory) is computer memory used to hold programmed instructions to the system.

The more memory you have in your computer, the more operations you can perform.

Input hardware

Input hardware collects data and converts them into a form suitable for computer processing. The most common input device is a keyboard. It looks

very much like a typewriter. The mouse is hand-held device connected to the computer by a small cable. As the mouse is rolled across the desktop, the cursor moves across the screen. When the cursor reaches the desired location, the user usually pushes a button on the mouse once or twice to give a command to the computer.

Review of computer systems

Hardware:

Computer Equipment

Software:

Computer Programs

Databases:

An organized collections of facts

Watch the video and check yourself!

I. Answer the following questions.

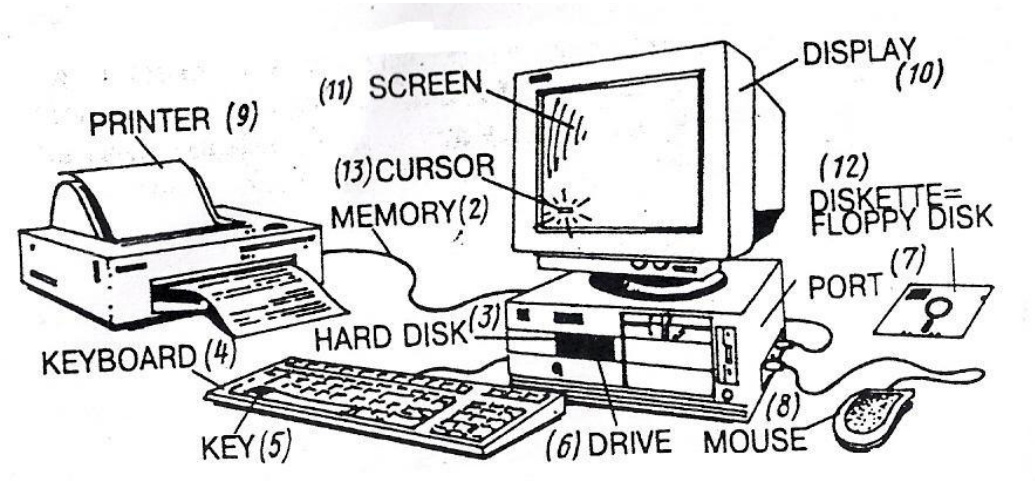
Questions and Answers

1. What is hardware?
2. What does input hardware do?
3. What is the most common input device?
4. What are the main components of processing hardware?
5. What is the purpose of storage hardware?
6. What do you think is a hard copy?

II. Agree or disagree with the statements.

1. Hard copy vanishes when we turn the computer off.
2. There are two types of input: soft copy and hard copy.
3. Processing occurs in the part of the computer called the mouse.
4. Information is stored in memory.
5. Hard copy can be read without using the computer.

III. Fill in the table. Use the picture.



№	English terms	
1		
2		Память
3	Hard disk	
4	Keyboard	
5		
6		Дисковод
7		Гнездо, порт
8	Mouse	
9	Print	
10	Display	
11		Экран
12		Дискета, гибкий диск
13	Cursor	

IV. Translate the sentences from Russian into English.

1. Одним из входных устройств является клавиатура.

2. К устройствам ввода относятся мышка, сканер, микрофон и многое другое.

3. Самая главная часть компьютера – центральный процессор.

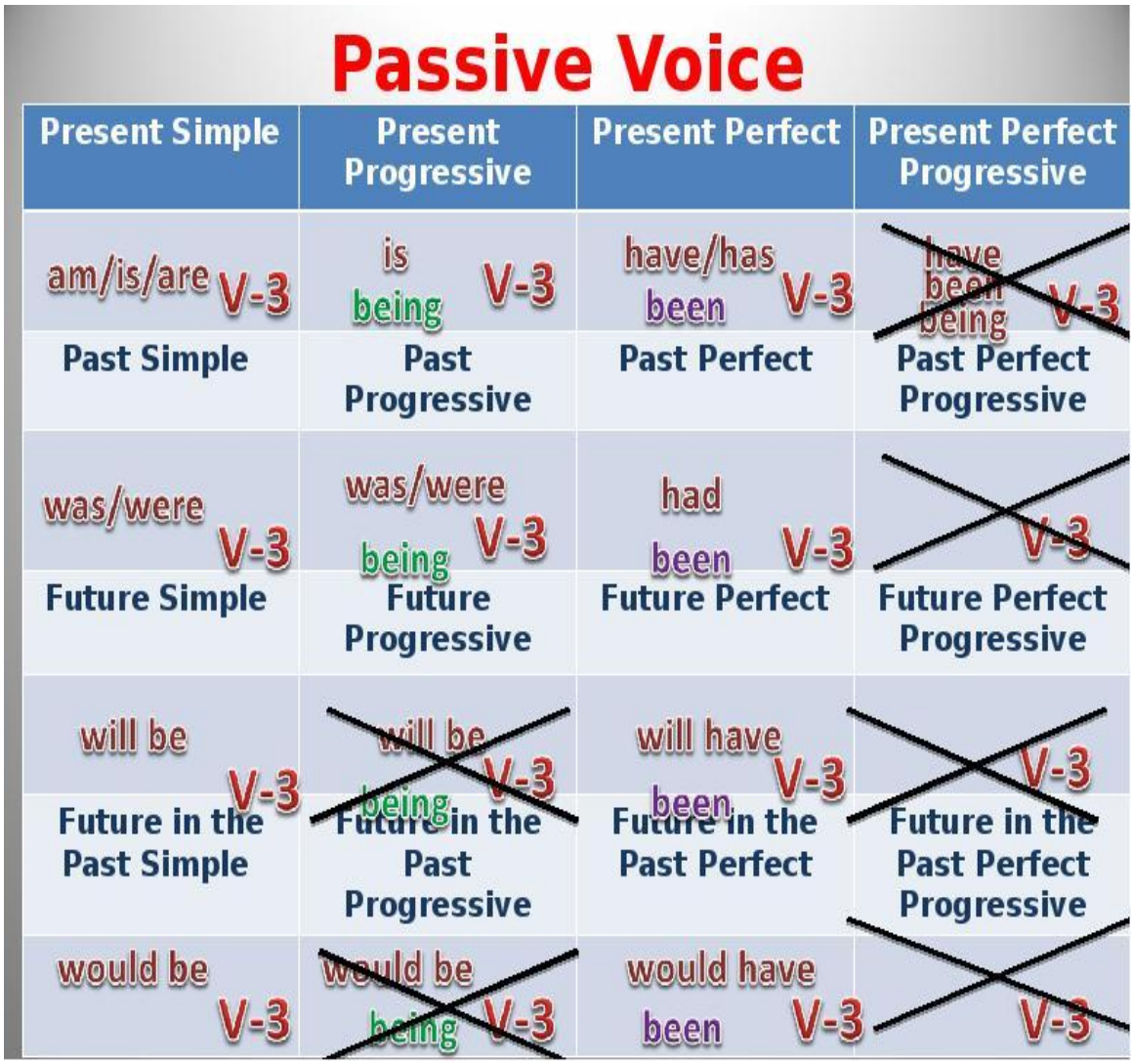
4. Память помогает компьютеру хранить информацию.

5. Чем больше память в компьютере, тем больше операций можно выполнять.

6. Существуют 2 типа входных устройств: мягкая копия и твердая копия.

Watch the video and check yourself!

Grammar: PassiveVoice



При спряжении глагола в страдательном залоге изменяется только глагол **to be**, смысловой глагол имеет во всех временах одну форму – Past Participle. Следовательно, время определяется формой, в котором стоит глагол в страдательном залоге, определяется формой , в которой стоит вспомогательный глагол **to be.**

Вспомогательный глагол ставится перед подлежащим при образовании вопросительной формы:

Am I asked?

Меня спрашивают?

Shall I be asked? Меня спросят?

Have I been asked?

Меня спросили?

When was the book written?

Когда была написана книга?

При образовании отрицательной формы Passive Voice частица *not* ставится после вспомогательного глагола:

I am not asked.

I shall not be asked.

С такими модальными глаголами как **have to, should, be to can (could), must, may (might), ought to,** страдательный залог образуется с помощью**to be**и Past Participle основного глагола.

This work must be finished today.

This report ought to be finished tonight.

That room cannot be used as a classroom.

(**see Appendix 6**)

1.) Rewrite these sentences in the Passive using Present Simple Tense:

1. Students write tests every month.
2. They make beautiful toys at this factory.
3. They export millions of cars from Japan every year.
4. Watchmakers repair watches.
5. The bill includes service.
6. They close the shop. at 8 p.m.
7. He translates articles every day.
8. She doesn't send telegrams before every holiday.

2.) Supply the Passive forms of the verbs in the box, using the Past Simple Tense: invent, plant, kill, write, discover, design, paint, build, name:

1. When _____ America_____ ?
2. Five fruit-trees _____ in our garden last year.
3. The picture Mona Liza_____ by Leonardo da Vinci.

4. Marat _____ in his bath.

5. Radio _____ by A.Popov.

6. The first pyramid of Egypt _____around 3000 BC.

7. The Winter Palace _____by Rastrelli.

8. "War and Peace" _____by L.Tolstoy.

9. Rossi street _____after a famous Russian architect.

3.) Make the following sentences active:

1. Peripheral devices can be attached to the computer.

2. Computer instructions are also called programs.

3. This work is usually performed manually.

4. Computers are used to monitor environmental problems.

5. Today the lives of most of us are affected by a computer every day.

6. This program was damaged by a computer virus.

7. The 'crash behavior' of the airplane was determined by the scientists.

8. This monitor was designed by Dell Corp.

4.) Make the following sentences passive:

1. Hardware also includes peripheral devices.

2. Educators use computers in the classroom.

3. Scientists can build computer models of airplane crashes.

4. Today many businesses and organizations own computers.

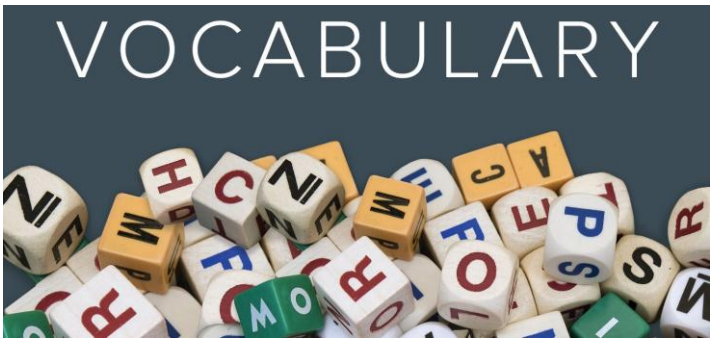
5. These organizations use computers for different purposes.

6. Computers can process data in a fraction of time.

7. Engineers use computers to design replacement for the damaged bone.

8. Computers are changing our life.

UNIT II. SOFTWARE. INTERNET TECHNOLOGY



network – (вычислительная, компьютерная) сеть

society – общество

to depend on – зависеть от чего-либо

application – приложение, прикладная программа

software – программное обеспечение; «софт»

productivity – производительность; продуктивность

to result in – кончаться, иметь результатом

privacy – индивидуальная сфера жизни

exotic curiosities – экзотическая редкость, диковинка

indispensable – незаменимый

business – (зд.) предприятие, фирма

origin – начало; происхождение

word processing program – программа обработки текстов

computer network – компьютерная сеть

to link – соединять, связывать

to share data – совместно использовать ресурс;

делиться данными

to transfer – передавать, переносить

Transmission Control Protocol (TCP) – протокол управления передачей

IP number (Internet Protocol Number) – IP-номер, IP-адрес

World Wide Web – всемирная паутина, сеть

interconnected – взаимосвязанный

to convert – преобразовывать

to transmit – передавать

Internet service provider – провайдер услуг Интернета

phone plugs – телефонные разъёмы

dial-up telephone connection – (коммутируемое) соединение по телефонной линии

digital subscriber line (DSL) – цифровая абонентская линия

cable broadband – кабельные широкополосные соединения

broadband technology – широкополосная технология; технология широкополосных передач

fiber-optic – волоконно-оптический

wireless – беспроводной

to compress data – сжимать (уплотнять) данные

to access the Internet – иметь доступ в Интернет

Wi-Fi (wireless fidelity) – беспроводная точность

radiowaves – радиоволны

appliances – бытовые электроприборы

to integrate – объединять

personal digital assistant (PDA) – персональный цифровой секретарь (помощник), (тип сверхлёгкого миниатюрного ПК)

To enable – давать возможность

power-line Internet – Интернет по линиям электропередач

intranet – интранет

customized Webpages – настроенные (заказные) Web –страницы

external source – внешний источник

extranet – экстранет

employee – служащий; работник

authorized user – авторизованный (полномочный)

пользователь

password – пароль

to gain access – получать доступ

a wide-areanetwork (WAN) – глобальная компьютерная сеть

a local area network (LAN) – локальная вычислительная сеть, ЛВС

in a close proximity – в тесной близости, вблизи

WLAN – беспроводная ЛВС

TEXT 1. INTERNET TECHNOLOGY

"We live in the Information Age; at no other time have data been so easily accessible and has information been so valuable"

John V. Thill, Chief Executive Officer

Communication Specialists of America

We live in a rapidly changing information society – that is, a society in which large groups of workers generate or depend on information to perform their jobs. The need for more and better information will only continue to grow. Information technology (IT) relates to processes and applications that create new methods to solve problems, perform tasks, and manage communication. Simply put, Information technology is the use of computers and software to manage information. Information technology plays a major role in the 21st century world; today, our economic productivity is based more on technology than on any other advance. IT has resulted in social issues related to privacy, intellectual property, and quality of life. Just a few decades ago computers were considered exotic curiosities, used only by scientists and the military. Today, they have become indispensable not only to businesses but to common people as well.

Who can imagine daily life without sending e-mails to friends, booking airline tickets over the Internet, or preparing reports with word processing program?

The Internet has profoundly changed the way people communicate, learn, do business, and find entertainment. Although many people believe the Internet began in the early 1990s, its origins can actually be traced to the late 1950s. Over the past decades, the network evolved from a system for government and university researchers into a tool used by millions around the globe for communication, information, entertainment, and e-business. Clearly, the Internet is here to stay.

«The Internet is an International computer Network made up of thousands of networks linked together. All these computers communicate with one another; they share data, resources, transfer information, etc. To do it they need to use the same language or protocol: TCP / IP (Transmission Control Protocol / Internet Protocol) and every computer is given an address or IP number. This number is a way to identify the computer on the Internet.

The Internet's most commonly used network for finding information is the World Wide Web (or more simply, the Web. The Web is a collection of interconnected Web sites or "pages" of text, graphics, audio and video within the Internet. To get on the Internet, you need a computer, a modem, and an Internet service provider (ISP). The modem (modulator-demodulator) converts the digital signals that can be transmitted over telephone lines. Internet service providers provide customers with a connection to the Internet through various phone plugs and cables. Today, connections to the Internet include simple telephone lines (a dial-up telephone connection) or faster digital subscriber lines (DSLs) and cable broadband that carry larger amounts of data at quicker transfer speeds. Broadband technology is a general term referring to higher speed Internet connections that deliver data, voice, and video material. Broadband technology combines digital, fiber-optic, and wireless network technologies that compress data and transmit them at blinding speeds. And with new wireless

technology, it is possible to access the Internet by using your laptop computer, cellular phone, and other wireless communications devices»

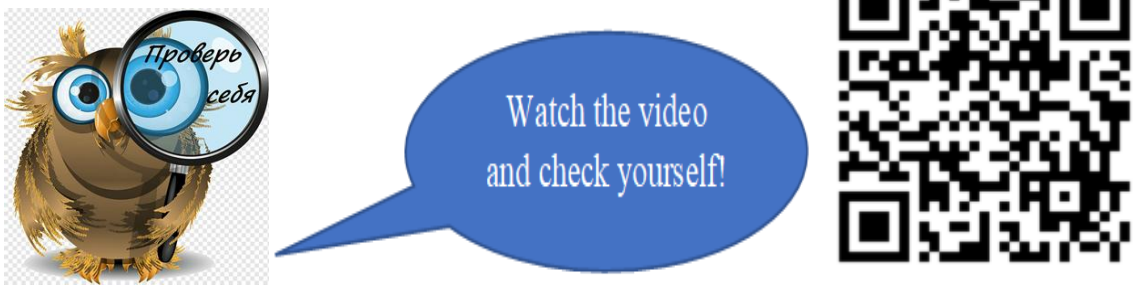
The most popular wireless network currently is Wi-Fi. Wi-Fi – short for wireless fidelity – is a wireless network that connects various devices and allows them to communicate with one another through radio waves. Wi-Fi allows high-speed wireless Internet connections when linked to a specially equipped modem. In the not-too-distant future, experts expect Wi-Fi to link all sorts of devices – not just computers, but lamps, stereos, appliances, and more – and to fully integrate the Internet into our lives. The basic equipment has changed drastically in the last few years. You may no longer need a computer to use the Internet. New Generation mobile phones and PDAs, personal digital assistants, also allow you to go online with wireless connections, without cables. Telephone lines are not essential either. Satellites orbiting the Earth enable your computer to send and receive Internet files. Finally, the power-line Internet, still under development, provides access via a power plug.

An intranet is a smaller version of the Internet for use within an organization. Using a series of customized Web pages, employees can quickly find information about their firm as well as connect to external sources. Intranets limit access only to employees or other authorized users. Generally, intranet sites are protected, and users must supply both a user name and a password to gain access to a company's intranet site. Some firms open up their intranets to other selected users through an extranet, a network of computers that permits selected companies and organizations to access the same information. An extranet allows users to share data, process orders, and manage information.

Both the Internet and intranets are examples of a computer network. Today, two basic types of networks affect the way people obtain data and information. A wide-area network (WAN) is a network that connects computers over a large geographic area. The world's most popular WAN is the Internet. A

local-area network (LAN) is a network that connects computers that are in close proximity to each other, such as an office building or a college campus.

Most networks are linked with cables or wires but new Wi-Fi, wireless fidelity, technologies allow the creation of WLANs, where cables or wires are replaced by radio waves.



Ex. 1. Read and translate the KEY TERMS

information technology, broadband technology, WI-Fi, Internet, Internet service providers, LAN, network, intranet, WAN, World Wide Web, extranet, WLAN

Ex. 2. Choose the correct alternative to complete each sentence:

1. Information technology relates to processes and applications that create new methods to send sounds and signals through space by means of electromagnetic waves / to solve problems, perform tasks, and manage communication.

2. Simply put, Information technology is the use of computers and software to manage the information society / information systems / information.

3. IT plays a major / secondary role in the 21st century world; our economic productivity is based less / more on technology than on any other advance.

4. The IP number is the abbreviation for Internet Provider number / Internet Protocol number / Intel Processor number.

5. Although most of us think that the Internet began in the early 1990s, its origins can actually be traced to the late1930s / the late 1940s / the late 1950s.

6. The Internet / the World Wide Web is the global information system that links many computer networks together.

7. A collection of interconnected files or pages of audio, visual, and text data within the Internet is known as Telnet / DSL / the Web.

8. The modem converts the different sounds / digital signals that can be transported / transmitted over telephone lines / TV cables.

9. Simple telephone lines carry smaller / larger amounts of data at quicker / slower transfer speeds than DSLs and cable broadband.

10. Digital, fiber-optic, and wireless network technology that compresses data and transmits them at blinding speeds is termed Wi-Fi / broadband technology / Bluetooth technology.

11. Wi-Fi – short for wired fidelity / wireless fidelity – is a wireless / wired network that connects various devices and allows them to communicate with one another through radio waves / telephone lines.

12. «The power-line Internet, still under development / which has been developed recently provides access via a power plug».

13. An intranet / extranet is a smaller version of the Internet for use within an organization.

14. An intranet / extranet is a network of computers that permits selected companies and organizations to access the same information and may allow communication about the information.

15. LANs / WANs are usually placed in the same building while LANs / WANs have no geographical limit and may connect computers on opposite sides of the world.

Ex. 3. Answer the questions

1. What is information technology? What role does information technology play in the 21st century world?

2. How has the evolution of the Internet affected the world?

3. What connections to the Internet are available nowadays?

3. Characterize broadband technology.

4. What is Wi-Fi?

5. What is an intranet? An extranet? How are they used?

6. Distinguish between WAN and LAN.

7. Explain what WLANS are.

Ex. 4. Choose the right word or word-combination and put it in the sentence. Translate the sentences into Russian.

World Wide Web, computer network, fiber-optic, IP number, broadband technology, Information, WAN, LANs, linking, protocol (TCP/IP), intranet, password, modem, connections, radio waves

1. A ---------- is a group of two or more computers linked together that allows users to share data and information.

2. An ---------- is a network of computers similar to the Internet that is available only to people inside an organization.

3. With the digital data compression and bigger “lanes” of ---------- , the same amount of information can travel faster from one destination to another.

4. Wi-Fi allows high-speed wireless connections when linked to a specially equipped ---------- .

5. In the early 1990s, a British man called Tim Berners-Lee invented ---------- . With ---------- it was much easier to find information on the Internet, and to

move from one part of the Internet to another. (The same word-combination is used twice).

6. Information technology has improved global access by ---------- people in business through telecommunications.

7. Satellites permit instant visual and electronic voice ---------- almost anywhere in the world.

8. ---------- is a way to identify the computer on the Internet.

9. ---------- is data presented in a form that is useful for a specific purpose.

10. Many companies connect their offices and buildings by creating ---------- , computer networks that connect computers within limited areas, such as a building or several buildings near one another.

11. Optical networks are one of the newest broadband technologies. They convert information into tiny bits of light that are transmitted over ---------- cables made of glass.

12. A ---------- is a network that connects computers over a large geographic area, such as a city, a state, or even the world.

13. A ---------- is a secret code used to control access to a network system.

14. Wi-Fi sends Web pages and other information to your laptop computer or other electronic device using ---------- .

15. Computers need to use the same ---------- to communicate with each other.

Ex. 5. Find in the text English equivalents of the word-combinations.

1. быстро меняющееся информационное общество; 2. зависеть от информации; 3. потребность в большей и лучшей информации; 4. решать проблемы; 5. выполнять задачи; 6. управлять (владеть) информацией; 7. в мире XXI века; 8. социальные вопросы; 9. Стать незаменимы-ми не только для предприятий, но и для обычных людей; 10. за последние десятилетия; 11. составленный из тысячи сетей, связанных вместе; 12. использовать

одинаковый язык или протокол; 13. наиболее широко используемая сеть для поиска информации; 14. собрание взаимосвязанных веб-сайтов; 15. провайдеры услуг Интернета; 16. преобразовывать цифровые сигналы; 17. подключение к Интернету через различные телефонные разъёмы и кабели; 18. абонентские цифровые линии; 19. при более быстрых скоростях передачи; 20. широкополосная технология; 21. цифровая, волоконно-оптическая и беспроводная технологии; 22. получать доступ в Интернет; 23. беспроводная сеть; 24. различные устройства; 25. основное оборудование; 26. Интернет по электросетям; 27. всё ещё в стадии разработки; 28. в пределах (внутри) организации; 29. внешние источники; 30. ограничивать доступ 31. авторизованные пользователи; 32. совместно использовать данные; 33. самая популярная в мире глобальная компьютерная сеть.

Ex. 6. Match the verbs on the left with the prepositions and phrases on the right.

1. to provide	a) our life without sending e-mails
2. to depend	b) customers with a connection to the Internet
3. to play	c) the way people obtain data and information
4. to result	d) the Internet by using a mobile phone
5. to transmit	e) the computer on the Internet
6. to share	f) on advances in technology
7. to convert	g) a major role in the 21st century world
8. to imagine	h) information and resources through an extranet

9. to communicate	i) to the area of information technology
10. to limit	j) with each other through radio waves
11. to affect	k) data over DSLs and fiber-optic cables
12. to identify	l) the digital signals into the analog audio signals
13. to access	m) access only to authorized users
14. to relate	n) all sorts of devices together
15. to link	o) in social issues

Ex.7. Read and translate the text to perform the tasks given below the text.

Text 2.

THE WORLD WIDE WEB

«The World Wide Web, Web or WWW is a network of documents that works in a hypertext (гипертекст) environment, i.e. using text that contains links, hyperlinks (гиперссылка) to other documents.

The files, web pages, are stored in computers, which act as servers. Your computer, the client, uses a web browser, a special program to access and download them. The web pages are organized in websites, groups of pages located on the Web, maintained by a webmaster, the manager of a website.

The Web enables you to post and access all sorts of interactive multimedia information and has become a real information highway. (информационная магистраль)

To surf (путешествовать по Интернету) or navigate the Web, access and retrieve web pages or websites, you need a computer with an Internet connection and a web browser. After you have launched it, you must type the website address or URL (Uniform Resource Locator). (идентификатор информ. ресурса)

To find interesting sites you can use search engines (поисковый механизм), where the website information is compiled by spiders, computer-robot programs that collect information from sites by using keywords, or through web indexes, subject directories (каталоги) that are selected by people and organized into hierarchical subject categories. Some web portals – websites that offer all types of services, e.g. email, forums, search engines, etc. – are also good starting points.

The most relevant website addresses can be stored in your computer using the bookmarks (закладки) or favourites function in your browser. Websites usually have a beginning page or home page. From this starting point you can navigate by clicking your mouse on hyperlinks in texts or images».

Ex. 1. Solve the clues and complete the puzzle with words from the text.

1. The WWW is also called the information ……. .
2. A link in a web page.
3. A website that offers a variety of services.
4. The first page of a website is the ……. page.
5. A person who keeps a blog.
6. The manager of a web page is its web ……. .
7. An animal closely linked to the Web.
8. Another word for directory.

9. Another word for bookmark.

The hidden word is …….. , text with links.

Ex. 2. Complete these instructions about how to navigate with the words in the box.

"Client, web page, surf web, browser search, engine, web server, website, URL."

1 Start up your computer and connect to the Internet.

2 Open your ..... …… .

3 Type the …… to access a website.

4 Your web browser sends the request to the correct ..... …… .

5 The server looks for the document and sends it to the …… computer.

6 Your web browser displays the selected ..... …… on the screen.

7 From the home page of the ..... you can ……. to other pages by clicking on hyperlinks.

8 If you want to find more websites, use a ..... …….. .

Ex. 3. Read the text and complete the text with words from the box.

A Digital Era

Computers have changed the way we do everyday things, such as working, shopping and looking for information. We (1) …… houses with the help of PCs; we buy books or make flight reservations on the (2) …… ; we use gadgets that spring to life the instant they are switched on, for example the mobile phone, the music player, or the car ignition, all of which use (3) …… . Many people now work at home, and they communicate with their office by computer and telephone. This is called "teleworking".

With the appropriate hardware and software, a PC can do almost anything you ask. It's a magical typewriter that allows you to type and (4) …….. any sort of document. It's a calculating machine that makes (5) …… calculations. It's a filing cabinet that manages large collections of data. It's a personal communicator that lets you interact with friends. It's a small lab that helps you edit photos and movies. And if you like (6) …… entertainment, you can also use it to relax with games.

Ex. 4. Match the words in the box (ex.5) with the following definitions.

1. tiny pieces of silicon containing complex electronic circuits (схемы)
2. to make or draw plans for something
3. relating to money or how money is managed
4. involving the use of electric current in devices such as TV sets or computers
5. the large system of connected computers around the world
6. to produce text and pictures using a printer

6. Living with computers.

Read the following abstract and do the task given below it.

People who have grown up with PCs and microchips are often called the digital generation. This is how some people answered when questioned about the use of computers in their lives.

1. "I have a GPS, Global Positioning System, fitted in my car. With this navigation system I never get lost. And the DVD recorder is perfect for my children's entertainment".

2. "I use an interactive whiteboard (интерактивная лекционная доска), like a large touchscreen monitor, at school. I find computers very useful in education."

3. Assistive technology (вспомогательные технологии), for people with disabilities, has helped me a lot. I can hardly see, so I use a screen reader, a program that reads aloud onscreen text, menus, and icons."

4. "This new HMD, head-mounted display, (шлем-дисплей) allows me to watch films, and enjoy virtual reality, the artificial environment of the latest video games."

5. "The upgraded wireless network at my university is great: we can connect our laptops, PDAs and Wi-Fi cell phones to the network anywhere in the campus. Communication is becoming easier and easier."

Ex. 5. Complete these sentences words from the text above.

1. The ..... …… is a piece of software that interfaces with your PC and allows you, via keyboard commands, to get any text information read to you in synthetic speech.

2. A …… …… …… , as popularized by virtual reality, lets the user immerse him/herself in a synthetically generated environment.

3. An …… …… is a touch-sensitive device where a special pen or your finger can act as a mouse.

4. Tony Adams is now the proud owner of a dark silver Vogue, complete with leather interior, …… navigation, and a …… …… with LCD TV screens.

Ex. 6. Speaking. The table below shows the dates of the events and their significance in the history of IT. Complete the gaps in the table with the appropriate events from the list below the table. Compare your answers with other students in your group. Describe the stages in the history of IT.

History of Information Technology

Year

Event

Significance

1836

The telegraph revolutionized human (tele)communications with Morse code, a series of dots and dashes used to communicate between humans

1858– 1866

The Transatlantic cable allowed direct instant (мгновенный) communication across the Atlantic Ocean

1876

The telephone created voice communication, and telephone exchanges provide the backbone (магистраль)) of Internet connections today

1957

Sputnik was the first artificial earth satellite and the start of global communications

1962– 1968

The Internet relies on packet switching networks (сети с коммутацией пакетов), which split data into tiny packets that may take different routes (маршруты) to a destination

1971

People communicate over the Internet with a program to send messages across a distributed network

1991

User-friendly interface to the World Wide Web is established with text-based, menu-driven interface to access Internet resources

1992

The term “surfing the Internet” is coined. (путешествие, перемещение по Интернету)

1995

Online dial-up systems (CompuServe, America Online, Prodigy) begin to provide Internet access

2000

Provides fast access to multimedia and large text files

2002

Mobile phones, handheld computers, and personal data assistants provide wireless access to the Internet

2004

Use of radio waves to send e-mail, Web pages, and other information through the air (Wi-Fi)

2006

Worldwide expansion of smart phones and Wi-Fi in developing countries.

Beginning of the Internet Transatlantic cable Advances in wireless Internet service providers advance USSR launches Sputnik Wireless expands globally World Wide Web established Telegraph Multimedia changes the face of the Internet Wireless technology expands Broadband connections to the Internet emerge Packet switching networks developed Telephone

2. COMPONENTS OF THE INTERNET

A) Read and translate the text.

The Internet consists of many systems that offer different facilities to users.

WWW, the World Wide Web, is a collection of files or pages containing links to other documents on the Net. It’s by far the most popular system. Most Internet services are now integrated on the Web.

Email, or electronic mail, for the exchange of messages and attached files.

Mailing lists (or list servs) (списки почтовой рассылки) based on programs that send messages on a certain topic to all the computers whose users have subscribed to the list.

Chat and instant messaging, for real-time conversations; you type your messages on the keyboard.

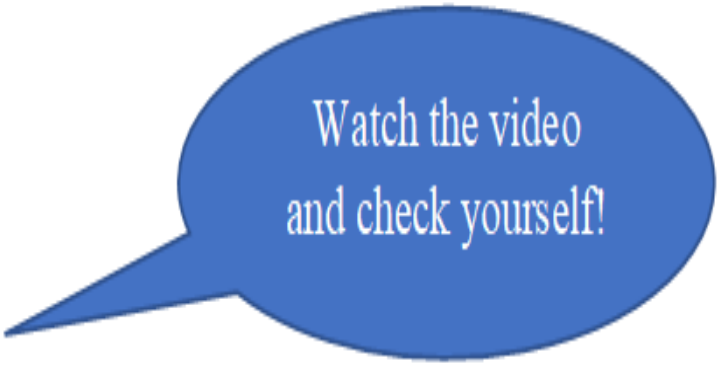
Internet telephone, a system that lets people make voice calls via the Internet.

Video conference, a system that allows the transmission of video and audio signals in real time so the participants can exchange data, talk and see one another on the screen.

File Transfer Protocol (FTP), used to transfer files between computers.

Newsgroups (тематическая [теле] конференция в Интернете), where people send, read and respond to public bulletin board (электронная доска объявлений) messages stored on a central computer.

TELNET, a program that enables a computer to function as a terminal working from a remote computer and so use online databases or library catalogs.



Answer the question:

What Internet system from the text should these people use?

1. “I like receiving daily updates and headlines from newspapers on my computer.”

2. “I’m doing some research and need computer access to the University library.”

3. “I’d like to avoid flying to Japan to attend the meeting but I want to see what’s going on there.”

4. “I want to read people’s opinions about environmental issues and express my views.”

5. “I have designed a web page and want to transfer the data to my reserved web space.”

6. “I’d like to check my students’ draft essays on my computer and send them back with my suggestions.”

7. “I don’t want to spend too much money on international phone calls but I love hearing his voice.”

8. “I live in a small village where there are no other teenagers. I wish I had the chance to meet and chat with friends.”

3. THE FUTURE OF ICT

(Information and Communication Technology)

Study these statements about the future trends in ICT and try to predict the year by which each event may happen.

Computers will be embedded or hidden, in a variety of items. For example, we’ll have wearable computers that will be embedded in a belt or a piece of jewellery, etc. ICT devices will be mobile and multimedia: we’ll watch mobile TV programs on our phones, which will also access the Internet and work as a mobile office. In the near future we’ll be able to swim in the

immersive Internet, a technology that will change the two-dimensional world of the Internet into a 3-D experience with three-dimensional sound and images and even the sense of touch. User interfaces, the systems that facilitate communication between people and computers, will resemble human communication. There will be gesture interfaces based on facial-hand recognition systems. Computer chips can be injected under the skin: RFID, radio-frequency identification tags (чип-передатчик), might be used to track or identify people or to store information, such as medical data, although there are concerns about privacy and personal safety. By the year 2040 there might be intelligent robots, machines that will be able to think creatively. The processing power of computers may have reached 1,000,000,000 MIPS (millions of instructions per second), the estimated speed of human thought.

DID YOU KNOW?

Our society has developed technological dependence. The average young adult will spend 9 years 11 months on the Internet during his or her life. The average Internet user will send 304,200 electronic messages during his or her lifetime. Men are still slightly more intense Internet users than women. Cybercrime, crime committed with the help of computers is creating serious problems.

Ex. 1. Choose the correct option.

1. People (to use) the Internet mainly for communication, information, entertainment, and e-business.

a) use b) are using c) used

2. Wi-Fi (to send) Web pages and other information to your computer or other electronic device using radio waves.

a) send b) sent c) has sent

3. Tom (to play) a computer game at the moment.

a) plays b) is playing c) has played

4. The world (to change). Things never stay the same.

a) changes b) changed c) is changing

5. We (to discuss) this problem at the next lesson.

a) discuss) b) will have discussed c) will discuss

6. The second half of the 20th century (to see) the start of the Computer Age.

a) saw b) was seeing c) had seen

7. Apple (to launch) its first iPhone in 2007.

a) has launched b) had launched c) launched

8. Apple (to produce) iPhones since 2007.

a) produces b) produced c) has produced

9. I (to study) the basics of computer engineering for 2 years

a) study b) studied c) have been studying

10. The students (just to finish) writing the test.

a) just finished b) have just finished) c) had just finished

11. When I came to the class the students (to write) the test.

a) were writing b) wrote c) have written

12. Yesterday from 10.00 till 10.30 I (to send) emails to my friends.

a) send b) sent c) was sending

13. On my way to the office I remembered that I (to leave) my notebook at home.

a) left b) have left c) had left

14. I received an iPod as a present on my birthday. I (never to have) an iPod before.

a) have never had b) had never had c) never had

15. Perhaps a different kind of computer (to appear) in the future.

a) appears b) will appear c) is appearing

Ex. 2. Use the verbs in brackets in the correct tense-forms.

1. Today, a great number of Americans (to have) high speed Internet access at home.

2. Tom is busy now. He (to work) on his computer.

3. Next year Apple (to produce) the new generation iPhones.

4. At 8 o'clock yesterday evening I (to surf) the Internet.

5. When I came to the class, the students (to discuss) the advantages of broadband technology. .

6. In the 1820s, a British mathematician called Charles Babbage (to invent) a machine that (to do) very difficult calculations automatically. He (to call) his machine a Difference Engine.

7. Over the last few decades, information technology (to change) the way people communicate, learn, do business, and find entertainment.

8. E-mail (to be) fast, easy to use, and convenient.

9. – Where is Peter?

– He (to talk) on his mobile phone.

10. At first most computers (to use) a dial-up telephone connection that (to work) through standard telephone lines; nowadays, a broadband connection (to become) more popular.

11. For many years people (to use) simple typewriters for typing texts and abacuses (счёты) for doing calculations before computers began to appear in offices and homes.

12. At the moment, scientists (to work) on artificial Intelligence (искусственный интеллект) which imitates the brain.

13. Most people think that computers (to do) many different jobs in the world of the future.

14. We (to solve) this problem by the beginning of the next year.

15. He felt very tired at 5.30 because he (to do) a lot of things by that time.

16. She (to learn) English for three years before she could speak fluently.

17. Since the beginning of the year the company (to produce) the new generation computers.

18. In 1975 Bill Gates and his friend Paul Allen (to write) a computer program for a new personal computer, the Altair 8800. They (to show) it to Ed Roberts, the man who (to invent) the Altair 8800.

19. Could you help me? I (to try) to translate a letter from a German client and I don’t know what this word (to mean).

20. Personal computers probably (not to get) much smaller. They will be too difficult to use and too easy to lose.

Ex. 3.**Make questions from the words in brackets.**

1. (always/ live/ in that city)_____ _____
2. (ever/ be/ Taxes)_____
3. (ever/ ride/ bike) *Have you ever ridden a bike?*
4. (ever/ run/ marathon)_____ _____
5. (ever/ read/ famous writer)_____ _____
6. (most beautiful city/ ever/ visit) What_____

Ex. 4**. Complete these sentences using** *today/ this year/ this term* **etc**.

1. I saw Mary last week but *I haven't seen him today.*
2. I read a newspaper yesterday but I_____
3. Last month the company made a profit but this month_____
4. Tracy worked hard at college last term but_____
5. It rained a lot last autumn but_____
6. Our handball team won a lot of games last year but we_____

ASPECT		SIMPLE	PROGRESSIVE	PERFECT	PERFECT PROGRESSIVE
MEANING		*a common aspect*	*a process*	*priority*	*priority + process*
		When?	**At what time?**	**By what time?**	**Since what time? How long?**
Period of time		*usually, often, always, seldom, every day (week, month, year)*	*now, at the moment*	*ever, never, just, already, not...yet, by 3 p.m.*	*since 3 p.m., for a long time, for a month...*
Present	+	**V, Vs**	**am / is / are + Ving**	**have / has + Ved, V_3**	**have / has + been + Ving**
	?	do, does...V	inversion	inversion	inversion
	–	do, does + not + V	am, is, are + not + Ving	have, has + not + Ved, V_3	have, has + not + been + Ving
Period of time		*yesterday, last week (month, year), long ago*	*yesterday at 3 p.m., yesterday from 6 till 7, when you came...*	*yesterday by 3p.m., before some time in the past...*	*yesterday since 3 p.m., for some time in the past*
Past	+	**Ved, V_2**	**was / were + Ving**	**had + Ved, V_3**	**had + been + Ving**
	?	did...V	inversion	inversion	inversion
	–	did + not + V	was, were + not + Ving	had + not + Ved, V_3	had + not + been + Ving
Period of time		*tomorrow, next week (month, year)*	*tomorrow at 3 p.m., tomorrow from 6 till 7, when you come*	*tomorrow by 3p.m., by some time in the future*	*tomorrow since 3p.m., for some time in the future*
Future	+	**will + V**	**will + be + Ving**	**will + have + Ved, V_3**	**will + have + been + Ving**
	?	inversion	inversion	inversion	inversion
	–	won't + V	won't + be +Ving	won't + have + Ved, V_3	won't + have + been + Ving

Ex. 5. Supply either the Present Simple or the Present Perfect in the following sentences.

1. I can't speak about the book. I (not read)_____ _____ it yet.

2. Every Monday I (wind up)_____ my clock at 8 a.m in the morning.

3. It is Friday. ... you (see)_____ him this week?

4. Students usually (buy)_____ books at the House of Books.

5. It's a pity, but I (not buy)____ _____ this dictionary yet.

6. As a rule we (do)___ _____ many exercises in class.

7. Re (tell)___ _____ this joke many times.

8. Something (go)__ _____ wrong with my watch.

9. I already (translate)_____ _____ these sentences into French.

10. They (have)___ _____ their English many hours a week.

11. She (work)__ _____ much and usually (get) many' good marks.

12. We (buy)___ _____ a new TV set this year.

Ex. 6. Rewrite the sentences using the Present Perfect or the Past Simple:

Examples: I am writing a letter to my cousin (already. yesterday).

I have already written a letter to my cousin.

I wrote a letter to my cousin yesterday.

1. The waitress is bringing our tea. (a few minutes ago. not yet)

_____

2. The bell is ringing, (just; some minutes ago)

_____

3. He is going to London in a few days. (already; last week)

_____

4. The girls are playing violins in the concert hall now. (yesterday; many times)_____

5. My mother is reading a new novel. (this month; last year)

_____

6. Students are cleaning their classrooms. (already, last Saturday)

_____

7. The teacher is explaining a new rule. (Just; at the previous lesson)

_____

8. Ann is doing her homework now. (just; on Friday)

_____

9. They are discussing this problem again. (many times; a few days ago)

_____

10. Granny is making a birthday cake. (just, yesterday)

_____

11. The birds are flying to the South, (already; at the end of August)

_____

1 2. The train is coming. (just; an hour ago)

_____

13. Who is your friend speaking to? (yesterday, just)

_____

14. We are writing the words of Lesson 7. (Already, at the last lesson)

_____

Ex. 7. **Make questions from the words in brackets.**

7. (always/ live/ in that city)_____ _____
8. (ever/ be/ Taxes)_____
9. (ever/ ride/ bike) *Have you ever ridden a bike?*
10. (ever/ run/ marathon)_____ _____
11. (ever/ read/ famous writer)_____ _____
12. (most beautiful city/ ever/ visit) What_____

Ex. 8**. Complete these sentences using** *today/ this year/ this term* **etc**.

1. I saw Mary last week but *I haven't seen him today.*
2. I read a newspaper yesterday but I_____
3. Last month the company made a profit but this month_____
4. Tracy worked hard at college last term but_____
5. It rained a lot last autumn but_____
6. Our handball team won a lot of games last year but we_____

Ex. 9**. Supply either the Present Simple or the Present Perfect in the following sentences.**

1. I can't speak about the book. I (not read)_____ _____ it yet.
2. Every Monday I (wind up)_____ my clock at 8 a.m in the morning.
3. It is Friday. ... you (see)_____ him this week?
4. Students usually (buy)_____ books at the House of Books.
5. It's a pity, but I (not buy)____ _____ this dictionary yet.
6. As a rule we (do)___ _____ many exercises in class.
7. Re (tell)___ _____ this joke many times.
8. Something (go)__ _____ wrong with my watch.
9. I already (translate)_____ _____ these sentences into French.
10. They (have)___ _____ their English many hours a week.
11. She (work)__ _____ much and usually (get) many' good marks.
12. We (buy)___ _____ a new TV set this year.

Ex. 10. **Rewrite the sentences using the Present Perfect or the Past Simple:**

Examples: I am writing a letter to my cousin (already. yesterday).

I have already written a letter to my cousin.

I wrote a letter to my cousin yesterday.

1. The waitress is bringing our tea. (a few minutes ago. not yet)

_____

2. The bell is ringing, (just; some minutes ago)

_____

3. He is going to London in a few days. (already; last week)

_____

4. The girls are playing violins in the concert hall now. (yesterday; many times)_____

5. My mother is reading a new novel. (this month; last year)

_____

6. Students are cleaning their classrooms. (already, last Saturday)

_____

7. The teacher is explaining a new rule. (Just; at the previous lesson)

_____

8. Ann is doing her homework now. (just; on Friday)

_____

9. They are discussing this problem again. (many times; a few days ago)

_____

10. Granny is making a birthday cake. (just, yesterday)

_____

11. The birds are flying to the South, (already; at the end of August)

_____

1 2. The train is coming. (just; an hour ago)_____

13. Who is your friend speaking to? (yesterday, just)

_____

14. We are writing the words of Lesson 7. (Already, at the last lesson)

_____

UNIT III. COMMUNICATION SYSTEMS.

COMPUTER NETWORK.

Types of Computer Systems

- **Mobile/Micro/Minicomputers**
  - Personal computing, workstation,network server.
  - Departmental and workgroup systems, network server, workstation.
- **Mainframes**
  - **Speed: MIPS million instructions per second**
    - 26 MIPS to about 17,801 MIPS
  - Enterprisewide systems
  - for organizations have to deal with huge amounts of data. Giga-record or tera-record files are not unusual.
  - Data mining and warehousing
- **Supercomputers**
  - Speed: Floating-point operations per second
    - 20 peta flops
  - Supercomputers are often purpose-built for one or a very few specific institutional tasks (E.g. Simulation and Modeling).
  - **Scientific calculations**
- **Networked computer systems**
  - **WAN, LAN, PAN**

Text 1. TYPES OF COMPUTER SYSTEMS

From mainframes to wearable computers

A mainframe is the most powerful type of computer. It can process and store large amounts of data. It supports multiple users at the same time and can support more simultaneous processes than a PC. The central system is a large server connected to hundreds of terminals over a network. Mainframes are used for large-scale computing purposes in banks, big companies, and universities.

A desktop PC has its own processing unit (CPU), monitor and keyboard. It is used as a personal computer in the home or as a workstation for group work. Typical examples are the IBM PC and the Apple Macintosh. It's designed to be placed on your desk. Some models have a vertical case called a tower

A laptop (also called a notebook PC) is a lightweight computer that you can transport easily. It can work as fast as a desktop PC, with similar processors, memory capacity, and disk drives, but it is portable and has a smaller screen. Modern notebooks have a TFT (Thin Film Transistor) screen that produces very sharp images.

Instead of a mouse, they have a touchpad built into the keyboard – a sensitive pad that you can touch to move the pointer on the screen.

They offer a lot of connectivity options: USB ports for connecting peripherals, slots for memory cards, etc. They come with battery packs, which let you use the computer when there are no electrical outlets available.

A tablet PC looks like a book, with an LCD screen on which you can write using a special digital pen. You can fold and rotate the screen 180 degrees. Your handwriting can be recognized and converted into editable text. You can also type at the detached keyboard or use voice recognition. It's mobile and versatile.

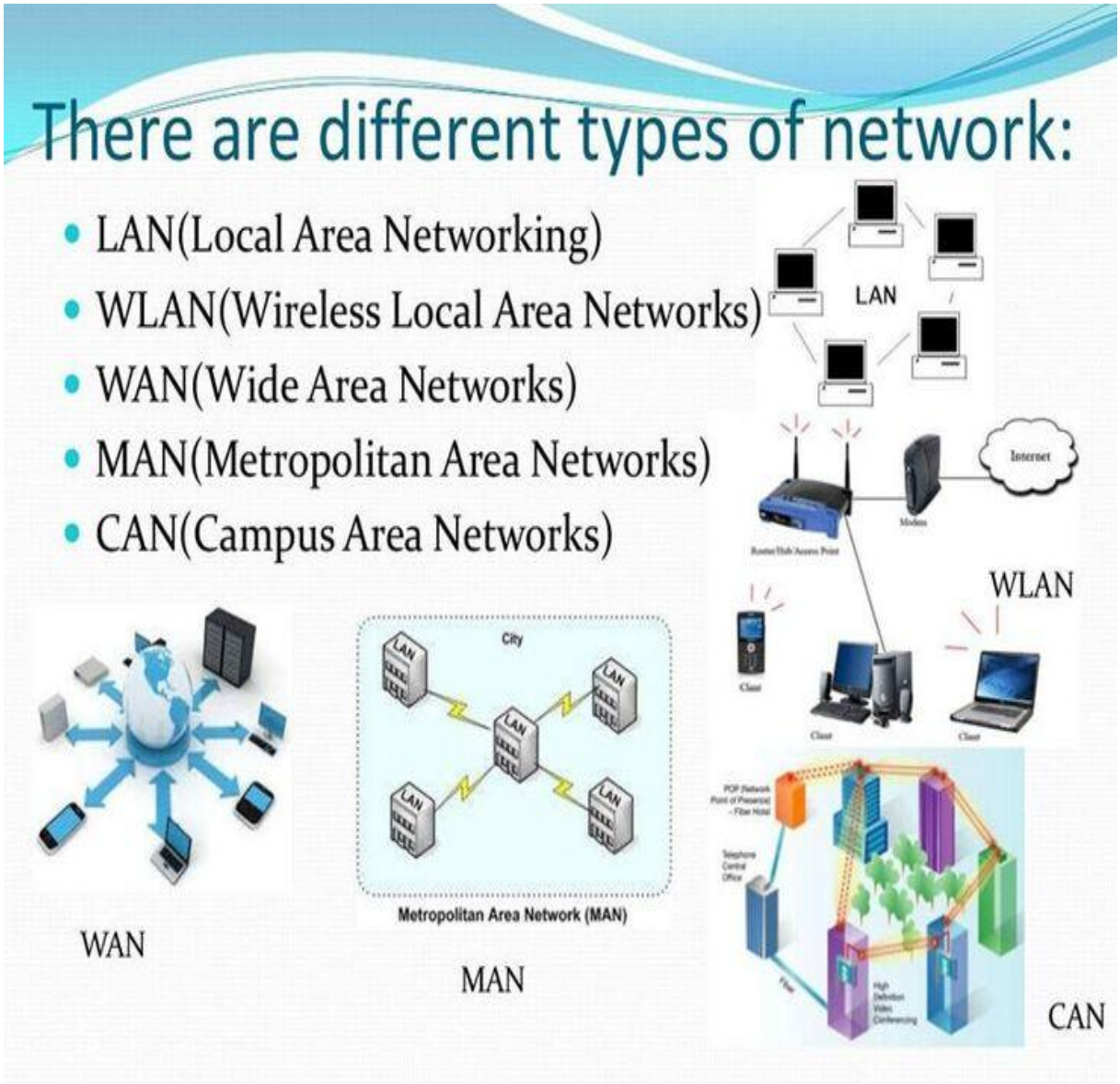
A personal digital assistant or PDA is a tiny computer which can be held in one hand. The term PDA refers to a wide variety of hand-held devices, palmtops, and pocket PCs.

For input, you type at a small keyboard or use a stylus – a special pen used with a touch screen to select items, draw pictures, etc. Some models incorporate handwriting recognition, which enables a PDA to recognize characters written by hand. Some PDAs recognize spoken words by using voice recognition software.

They can be used as mobile phones or as personal organizers for storing notes, reminders, and addresses. They also let you access the Internet via wireless technology, without cables.

A wearable computer runs on batteries and is worn on the user's body, e.g. on a belt, backpack, or vest; it is designed for mobile or hands-free operation. Some devices are equipped with a wireless modem, a small keyboard, and a screen; others are voice-activated and can access email or voice mail.

Ex1. Read and translate the following:



Ex2. Read this interview with Adam Hawkins, an IT manager, and complete it with words from the PDA section in the text above.

Interviewer: – What are the basic features of a PDA?

Adam: – Well, a typical PDA is a (1) …… device that runs on batteries and combines computing, phone and Net capabilities.

Interviewer: – And how do you enter information?

Adam: – For input, you use a (2) …… or pen to write and make selections on a (3) ……. ……. ; they also have buttons for launching programs. Some models have a small keyboard. They may have a (4) …….system that reacts to the user's voice.

Interviewer: – Do they need special software?

Adam: – Yes, most of them run on Windows Mobile. Palmtops supported by Palm Inc. use Palm OS. Pen-based systems include (5) ……. ……. , so you write on the screen and the computer recognizes your handwriting and inserts the appropriate letters.

Interviewer: – What sort of things can you do with a PDA?

Adam: – You can store personal information, take notes, draw diagrams and make calculations. Many PDAs can access the Net via (6) …….. technology.

Ex3. . In pairs decide what sort of computer is best for each of these users.

1. John Willis is a salesperson and he spends a lot of time visiting customers. He wants a computer to carry with him so he can access data about his customers and record his sales.

2. Mary Smith is a secretary in the office. She needs a computer to keep staff records and to keep a diary of appointments. She also needs a computer for writing letters.

3. The University of Arkansas needs a computer to look after its accounts, its network, the records of all students and staff, and to help with scientific research.

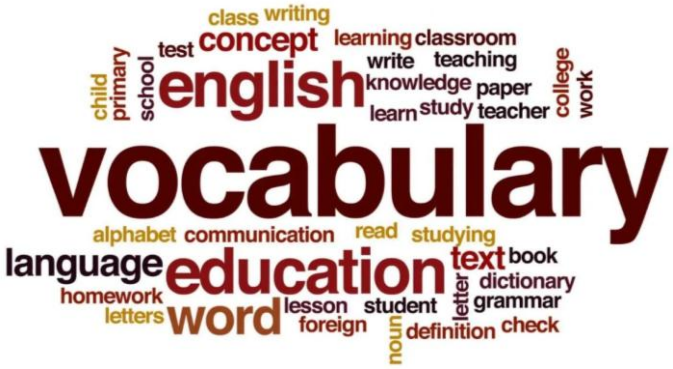
4. The James family want a computer for entertainment, writing letters, the Internet, and for calculating tax.

5. Peter Brawn is a businessperson and he must always keep in touch with clients while travelling. He needs a hand-held device that runs on batteries and combines computing, phone, and Net capabilities.

6. Kate is a college student and she has to use much paper for writing work at her classes. She wants a lightweight full-function PC to carry with her so she can write directly on the screen saving handwritten content in a digital format. She also wants the computer to provide sound, graphics and video.

7. Sam is a beginning mountain climber. In addition to the basic equipment Sam needs a portable voice-activated computer for hands-free operation.

Part 2. COMPUTER NETWORKS.



business assets – бизнес-активы; капитал; достояние деловой жизни

information security – информационная безопасность, обеспечение информационной безопасности

unauthorized user – несанкционированный; неполномочный пользователь

disclosure – раскрытие

disruption – срыв; нарушение

modification – модификация, видоизменение

inspection – инспекция: проверка

destruction – уничтожение, разрушение

threat – угроза

computer crime – компьютерная преступность

(преступление)

disaster – бедствие; авария; катастрофа

malicious intentions – вредоносные (преступные) намерения

cracker – “крэкер”; взломщик компьютерных систем

blackhat hacker – “чёрный” хакер

classified information = – засекреченная информация;

sensitive information секретные сведения

outsider – постороннее лицо

to alter data – изменять данные

inaccurate – неточный

misleading – вводящий в заблуждение; обманный

illegal transactions – незаконные сделки

illicit benefit – незаконная выгода

violation – нарушение; преступление

the Computer Emergency Response Team Center – координационный центр реагирования на чрезвычайные компьютерные происшествия (США)

to soar – резко возрастать

scam – надувательство, обман

fraud – мошенничество

phishing – фишинг (рассылка электронных сообщений по Интернету от имени солидных компаний с целью получения их личных данных)

piracy – компьютерное пиратство

copyrighted software – программы, охраняемые авторским
правом

vulnerable – уязвимый

to hack into – взламывать; проникать

to embarrass – приводить в замешательство

supposedly – предположительно

to post evidence – отправить доказательства

(to) break-in – взлом; взламывать

the U.S. Space and Naval
War Systems Command – командование военными
космическими и морскими системами (США)

competitor – конкурент

thief – вор

to raid – рейдерски захватывать; грабить

database – база данных

security breach – (зд) взлом системы безопасности

annually – ежегодно

estimated cost – подсчитанные затраты

system administrator – системный администратор

to implement – выполнять, осуществлять, проводить

to prevent – предотвращать, предупреждать

firewall – межсетевой защитный экран, брандмауэр

to log system use – регистрировать пользование системой

to log on with invalid password – входить в систему с недействительным паролем

encryption – шифрование

decryption – расшифровка

to encode = to encipher =

to scramble – шифровать, кодировать

cryptography – криптография

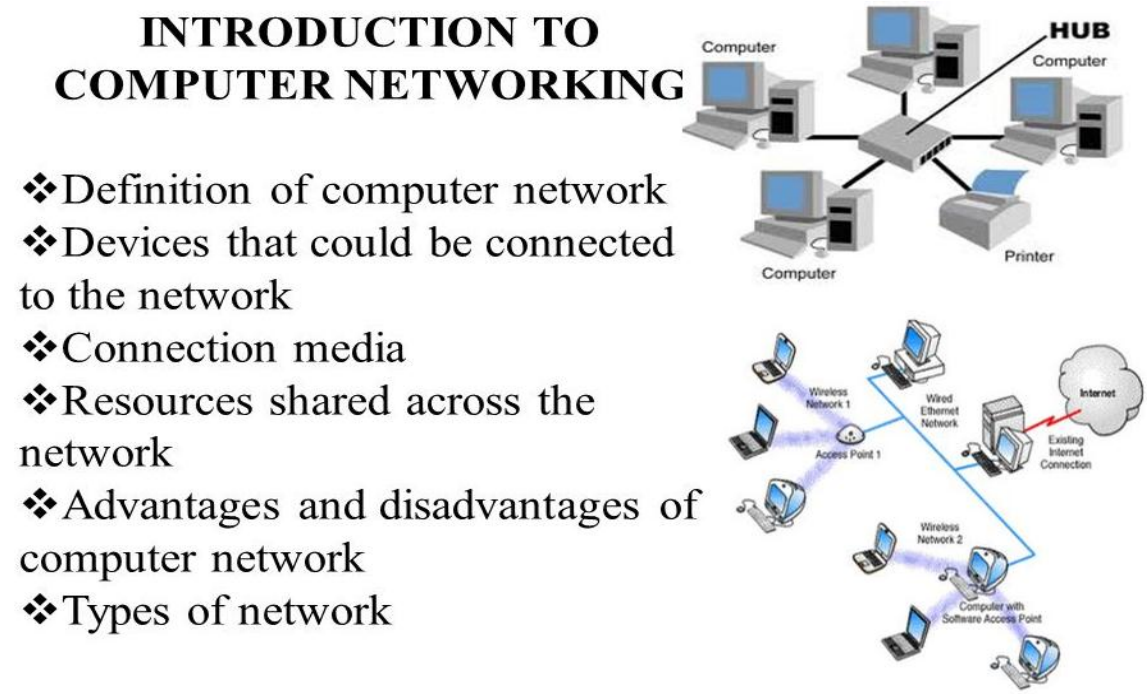
cryptographic key – криптографический ключ

available – доступный; готовый к использованию

intransit – в пути; в процессе передачи

elaborate – сложный; усовершенствованный

protective measures – меры защиты



As information systems become increasingly important business assets, they also become progressively harder to replace. When computers are connected to a network, a problem at any location can affect the entire work. Perhaps the most significant problem businesses face as a result of computer technology is information security. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. There are three important security threats that may damage information systems: computer crime, viruses, and disasters.

COMPUTER CRIME

Computers provide efficient ways for people to share information. But they may also allow people with more malicious intentions to access information. Or they may allow crackers, or black hat hackers – computer criminals who use technology to perform a variety of crimes – to gain access to classified information. Common computer crimes involve stealing or altering data in several ways: Employees or outsiders may change or invent data to produce inaccurate or misleading information. Employees or outsiders may modify computer programs to create false information or illegal transactions or to insert viruses. Unauthorized people can access computer systems for their own illicit benefit or knowledge or just to see if they can get it.

Computer crime is on the rise. The number of violations of Internet security as reported to the Computer Emergency Response Team Coordination Center, located on the Web at http://www.cert.org, has risen

sharply in recent years. In 1990, only six incidents were reported. Recently, the number of reported incidents soared to over 82,000. Of course, the statistics don’t include the number of incidents that were not reported, so the total is probably much higher.

Internet-based crimes include scam, email fraud to obtain money or valuables, and phishing, bank fraud, to get banking information such as

passwords of Internet bank accounts or credit card details. Both crimes use emails or websites that look like those of real organizations. Piracy, the illegal copying and distribution of copyrighted software, information, music, and video files, is widespread.

Individuals, businesses, and government agencies are all vulnerable to computer crime. Computer hackers sometimes work alone and sometimes in groups. One pair of hackers, nicknamed the “Deceptive Duo”, once claimed that they hacked into Midwest Express Airlines’ intranet. In an email to several news organizations, the hackers said that their goal was to embarrass the airline and show how easy it is to gain access to supposedly secure networks. The hackers even posted evidence of their break-in on the Web site of the U.S. Space and Naval War Systems Command. In one recent case, Russian hackers broke into Citibank’s network and electronically stole $10 million.

Companies with valuable or sensitive information stored in a computer worry about competitors or thieves raiding the database simply by dialing in through a modem. Even firms that don’t share their databases are subject to security breaches. In recent years U.S. corporations have spent more than $10 billion annually on network security. Even so, the estimated annual cost of computer crime is as high as $15 billion. The entire U.S. electronic infrastructure, including banks, financial markets, transportation systems, power grids, and telecommunication systems, could be vulnerable to attack. Companies and organizations must take strong precautions to protect themselves.

System administrators implement two basic protections against computer crime: They try to prevent access to their systems by unauthorized users and the viewing of data by unauthorized system users. To prevent access, the simplest method requires authorized users to enter passwords. An intranet blocks outsiders without valid passwords from entering its network by incorporating software known as a firewall. Firewalls limit data transfers to certain locations

and log system use so managers can identify attempts to log on with invalid passwords and other threats to system security.

To prevent system users from reading sensitive information, the company may use encryption software, which encodes, or scrambles, messages. Information security uses cryptography to transform information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. To read encrypted messages, users must use a key to convert them to regular text. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. The length and strength of the cryptographic key is an important consideration. A key that is weak or too short will produce weak encryption. More than one key can be used to encrypt and decrypt sensitive information. The keys used for encryption and decryption must be protected from disclosure and destruction and they must be available when needed. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit and while information is in storage. But as fast as software developers invent new and more elaborate protective measures, hackers seem to break through their defenses. So security is an ongoing battle.

Ex 1. Scan the text to determine whether these statements are true (T) or false (F). If the statement is false, give the right variant.

e.g. In my opinion it is true that… / To my mind it is false that … because…

1. The growth of information technology and the Internet has resulted in such a significant problem as information security.

2. There are two important security threats that may damage information systems: computer crime and viruses.

3. Crackers, or black hat hackers, are computer criminals who use technology to perform various crimes.

4. The number of violations of Internet security has fallen sharply in recent years.

5. Internet-based crimes include phishing, email fraud to obtain money or valuables, and scam, bank fraud, to get banking information.

6. Computer technology is widely used to pirate copyrighted works such as films and music.

7. Nowadays all organizations are vulnerable to computer crime.

8. Sometimes hackers want to show how easy it is to gain access to supposedly secure networks.

9. The firms that don't share their databases are completely protected against security breaches.

10. U.S. corporations seldom spend money on network security though the estimated annual cost of computer crime is as high as $15 billion.

11. The most complex method to prevent access is to enter passwords.

12. A firewall is a program designed to prevent spyware from gaining access to the internal network.

13. The process of transforming information into a form that renders it unusable by anyone other than authorized user is known as decryption.

14. Cryptographic keys are used to convert encrypted messages into their original usable form.

15. Only one key can be used to encrypt and decrypt the sensitive information.

16. Cryptography is used in information security to protect information from unauthorized disclosure while the information is in transit.

Ex.2. Answer the questions

1. Name the most significant problem that businesses and organizations face as a result of computer technology.

2. What is information security?

3. Identify the three important threats that may damage information systems.

4. Explain the term “black hat hacker”.

5. What do common computer crimes involve?

6. What do Internet-based crimes include? Explain the terms “scam”, “phishing” and “piracy”.

7. Why must companies and organizations take strong precautions to protect themselves?

8. What basic protections do system administrators implement against computer crime?

9. Explain how firewalls work.

10. What is cryptography used for? Describe the processes of encryption and decryption.

11. Why is it said that security is an ongoing battle?

Ex 3. Replace the underlined words or word-combinations with their equivalents given in the box.

vulnerable to, phishing, malicious, location, crackers, to protect, crimes, confidentiality, implement, breaking into, sensitive, unauthorized, annually, to affect, elaborate, precautions, cryptographic key, hack into, encode, on rise, breaches, entire, security, encrypt

1. Information security is concerned with the secrecy, integrity and availability of data.

2. One of the tasks of information security is to defend information systems from illicit access.

3. When computers are connected to a network, a problem at any place or position can influence the whole network.

4. People with evil intentions may break into computer systems; such actions are regarded as computer offenses.

5. To prevent black hat hackers from getting into your internal network and obtaining your data, install a firewall.

6. Security specialists carry out different protective measures against security break-ins.

7. Computer crime is increasing. Individuals, businesses, and government agencies are all not completely protected against computer crime

8. Governments, military, corporations, banks, hospitals, and private businesses worry about safety of the classified information stored in computers.

9. Check with your bank before sending information to avoid bank fraud.

10. Every year U.S. corporations spend billions of dollars on network security.

11. Companies must still take strong preventive measures against computer theft cases.

12. A scrambler is a special device used in cryptography to encipher messages.

13. The key used for decryption and encryption must be protected with the same degree of rigor as any other confidential information.

14. Today's web browsers automatically scramble text when making a connection to a secure server. This prevents intruders from listening in on private communications.

15. Software developers constantly work out new and more complex protective measures.

Ex 4. Match the terms on the right with their definitions on the left.

1. password	a) the illegal copying and distribution of copyrighted software, information, music and video files
2. cryptographic key	b) combination of hardware and software used to control the data going into and out of a network.
3. encryption	c) software created to damage or alter the computer data or its operations
4. decryption	d) a secret code used to control access to a network system
5. valid	e) a computer security expert who uses his skills to make cyberspace safer
6. firewall	f) a computer criminal who uses technology to perform a variety of crimes
7. phishing	g) a sequence of symbols that controls the operation of a cryptographic transformation (e.g. encryption, decryption)
8. scam	h) a process in which the sender

encrypts / scrambles the message in such a way that only the recipient will be able to decrypt the message

9. piracy — i) legally binding or effective

10. malware (malicious software) — j) email fraud to obtain money or valuables

11. spyware (spy software) — k) the process of changing information that has a special code back into its original form so that it can be easily understood

12. black hat hacker — l) pretending to be someone that can be trusted, in order to steal banking information such as passwords of Internet bank accounts or credit card details

13. white hat hacker — m) a type of malware that is designed to spy on the victim's activities, capturing sensitive data such as the person's passwords, online shopping, etc.

Ex.5. Read and translate the text to perform the tasks given below the text.

Text 3. TYPES OF DATA ENCRYPTION

The data transferred from one system to another over the public network can be protected by the method of encryption. On encryption the data is encrypted / scrambled by any encryption algorithm using the key. Only a user having access to the same key can decrypt / descramble the encrypted data. A

single secret cryptographic key is used for both encryption and decryption. This method is known as private key or symmetric key cryptography.

There are several standard symmetric key algorithms defined. Examples are AES, 3DES and Blowfish. These standard symmetric algorithms are proven to be highly secured and time tested. But the problem with these algorithms is the key exchange. The communicating parties require a shared secret, key, to be exchanged between them to have a secured communication. The security of the symmetric key algorithm depends on the secrecy of the key. Keys are typically hundreds of bits in length, depending on the algorithm used. Since there may be a number of intermediate points between the communicating parties through which the data passes, these keys cannot be exchanged online in a secured manner. In a large network, where there are hundreds of systems connected, offline key exchange seems too difficult and even unrealistic.

This is where public key cryptography, also known as asymmetric cryptography, is a help. Using public key algorithm a shared secret can be established online between communicating parties without the need for exchanging any secret key. In public key cryptography, each user has a pair of cryptographic keys – a public key and a private key. Only the particular user / device knows the private key whereas the public key is distributed to all users / devices taking part in the communication. The sender encrypts / scrambles the message in such a way that only the recipient will be able to decrypt / descramble the message. A disadvantage of using public-key cryptography for encryption is speed. Asymmetric key algorithms are hundreds to thousands times slower than symmetric key algorithms.

Consider a device B whose private key and public key are PB and UB respectively. Since UB is public key all devices will be able to use it. For any device that needs to send the message `Msg' in a secured way to device B, it will encrypt the data using B's public key to obtain the cipher text `Ctx'. The encrypted message, cipher text, can only be decrypted using B's private key. On

receiving the message B decrypts it using the private key PB. Since only B knows the private key PB none other including A can decrypt the message.

It is important that device A receives the correct public key from device B, i.e. no middleman must tamper or change the public key to its public key. Digital Certificate helps to deliver the public key in an authenticated method. The Digital Certificate is an electronic document that uses a digital signature to bind a public key with an identity – information such as the name of a person or an organization, their address, and so forth.

A digital signature is a mathematical scheme for demonstrating the authenticity of an electronic message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. If any the data or signature is modified, the signature verification fails.

Ex 1. Find in the text the English equivalents of the following word-combinations:

1. данные, передаваемые от одной системы к другой
2. по сети общего пользования
3. любой алгоритм шифрования
4. единственный секретный криптографический ключ
5. криптография с секретным ключом (одноключевая криптография)
6. криптография с открытым ключом или ассиметричная криптография
7. стандартные алгоритмы с симметричным ключом
8. быть на высоком уровне безопасности и проверенными временем
9. обмен ключа
10. взаимодействующие стороны
11. совместно используемый секретный ключ
12. ряд промежуточных пунктов

13. внесетевой (в режиме офлайн) обмен ключа

14. отправитель и получатель

15. недостаток в использовании криптографии с открытым ключом

16. в сотни и тысячи раз медленнее

17. являться PB и UB соответственно

18. поскольку UB есть открытый ключ…

19. расшифровать сообщение

20. посредник

21. подделывать или изменять открытый ключ

22. цифровой сертификат

23. доставлять открытый ключ

24.аутенфикациооным методом (методом удостоверения подлинности)

25. цифровая (электронная) подпись

26. связывать открытый ключ с идентификационной информацией

27. математическая схема

28. аутентичность (подлинность) электронного сообщения или документа

29. верификация (подтверждение подлинности) подписи не выполняется

Ex 2. Choose the right option to complete the sentences.

1. The main problem with symmetric key algorithms is

a) the key length

b) the key weakness

c) the key exchange

2. Public-key cryptography is also known as

a) symmetric cryptography

b) asymmetric cryptography

c) shared-key cryptography

Ex. 3. A message encrypted with the recipient's public key can only be decrypted with

a) the sender's private key

b) the sender's public key

c) the recipient's private key

Ex. 4. Symmetric-key algorithms are

a) as fast as asymmetric key algorithms

b) hundreds to thousands times slower than asymmetric key algorithms

c) hundreds to thousands times faster than asymmetric key algorithms

Ex. 5. A Digital Certificate is

a) a small block of data that is attached to the documents you sign

b) an electronic document which proves your identity when you are doing business on the Internet

c) a program designed to prevent unauthorized access to the network by hackers

Ex.6. A digital signature is a mathematical scheme for demonstrating

a) the privacy of an electronic message or document

b) the availability of an electronic message or document

c) the authenticity of an electronic message or document

Ex. 1. Translate the sentences into English using an appropriate modal verb equivalent.

1. Я должен это сделать. (обязательно)
2. Я должен был это сделать. (вчера)
3. Мне приходится это делать. (даже если я не хочу)
4. Мне пришлось это сделать. (я был вынужден)
5. Мне следует это сделать. (потому что это разумно)
6. Я могу это сделать. (потому что умею)
7. Я умел это делать. (раньше)
8. Я смогу это сделать. (завтра)
9. Я могу это делать. (потому что мне можно)
10. Я смогу это сделать. (завтра, потому что мне разрешат)
11. Мне нужно это сделать. (я в этом нуждаюсь)
12. Мне не нужно это делать. (нет необходимости)

Ex 2. Choose the right variant:

1. Computer crime is on the rise. Companies and organizations ---------- consistently take strong precautions to protect themselves against security breaches.

a) can b) may c) must

2. Hackers use various methods to break into computer systems. For instance, they -------- simply dial in through a modem.

a) may b) must c) should

3. Sometimes companies -------- hire former black-hat hackers to defend their companies' networks.

a) must b) have to c) are to

4. Malicious software, malware, -------- be avoided by following some basic rules.

a) can b) must c) need

5. Install a firewall. It -------- prevent spyware from getting access to the internal network.

a) must b) should c) might

6. People doing business over the Internet -------- get a Digital Certificate, an electronic identity card.

a) must b) should c) are able to

7. When a Digital Certificate is issued, it is valid for a fixed period of time. You -------- renew or update your Digital Certificate before it expires.

a) have to b) might c) are able to

8. A message encrypted with the recipient's public key -------- only be decrypted with the recipient's private key.

a) needn't b) can c) should

9. The primary advantage of public-key cryptography is increased security: the communicating parties -------- exchange a private key between them. In a secret-key system, by contrast, there is always a chance that an enemy ------- discover the secret key while it is being transmitted.

a) mustn't; may b) shouldn't; is able to c) needn't; can

10. Gentlemen, the situation is critical. A few days ago the system was broken into. A great deal of confidential information has been disclosed. We --

fire several specialists of the security department. Now we -------- analyze the situation to prevent such incidents in the future.

a) could; may b) had to; should c) might; can

11. I've been working on this program for many hours. I'm tired to the bone and I think I -------- have a break. I hope I'll -------- to go on with this work tomorrow morning.

a) should; be able to b) may; must c) can; need

12. You -------- believe everything you read on the Net. Be suspicious of any wonderful offer. It -------- be a fraud.

a) could not; might b) don't have to; can c) shouldn't; may

13. You -------- read these documents. They are top-secret.

a) may not b) cannot c) needn't

14. The conference on the problems of the security of information systems ------- begin next Monday.

a) must b) has to c) is to

15. We -------- do everything we -------- to keep this information secret.

a) need; may b) may; should c) must; can

16. I -------- speak English fluently now. Two years ago I -------- say only a few words in English.

a) may; might b) can; could c) could; can

17. – This message is urgent. -------- I send it right now?

– No, you -------- . I have already sent it.

a) Can; can't b) Must; mustn't c) Must; needn't

Ex 4. Put the parts of the sentences into the correct order.

1. software and hardware / security specialists / from malware / to protect information / in the design of / specialize.

2. a program / from gaining access / is / a firewall / to the internal network / designed / to prevent spyware.

3. high-risk / don't / sources / accept / from / files.

4. signatures / to authenticate / are / digital / used / documents.

5. increased security / public-key cryptography / is / of / the primary advantage.

6. the practice of modifying / to accomplish a goal / computer hardware and software / is / computer hacking / the creator's original purpose / outside of.

7. key algorithms / such as / asymmetric / RSA, SSL and TSL / data / will keep / private.

8. extremely / secret-key / important / remains / cryptography.

Ex 5. Turn into Passive Voice

Passive Voice

	Past	Present	Future
Simple (Indefinite)	was/were + V_3^{ed}	am/is/are + V_3^{ed}	shall/will be + V_3^{ed}
Progressive (Continious)	was/were being + V_3^{ed}	am/is/are being + V_3^{ed}	——— *(употреблять Future Simple)*
Perfect	had been + V_3^{ed}	has/have been + V_3^{ed}	shall/will have been + V_3^{ed}
Perfect Progressive (Continious)	———	———	———
	(употреблять формы Perfect)		

1. I complete these forms after dinner.
2. My father exports luxurious products to Africa.
3. Tom doesn't want a noisy room.
4. I want breakfast in my room.

5. Tim rings the operator.
6. A photocopier makes fast copies.
7. Our company imports goods from Europe.
8. Peter sells photocopiers.
9. We have breakfast at 8.00.
10. Tom rings Mary everyday.
11. You make plastic products.
12. The photocopier makes ten copies per minute.
13. That company makes cell phones.
14. The customer wants red files.
15. My secretary does the filling.
16. I want a drink.
17. You file these documents.
18. We sell excellent leather products from Argentina.
19. We need finance for our new company in Paris.
20. I need your investment.
21. We want to invest in your country.
22. She needs money from London for her project.
23. You wait a call from Paris.
24. The secretary prepares coffee in the office.
25. I meet a lot of people.

26.I do a lot filing at the office.

27.You answer the phone quickly.

28.Susan studies Maths at University.

29.She does a course in Business studies.

30.They need some order forms.

UNIT IV. PROGRAMMING: LANGUAGES,

METHODS AND TECHNOLOGIES.

Equation	уравнение
List of instructions	перечень команд
Enable	давать возможность
Guard	защищать, предохранять, заканчивать
Appropriate sequence	необходимая последовательность
Program logic	логическая последовательность выполнения программы
Flowchart	блок-схема, составлять блок-схему
Flowcharting	построение блок-схемы

Pictorial representation наглядное представление

Predefined symbols заранее заданные символы

Emplate шаблон, образец

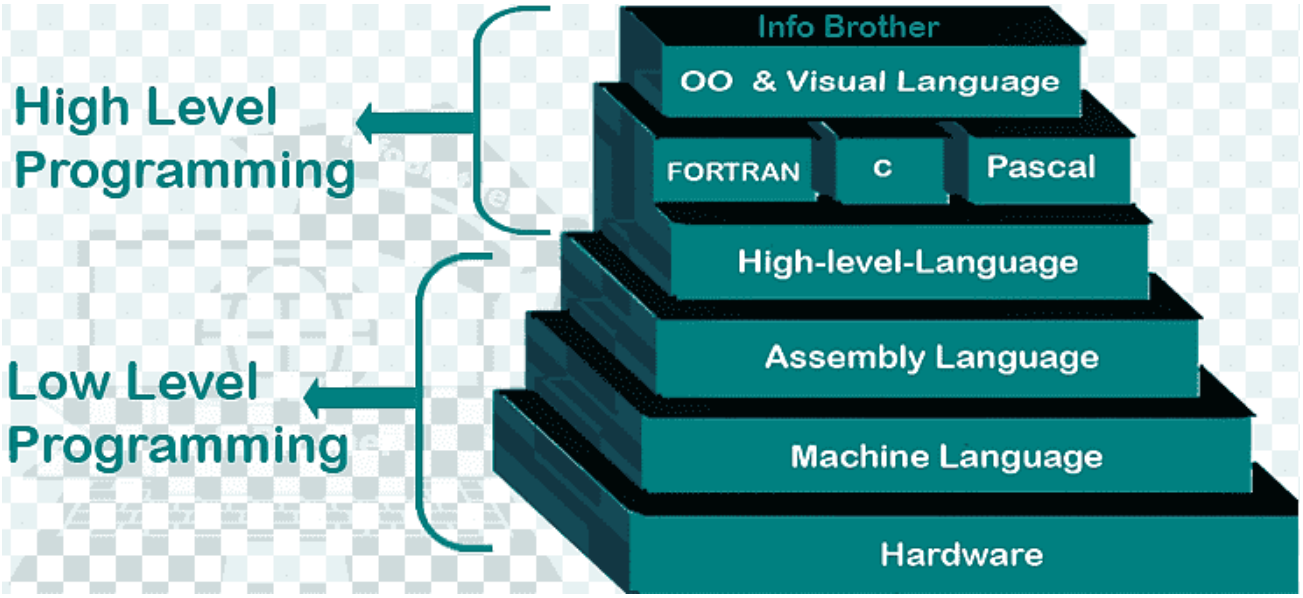
Pseudocode псевдокод, псевдопрограмма

Burden издержки, затраты

Consume потреблять, расходовать

Top-down approach принцип нисходящей разработки

Looping logic логическая схема выполнения (операций)в цикле



Text 1. Computer Programming

Programming is the process of preparing a set of coded instructions which enables the computer to solve specific problems or to perform specific functions. The essence of computer programming is the encoding of the program for the computer by means of algorithms. The thing is that any problem is expressed in mathematical terms, it contains formulae, equations and calculations. But the

computer cannot manipulate formulae, equations and calculations. Any problem must be specially processed for the computer to understand it, that is – coded or programmed.

The phase in which the system's computers are written is called the development phase. The programs are lists of instructions that will be followed by the control unit of the central processing unit (CPU). The instructions of the program must be complete and in the appropriate sequence, or else the wrong answers will result. To guard against these errors in logic and to document the program's logical approach, logic plans should be developed.

There are two common techniques for planning the logic of a program. The first technique is flowcharting. A flowchart is a plan in the form of a graphic or pictorial representation that uses predefined symbols to illustrate the program logic. It is, therefore, a ''picture'' of the logical steps to be performed by the computer. Each of the predefined symbols shapes stands for a general operation. The symbol shape communicates the nature of the general operation, and the specifics are written within the symbol. A plastic or metal guide called a template is used to make drawing the symbols easier.

The second technique for planning program logic is called pseudocode. Pseudocode is an imitation of actual program instructions. It allows a program-like structure without the burden of programming rules to follow. Pseudocode is less time-consuming for the professional programmer than is flowcharting. It also emphasizes a top-down approach to program structure.

Pseudocode has three basic structures: sequence, decision, and looping logic. With these structures, any required logic can be expressed.

Ex. 1. Find in the text above the English equivalents for the following words and expressions:

- совокупность закодированных команд

- формулы, уравнения, вычисления

- необходимая последовательность

- защищать от ошибок

- общепринятая методика

- построение блок-схемы

- наглядное представление

- без издержек

- выделять принцип нисходящей обработки

- логическая схема выполнения операций в цикле

Ex 2. **Match the following English key words with their Russian equivalents:**

1) access program a) сторожевая программа

2) application program b) вспомогательная программа

3) archived program c) дистанционная программа

4) binary program d) программа доступа

5) database program e) сетевая программа

6) debugging program f) программа в двоичном коде

7) on-line program g) заархивированная программа

8) support program h) программа отладки

9) remote program i) прикладная программа

10) watch-dog program j) программа, работающая с базой данных

Ex 3. **Say if it is right or wrong. Give a full answer:**

1. The essence of computer programming is the encoding of the program for the computer by means of algorithms.

2. The computer can easily manipulate formulae, equations and calculations.

3. The instructions of the program must not be complete and in the appropriate sequence.

4. There are three common techniques for planning the logic of a program.

5. Pseudocode is an imitation of actual program instructions.

6. Pseudocode doesn’t emphasize a top-down approach to program structure.

7. Pseudocode has two basic structures: sequence and looping logic.

Ex 4. **Complete the sentences:**

1. Programming is the process of preparing a set of coded instructions which enables the computer to solve … .

2. The phase in which the system's computers are written is called … .

3. … … these errors in logic and to document the program's logical approach, logic plans should be developed.

4. A plastic or metal guide called a template is used to make … .

5. … is an imitation of actual program instructions.

6. Pseudocode is less time-consuming for the professional programmer … .

Ex 5. **Read and translate the following sentences:**

1. We have done it already. 2. I have become a teleworker, a person who can work at home, thanks for teleworking or telecommuting. 3. ICT has made my job much better and easier. 4. We have decided to install computers in all departments but we haven't spent a lot of money on them. 5. He has designed a web page and wants to transfer the data to his reserved web space. 6. A network worm has struck 6.200 machines that formed 7.3% computers to network. 7. When you came I had already written my email.

Ex 6. **Think of questions for which the following might be answer.**

1. Mary has designed a flowchart. 2. He has written the instructions in a high-level language. 3. She hasn't seen him since the summer. 4. He has given her a machine code. 5. She has put her notebook into the bag. 6. She has changed her nick. 7. She has always tried to stop him. 7. Most online banks have introduced the concept of two-factor authentication.

Ex 7. Translate into English using the Present Perfect.

1. Что случилось? 2.Мы только что разработали блок-схему. 3. Он никогда не слышал о правилах программирования. 4. Она ещё не рассказала ему о псевдокоде. 5. Я его еще не закончила. 6.Они уже знали правила программирования. 7. Ты когда-нибудь слышал о логической схеме выполнения операций в цикле.

Ex 8. Make up different word-combinations using the following words (A, B) and translate them:

A	**B**
Computer	symbols
Appropriate	phase
Mathematical	approach
Development	terms
Logical	representation
Graphic	program
Predefined	rules
Program	sequence

Ex 9. Translate the following sentences.

1. Суть компьютерного программирования заключается в кодировании посредством алгоритма.

2. Любая проблема должна быть обработана специальным образом для того, чтобы компьютер понял её, т.е. она должна быть закодирована или запрограммирована.

3. Существуют две общепринятые методики для планирования логической последовательности выполнения программ.

4. Блок-схема – это план в форме графического или наглядного представления, который использует заранее заданные символы, чтобы проиллюстрировать логическую последовательность выполнения программы.

5. Псевдокод имеет три основных компонента: последовательность, решение и логическую схему выполнения в цикле.

Ex 10. **Answer the following questions:**

1. What is programming?

2. What is the essence of programming?

3. What should be done with the problem before processing by the computer?

4. What is a program?

5. What are instructions?

6. What are the main techniques for planning the program logic?

7. What is a flowchart?

8. What is a template and what is it used for?

9. What do you understand by ‘’pseudocode’’?

10. What are the basic structures of pseudocode?

Ex 11. Complete the sentences using two of the words in each group.

1. *install crash log in*

I’ve just bought this game for my computer and I want to ____ it, but I’m worried that it’s going to make my computer _____ again.

2. *genius manual gadget*

I don’t understand how this _____ works – where’s the instruction _____ for it?

3. *revolutionized developed experimented*

Home computers _____ the world when they first came out and lots of us can’t remember what life was like before they were _____.

4. *research engineer progress*

The _____ who works in my department is doing _____ on a new kind of technology.

5. *guarantee laboratory test*

The scientists in the _____ realized that they had to do a different _____ to find the answer to their question.

Ex 12. **Choose the correct answers**.

1. A **database** is a program that lets you _____

a) delete information from your computer;

b) store large amounts of information on a computer

2. If you study **information technology** you will learn about ____

a) the laws of engineering;

b) storing and sending information on electronic equipment

3. **Graphic** design is the art of ____.

a) planning the decoration for the inside of a building;

b) designing pictures and text for books, advertisements and magazines

4. If someone is **computer literate**, they _____.

a) are not very familiar with computers and how they work;

b) are familiar with computers and how they work

5. If you make a **back-up copy** of your work on a computer, you ___.

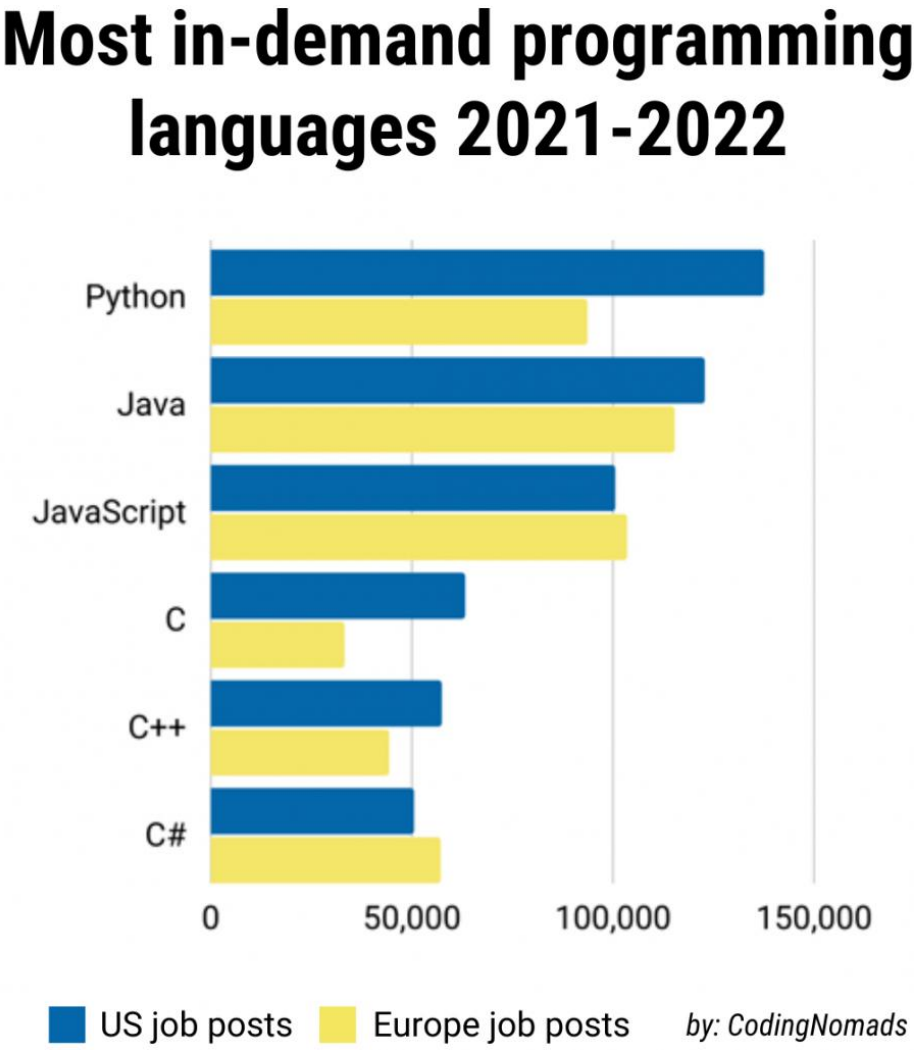
a) make an extra copy on a CD or other external memory;

b) print it out on paper and keep it in a folder

6. If you went to buy **computer hardware**, you would be looking for _____.

a) disk drives, modems, keyboard, monitors, etc.;

b) the programs needed to work the machine.



Text 2. Programming languages

Programming is the process of writing a program using a computer language. A *program* is a set of instructions which a computer uses to do a specific task (e.g. a solution to a Maths problem).

The only language a PC can directly execute is *machine code*, which consists of 1s and 0s. This language is difficult to write, so we use symbolic languages that are easier to understand. For example, *assembly languages* use abbreviations such as ADD, SUB, MPY to represent instructions. The program is then translated into machine code by software called an *assembler*.

Machine code and assembly languages are called low-level languages because they are closer to the hardware.

High-level languages, however, are closer to human languages; they use forms resembling English, which makes programming easier. The program is translated into machine code by software called a *compiler*. Some examples are:

- **FORTRAN** – used for scientific and mathematical applications

- **COBOL** – popular for business applications

- **BASIC** – used as a teaching language; Visual BASIC is now used to create Windows applications

- **C** – used to write system software, graphics and commercial programs

- **Java** – designed to run on the Web; Java applets are small program that run automatically on web pages and let you watch animated characters, and play music and games.

The languages used to create Web documents are called *markup languages*; they use instructions (markups) to format and link files. Examples are:

- **HTML** – the code used to create Web pages

- **Voice XML** – it makes Internet content accessible via *speech recognition* and phone. Instead of using a web browser on a PC, you use a telephone to access voice-equipped websites. You just *dial* the phone number of the website and then give spoken instructions, *commands*, and get the required information.

2. Steps in writing a program

To write a program, software developers usually follow these steps.

- First they try to understand the problem and define the purpose of the program.

- They design a flowchart, a diagram which shows the successive logical steps of the program.

- Next they write the instructions in a high-level language (Pascal, C, etc.). This is called coding. The program is then compiled.

- When the program is written, they test it: they run the program to see if it works and use special tools to detect bugs, or errors. Any errors are corrected until it runs smoothly. This is called debugging, or bug fixing.

- Finally, software companies write a detailed description of how the program works, called program documentation. They also have a maintenance program. They get reports from users about any errors found in the program. After it has been improved, it is published as an updated version.

Exercise 1. Match the terms from previous text 1 opposite with their definitions.

1. programming a) basic language which consists of binary codes

2. machine code b) programming language such as C, Java or Visual BASIC

3. assembly language c) writing computer programs

4. high- level language d) Low – level language translated into machine code by an assembler

5. Java applet e) software which converts a source program into machine code

6. compiler f) language used to create and format documents for Web

7. markup language g) small self-contained program written in Java

Ex 2. Complete this article about the Voice XML application language with the words from the bracket.

(*HTML dial Voice XML commands speech recognition*)

Internet: Voice recognition takes off

You don't need sophisticated суд phone to surf the Internet when you're on the road – just your own voice. That's the idea behind a new breed of voice service that is popping up all over the place. Subscribers (1)…….a toll-free phone number and use spoken (2)…….. to listen to anything from weather conditions to stock quotes, or flight information to new stories. Half a dozen of these services – such as Audiopoint, BeVocal, TellMe and TelSurf Networks – have already gone live or are testing their systems.

These launches are all happening because two crucial technologies have come of age. (3)…… ……. software from companies such as Lucent, Nuance and Speechworks can now understand a wide range of accents and diction without having to be trained to a specific voice. And computer languages such as VoiceXML make it as easy to write voice services (4)……. has made it to write web pages. With (5) …… , the human voice becomes a substitute for a computer mouse and the spoken command for a click. It doesn't, however, call up conventional web pages, but content which is especially composed for a telephone: sound clips, numbers, music, spoken text.

Ex 3. Solve the clues and complete the puzzle.

Across

1. A new radio communication system.

3. A system that integrates telephones and computer is a ……. centre

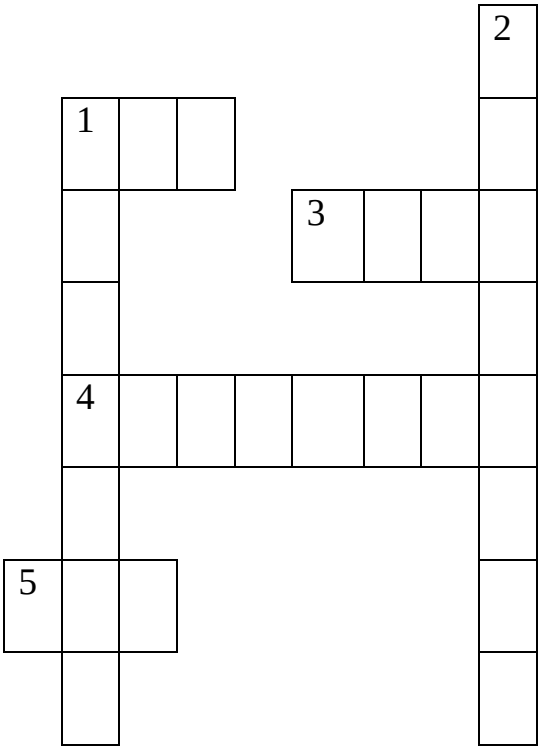
4. A global system of networks of integrated services.

5. A device used to send and receive exact copies of documents.

Down

1. Similar to interactive TV.

2. Written information you get on your TV screen.



TEXT 3. E-Russia

The information technologies are developing at a rapid pace in Russia and penetrate into everyday life of people. Many people, who can access to Internet, not only can buy and sale, same of them can't work and live without using this global electronic net. E-business and e-commerce are widely developing. The information technologies are being widely used in medicine, health care, education and science. Taking into consideration the rapid pace of IT development, the state began the work on e-government introduction in Russia. The government has to find new ways to complete its function, to interact with the citizens and produce the innovation in public management. The Target Program «E-Russia» was adopted. It was planned to develop the arrangements on the budget consolidation of different departments which help adopt new information technologies, and to create a platform for the integration of departmental databases and the organization of the end-to-end e-circulation of documents. At the very beginning of the program implementation considerable amendments to the E-Russia program were adopted as a result of a constructive discussion between all the participants concerned. The amendments turned the program from an interdepartmental program to the program of the introduction e-government. The E-Government Concept of the Russian Federation was adopted. The Concept established the main priorities directions, and stages of the e-government introduction in the Russian Federation. The government also adopted the Information-oriented Society Development Strategy of the Russian Federation which approves control values of the information-oriented society development in the Russian Federation for the period till 2015. Thus, these measures will have ensured the e-rendering of 74 state services by means of the state web portal, and will have provided the introduction of the interdepartmental end-to-end e-circulation of documents by 2015.

The government will face new forms of public participation in the decision-making. In the situation than information technologies (IT) possibilities allow each citizen to participate actively in the definition of public policy, the relation between government and citizens will be direct. The governments will have to find new ways to complete his function, to interact with the citizens and produce the innovation in public management. The Russia Federal Ministry of Communications and Information is the coordinator of the elaboration of the program. The realizing of that program will open the perspectives for the different sectors of economy, society, and will stimulate the innovational possibilities of private sector. There are several benefits derived from the e-Russia: the customizing of the services, the reduction of the distances and the time, the productivity and the efficiency, the decentralization, the transparency, the supply and provisions of integrated services, the best administration of the budget, among others.

However, the enormous digital gap that exists in countries as ours, between the inhabitants that have and those that do not have access to Internet, generates enormous challenges for a successful beginning of the electronic government.

Ex.1. Match 1-6 with a-g.

1. private sector	a. инновационные перспективы
2. innovational possibilities	в. частный сектор
3. rapid pace	с база данных департамента
4. departmental database	d. высокая скорость
5. participate actively	e. секторы экономики

6. sectors of economy f. активно участвовать

Ex.2. Make up sentences.

1. technologies are, The information, developing, in Russia, at a rapid pace.

2. have to find, The governments, new ways, to complete his function.

3. The state, e-government introduction, in Russia, began the work on.

4. The government, new forms of, public participation, will face.

5. is the coordinator of, The Russia Federal Ministry of Communications and Information, the elaboration of the program.

6. E-business and e-commerce, developing, are widely.

7. The state web portal, of 74 services, will ensure the e-rendering.

Ex. 3. Answer the questions to the text.

1. Do the information technologies penetrate into everyday life of Russian people?

2. How do Russians use the information technologies?

3. Did the state begin the work on e-government introduction in Russia?

4. Do IT technologies help the government to develop a new way of interaction with the citizens?

5. Does IT program plan to create a platform for the integration of departmental databases and the organization of the end-to-end e-circulation of documents?

6. Will the government face new forms of public participation in the decision-making?

7. What ministry is the coordinator of the elaboration of the program?

8. Will the realizing of that program open the perspectives for the different sectors of economy, society, and stimulate the innovational possibilities of private sector?

Ex.4. Choose the correct word and fill in the gaps. Use the text.

Access, developing, databases, sale, citizen, e-government, the innovation.

1. Many people, who can ……. to Internet, not only can buy and ….., some of them can't work and live without using this global electronic net.

2. E-business and e-commerce are widely……...

3. Taking into consideration the rapid pace of IT development, the state began the work on …….. introduction in Russia.

4. It was planned to develop the arrangements on the budget consolidation of different departments which help adopt new information technologies, and to create a platform for the integration of departmental …… and the organization of the end-to-end e-circulation of documents.

5. In the situation than information technologies (IT) possibilities allow each …… to participate actively in the definition of public policy, the relation between government and citizens will be direct.

6. The governments will have to find new ways to complete his function, to interact with the citizens and produce …….. in public management.

Ex.5. Speak about E-Russia.

a) information technologies in Russia using these words and phrases (are developing at a rapid pace, information technologies, can access to Internet, can buy and sale, live without, e-business, to develop, idly used in, healthcare.)

b) e-government introduction in Russia using these words and phrases (the state began, introduction, to find new ways, function, to interact with, the innovation, in public management, to create platform, of departmental databases, end-to-end circulation.)

c) new forms of public participation in the decision-making using these phrases (the e-rendering of, by means of, web portal, the interdepartmental e-circulation, will face new, IT possibilities, of public policy, new ways to complete, several benefits, the reduction of the distances.)

Ex.6. Translate from Russian into English.

1. Информационные технологии в России развиваются очень быстро.

2. Информационные технологии проникают в повседневную жизнь людей.

3. Информационные технологии используются в медицине, образовании и науке.

4. Правительству необходимо найти новые способы общения с народом.

5. Новая программа позволит создать платформу для объединения баз данных различных министерств.

6. Эти меры помогут государственным учреждениям оказывать услуги через государственный портал.

7. Внедрение информационных технологий поможет гражданам активно участвовать в определении государственной политики.

8. Осуществление электронных программ откроет новые перспективы в экономике.

9. Электронная программа дает много преимуществ, например, сокращение расстояния.

Ex. 7. Fill in the spaces with the verbs *go, come* and *walk*.

1. I ----- to last night, but you were out. 2. I think I will ----to see the football match tomorrow. 3. He ----back from his walk very tired. 4. I am ----to the country. 5. He ----- home because he wanted to take a breath of fresh air. 6. ----on with your reading. 7. We shall ----by train to the South. 8. Do you---much? 9. Ton is ill. –and bring the doctor. 10. Winter is -----. 11. I cannot -----so fast. 12. I saw a dog ----towards me. 13. let us ----on a trip to the mountains. 14. I have a headache after ----so long in the sun. 15. ----here quick! 16. You are late. The bus has just-----.

Ex. 8. Express in one word the meaning of each of the following phrases. You are given the first letter of each word and the number of letters in it.

1. Peaceful, wishing to live in peace (p----------)

2. Very, very large (e-------)

3. Come next after (s-------)

4. The opposite of low-lying (m----------)

5. Join together (c-------)

6. Belonging to the army (m-------)

7. A river that flows into a larger river (t--------)

8. Synonym of include (e-------)

Text 4. Programming languages.

Programming is the process of writing a program using a computer language. A program is a set of instructions which a computer uses to do a specific task (e.g. a solution to a Maths problem).

The only language a PC can directly execute is machine code, which consists of 1s and 0s. This language is difficult to write, so we use symbolic languages that are easier to understand. For example, assembly languages use abbreviations such as ADD, SUB, MPY to represent instructions. The program is then translated into a machine code by software called an assembler.

Machine code and assembly languages are called low-level languages because they are closer to the hardware.

High-level languages, however, are closer to human languages; they use forms resembling English, which makes programming easier. The program is translated into machine code by software called a compiler. Some examples are: FORTRAN – used for scientific and mathematical applications COBOL – popular for business applications BASIC – used as a teaching language; Visual BASIC is now used to create Windows applications C – used to write system software, graphics, and commercial programs Java – designed to run on the Web; Java applets (аплет, приложение) are small programs that run automatically on web pages and let you watch animated characters, and play music and games.

The languages used to create Web documents are called markup languages (язык разметки); they use instructions (markups) to format and link

text files. Examples are: HTML – the code used to create Web pages VoiceXML – it makes Internet content accessible via speech recognition and phone. Instead of using a web browser on a PC, you use a telephone to access voice-equipped websites. You just dial the phone number of the website and then give spoken instructions, commands, and get the required information.

Ex.1. Read and translate the text

Ex.2. Match the terms from the text above with their definitions.

1 programming a basic language which consists of binary codes

2 machine code b programming language such as C, Java or Visual BASIC

3 assembly language c writing computer programs

4 high-level language and low-level language translated into machine code by an assembler

5 Java applet e software which converts a source program into machine code.

6 compiler f language used to create and format documents for the Web

7 markup language g small self-contained program written in Java

Ex. 3. Study these sample sections of programs. Rank from 1 (easiest to understand) to 5 (most difficult to understand).

Ex. 4. Here is a list of language types used by programmers ranked from natural human language at the top to machine code at the bottom. Can you match any of the samples in Task 3 to this list?

1 Natural language

2 Very high-level language

3 High-level language

4 Assembly language

5 Machine code

6. Language Work:

ABBREVIATIONS

As in many genres of legal English the use of abbreviations is common in the language of cybercrime.

Look at the examples below and try to complete the missing words or letters (small spaces) in parentheses. Translate them.

1. AS (A _ _ _ _ s Server)

2. ATM (A_____ T_____Machine)

3. BT (B _ _ _ _ _ _ th)

4. BW (Band _ _ _ _ _)

5. CERT (Computer E_____R_____ Team)

6. CNP Transaction (C _ _ _ Not Present Transaction)

7. CPS (C_____s per Second)

8. CSP (C _ _ _ _ Service Provider)

9. CSV (C _ _ _ _ -separated values)

10. DBMS (D _ _ _ _ _ _ e M_____ ment System)

11. DL (D _ _ _ _ _ ad)

12. DNS (D _ _ _ _ n Name System)

13. EFS (En _ _ _ _ _ ing File System)

15. FAQs (F_____ A_____ Q_____)

15. FxP (F _ _ _ Exchange P _ _ _ _ _ ol)

16. GB (_____)

17. IP (I_____ Protocol)

18. IS (I_____ Systems)

19. ISP (I_____ S_____ Provider)

20. IT (I_____ T_____)

21. LCD (L _ _ _ _ d C _ _ _ _ _ _ Display)

22. MB (_____)

23. MS (M _ _ _ _ _ Stick)

24. NFS (Network F _ _ _ System)

25. ODBC (O _ _ _ D _ _ _ _ _ se Connectivity)

26. OLTP (Online T_____n Processing)

27. OS (O_____ System)

28. PDF (P _ _ _ _ _ le D _ _ _ _ _ nt Format)

29. RAS (R _ _ _ _ _ A _ _ _ _ _ Service)

30. RAM (R _ _ _ _ m A _ _ _ _ _ Memory)

31. RAT (R _ _ _ _ e Administration T _ _ l)

32. RC (R _ _ _ _ n Code)

33. ROM (R _ _ _ O _ _ _ Memory)

34. SMTP (S _ _ _ _ _ Mail T _ _ _ _ _ _ r Protocol)

35. SSD (Software Spe_____ Document)

36. TB (_____)

37. URL (U _____ Resource L _ _ _ tor)

38. VGA (Video Graphics Adapter)

39. VR (V_____ Reality)

40. WAN (W _ _ _ Area N _ _ _ _ _ k)

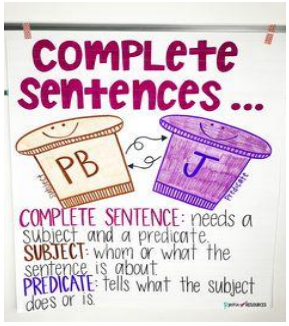
41. WAP (W _____ Access P _____)

42. WiFi (W_____ F _ _ _ _ _ _ y)

43. WLAN (W_____ L _ _ _ _ Area N_____)

44. WWW (_____)

Grammar



(see Appendix 4)

Ex 1. Complete the sentences in your own words:

1) The police officer would have gone abroad, if _____.

2) I would tell the officer about the accident, if _____.

3) We will go to the cinema, if _____.

4) If you have finished the work, _____.

5) If you lose your favorite umbrella, _____.

6) If I get a lot of money, _____.

7) I would have bought that expensive painting, if _____.

8) If he earned a lot, _____.

9) If you spend your holidays abroad, _____.

10) I will leave the door ajar, if _____.

11) You will miss your bus, if _____.

12) If it rains tomorrow, _____.

13) They would go boating after a busy working day, if _____.

14) If you should change your mind, _____.

15) If it was possible, _____.

Ex. 2. Put the verb into the correct form (Appendix 4):

1) If she ___ (to go) abroad, she ___ (to be) very happy.

2) I ___ (to visit) him in the hospital, if I ___ (to have) free time.

3) If we ___ (not to like) his suggestion, we ___ (to tell) him about it.

4) If John ___ (to want) the advice, he ___ (to ask) you.

5) If you ___ (to have) better qualification, you ___ (to be able to) apply for better job.

6) If you ___ (to want) to find necessary information, you ___ (to surf) the net.

7) If somebody ___ (to steal) your collection of stamps, you ___ (to call) the police.

8) If I ___ (to have) a billion dollars, I ___ (to travel) around the world.

9) You ___ (to feel) better, if you ___ (to go to bed) earlier.

10) You ___ (to have) free time, if you ___ (to do) everything in time at work.

11) If he ___ (not to lose) his ticket, he ___ (to go) home by train.

12) If you ___ (to ask) a militia officer, he ___ (to help) you to find your baggage.

13) Don't be nervous if you ___ (to hear) bad news.

14) Our group ___ (to go) to Paris, if we ___ (to win) the competition.

15) If I ___ (to know) her phone number, I ___ (to phone) her.

	If-clause	Main clause	use	Example
Type 0	If + any present form	Present Simple	Real - for general truth	If you heat the water, it boils.
Type 1 Real	If + any present form	Future / Imperative can/	Real - likely to happen in the	If you work hard, you'll be tired.
Type 2 Unreal	If + Past Simple / Past	Would/ could/ might + bare inf.	Unreal-unlikely to happen in the	If I were you, I wouldn't judge him.
Type 3 Unreal	If + Past Perfect/ Past	Would/ could/ might + have +	Unreal situation in the past; also used to	If you had locked the car, it wouldn't have

Ex 3. Work in pairs. Make a dialogue. Student A is a police officer. Student B is a tourist. Discuss all unpleasant situations which can happen with a tourist and the preventive methods:

e.g. A: If you go abroad on holiday, you should know the laws of the country you are going to.

B: Yes, I know, but I'd like to clarify some points. What should I do if I lose my passport?

A: If you do it, you should go to a militia station and…

Ex.4. Transform the sentences, using "I wish" (see Appendix 3):

1) I'd love to know five foreign languages.

2) Why don't we go to the restaurant more often?

3) She hates working on Saturdays.

4) He'd love to investigate this case.

5) I'd like to live in Great Britain.

6) They hate playing board games after dinner.

7) They didn't go to the party.

8) He decided to stop working as a detective.

9) He lost all his money.

10) Unfortunately, I didn't tell you the truth.

Ex 5. Imagine that you are a wizard and you can change your life.

Tell your group what you'd like to change. Use "I wish".

Ex. 6. Put the verb in brackets into the correct form (see Appendix 3).

1) I wish I ___ (to hang out with friends) after a busy working day.

2) He fell and broke his leg pursuing the criminal. I wish he ___ (to be) more careful.

3) I wish you ___ (to read) more English books in future, because it is necessary for working abroad.

4) I can't remember where I've put my binoculars. I wish I ___ (to can).

5) I wish I ___ (not to lend) him my new car. He has broken it.

6) My watch has stopped. I wish I ___ (to have) a better watch.

7) I feel so tired. I wish I ___ (not to stay up) so late last night.

8) I wish I ___ (not to spend) all my money last night.

9) I wish he ___ (to present) me his painting.

10) I wish I ___ (to watch) comedy show after stressful working day.

Ex.7. In pairs write a short story on "The ideal working day of a police officer".

Use "I wish" constructions. Write 80-100 words. (see Appendix 3)

Ex.8. Choose one correct variant

1. If she is as clever as you say, she ___ rich by now.

a) will be b) would be c) would have been

2. If he had finished his work yesterday, he ___ free now.

a) would be b) would have been c) will be

3. If I were you, I ___ the facts before I accused them.

a) would check b) will check c) would have checked

4. If she were in your position, she ___ him by now.

a) will help b) would help c) would have helped.

5. They ___ that expedition if they have enough free time.

a) will join b) would join c) would have joined

6. If her neighbors are too noisy, she always ___.

a) complains b) complained c) has complained

7. I wish cadets ___ more fashionable clothes.

a) wear b) wore c) worn

8. I wish she ___ more pleasant to the victims of the robbery.

a) had been b) is c) will be

9. I wish they ___ me more.

a) pay b) paid c) would pay

10. If they liked that souvenir, they ____ it.

a) will buy b) would buy c) would have bought

Ex. 9. Put the verbs in brackets into the correct tense:

"If you don't call the police, you 1)_____ (never find) your collection of badges". I remember my relatives saying me these words when my house was robbed. If I 2)_____ (listen) to them, I 3)_____ (get) back my badges. If I 4)_____ (explain) the situation to a police officer, he certainly 5)_____ (help) me. If I 6)_____ (can / change) anything about that situation, I 7)_____ (get) my badges back. But for me, everything8)_____ (find) and the thief 9)_____ (punish). If only I 10)_____(understand) it earlier.

ENGLISH-RUSSIAN VOCABULARY

A

accept- принимать

access- 1) доступ, 2) проход, подход, 3) выборка информации

according(to)- соответственно

active- 1) деятельный, активный; 2) действующий

add- прибавлять, присоединять

additional- добавочный, дополнительный

allow- позволять, разрешать

appearance- внешний вид, наружность

append- прибавлять, добивать

appendix- приложение

apply- использовать применять

archive- архив

arrange- приводить в порядок, систематизировать

assign- назначать, определять

attach- прикреплять, присоединять

attempt- 1) попытка 2) пытаться

attribute- свойства

avoid- избегать

B

backslash- обратная косая черта

back-up - дублирование

basic - основной, главный

batch - 1) ряд, партия 2) группа, серия

belong - принадлежать

blink - мерцание

boot - осуществить первоначальную загрузку

bootable - способный выполнить первоначальную загрузку

break - прерывать

buffer - 1) буфер 2) промежуточная область памяти

bug - ошибка, дефект, помеха

build - строить

build into - встраивать

C

cable - кабель, провод

capital - заглавная буква

carry on - продолжать

carry out - выполнять

cause - вызывать, быть причиной

caution - 1) осторожность 2) предосторожность

chain - последовательность, цепь

change - заряд, заряжать

check - проверять

choice - выбор

circular - круглый

clear - 1) чистый 2) очищать

close - закрывать

cluster - 1) группа 2) кластер, пакет, блок

code - 1) код 2) программа 3) кодировать

combine - объединять, комбинировать

compare - сравнивать

compatible - совместимый

complete - полный, законченный

completely - современно, полностью

compute - вычислять

connect - соединять

conserve - сохранять

consist (of) - состоять (из)

consistent - последовательный, совместный

console - 1) кронштейн 2) пульт

contain - содержать в себе

contents - содержимое

contiguous - смежный, соприкасающийся

continue - продолжать

control - управление, контроль, регулировать

cord - шнур

correct - правильный

correspond - соответствовать

cover - покрывать

current - 1) текущий 2) течение, ток

D

deal - заниматься чем-либо, иметь дело

debug - устранять неполадки, неисправности

define - определять

delete - стирать

deny - отрицать, отказываться

design - проектировать, предназначать

destination - назначение

destination disk - диск, на который ведется запись

destroy - разрушать

differ - отличаться, разлагать

direct - руководить, направлять

directory - директория

default directory - директория, имя которой можно не указывать

disk - диск

blank disk - гибкий диск

double-density disk- диск с удвоенной плотностью

double-sided disk - двустороний диск

master disk - диск оригинал

MS DOS installed disk - инсталляционный диск для установки операционной системы

single-sided disk - диск, с которого осуществляется копирование

write-protected disk - диск, защищенный от записи

divide - разделять

drive - дисковод

default drive - дисковод используется по умолчанию

external floppy disk drive - внешний дисковод

internal floppy disk drive - встроенный дисковод

drive identifier - идентификатор дисковода

E

echo - отображение выполненных команд на экране

edit - редактировать

editor - редактор

embedded - встроенный, включенный

empty - пустой

encounter - встречаться

entire - полный, целый, весь

equal - одинаковый

error - ошибка

disk error writing - ошибка допущенная при записи данных на диск

disk error reading - ошибка, допущенная при считывании

divide error - ошибка, допущенная при делении

escape - выход из текущего режима

exceed - превышать

except - кроме

except for - за исключением

executable - выполнимый

executive - исполнительный

extend - расширять, продлить

extension, file extension - расширение имени файла

extra - добавочный

extremely - крайне, чрезвычайно

F

fail - потерпеть неудачу

failure - отказ, сбой

fast - быстро

file - файл

batch file - файл, содержащий группу команд

finite -ограниченный

fit - соответствовать

fix - укреплять, закреплять

floppy - гибкий

follow - следовать

font - шрифт

format - 1) формат, 2) форматировать

H

halt - остановка

handle - управлять, оперировать

handler - программа обработки

handy - удобный

hard - жесткий

harm - вред, ущерб

hide - прятаться

hold - держать

I

identify - идентифицировать

illegal - недопустимый

include - включать, содержать в себе

indicate - показывать

initialize - инициализировать, устанавливать в исходное положение

input - 1) ввод информации, 2) информация на входе

insert - вставлять

install - устанавливать

interchangeably - заменяя друг друга

italics - курсив

J

job - задание, задача, работа

joint - соединяться

K

keep - иметь, хранить

kind - сорт, разновидность, класс

L

label - 1) метка, 2) маркировать, различать

leftmost - крайний левый

level - уровень

link - связь, соединение

list - список

locate - устанавливать

lowercase - нижний регистр

M

manage - руководить, управлять

menudriven - (программа) управляемая с помощью меню

message - сообщение

multilevel - многоуровневый

N

nest - 1) гнездо, 2) вставлять

network - сеть

notation - обозначение

notch - метка

numerical – числовой, цифровой

O

occupy – занимать, заполнять

option - выбор

optional – необязательный

order – 1) порядок 2) исправное состояние

overcome – преодолеть

overflow – переполнение

overview - обзор

overwrite – переполнить записью

P

path – тропа, путь к файлу

permit - разрушать

point – точка, пункт

portable – портативный, переносной

porition – часть, доля

power - мощность

powerful – сильный, мощный

press – жать, давить

prevent – предотвращать

previously – предварительно, заранее

primary – первоначальный

prompt – напоминание, подсказка

proper – правильный, надлежащий

protect – защищать

provide – обеспечивать

R

range – диапазон, предмет

rate – норма, скорость, степень

receive – получать, принимать

record – записывать, запись

recover – возвращать, восстанавливать

reload – перезагружать

remainder – остаток

remark – примечание

remove – передвигать

rename – переименовывать

repeat – повторять

replace – заменить

report – сообщать

require – требовать, нуждаться

reserved – запасной, резервный

reset – перенастроить

response – 1) ответ 2) реакция

restart – начинать снова

return – возвращение

review – рассматривать

S

safe – безопасный

sample – образец, шаблон, модель

schedule – список, каталог

select – отбирать

separate – отделять

sequence – последовательность

serial port – разъем

series – ряд, серия

session - сеанс работы с системой

set - устанавливать, назначать

share - разделять

shell - оболочка

shift - сдвиг

side - сторона

similar - подобный

skip - пропускать, перепрыгивать

slash - разрез, косая черта

specification - спецификация, перечень

specify - определять

spot - место

start-up - 1) начало, пуск, 2) начинать

string - ряд, последовательность

substitute - заменять, замещать

sufficient - достаточный

support - 1) поддержка, 2) поддерживать

suspend - приостанавливать

switch - 1) переключение, 2) переключатель

T

tab - учет

table - таблица, график

target - цель

template - шаблон, модель

temporary - временный

term - термин

terminate - завершать, заканчивать

track - дорожка

transfer - перенос, перемещение

transmit - сообщать, передавать

turn – поворачиваться, turn on – включать, turn off - выключать

in turn - в свою очередь

U

unable - неспособный

unigue - уникальный

unless - если не, пока не

unlock - открывать

update - модернизировать

uppercase - верхний регистр

utmost - крайний, предельный

V

vary - меняться

verify - проверять, контролировать

NEW ENGLISH-ENGLISH TECH DICTIONARY

5G Connectivity

5G is the fifth generation of mobile networks. It is said to be up to 100 times faster than 4G and it can provide higher speed, lower latency, greater capacity, more reliability and a more uniform experience. **Examples include:** Autonomous vehicles, AR and VR, smart cities, immersive entertainment

Artificial Intelligence (AI)

AI, also known as machine intelligence, is intelligence demonstrated by machines, as opposed to natural intelligence displayed by humans and animals. It is the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. **Examples include**: self-driving cars, a virtual travel booking agent, manufacturing robots

Augmented reality (AR)

Augmented reality, or AR, is an enhanced version of the real (physical) world. AI is achieved through the use of digital elements via technology. **Examples include:** Snapchat, Google Street View, Pokémon Go

Big Data

Big data treats ways to analyze, systematically extract information from, or otherwise deal with data sets that are too large or complex to be dealt with by traditional data-processing application software. **Examples include:** Personalized marketing, finding new customer leads, medical records, social media

Blockchain

A blockchain is a decentralized, digitally distributed and often public ledger consisting of records called blocks that is used to record transactions across many computers so that any involved block cannot be altered

retroactively, without the alteration of all subsequent blocks. Blockchains store blocks of information in a chronological order that are irreversible and immutable. Blockchains are mostly known for their role in cryptocurrency systems such as Bitcoin.

Examples include: NFT marketplaces, electronic voting, tracking of music royalties

Cryptocurrency

Cryptocurrency is a digital or virtual currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority. Cryptocurrencies can also be defined as tradable digital assets or digital form of money built on blockchain technology that only exists online.

Examples include: Bitcoin, Ethereum, utility tokens

Datafication

Datafication, also known as datafy, is a technological trend that turns many aspects of our life (subjects, objects, and practices) into online quantified data which is subsequently transferred into information realised as a new form of value. It allows for real-time tracking and predictive analysis. **Examples of the datafication process include:** Netflix, or social platforms such as Facebook and Instagram that collect and monitor our data information in order to market products we would be interested in.

Data mining

Data mining is the process of extracting raw data and turning it into useful information by using software to look for patterns in large batches of data. **Examples include:** Cross-selling and upselling the Ecommerce sector, Collect and store data techniques in science and engineering

Digital Divide

The gap between those (individuals, households, businesses and geographic areas) who benefit from the Digital Age (who have ready access to

computers and the internet) and those who do not. **Examples/causes of the digital divide include:** Infrastructure, low literacy, low income levels

ALSO SEE: A beginner's guide to understanding technology

Digital twins

A digital twin is a virtual model, representation or replica that serves as the real-time digital counterpart, or mirror, of a physical object or process. **An example include:** Automotive manufacturers use digital twin technology to change the way cars are being made

Edge Computing

A distributed computing paradigm that brings computation and data storage closer to the sources of data.

Examples include: Cloud gaming, smart homes, predictive maintenance

Extended Reality (XR)

Extend Reality, or XR, is an umbrella term for AR, MR, VR, as well as other immersive technologies. XR refers to all real-and-virtual combined environments and human-machine interactions that are generated by technology and wearables.

Examples include: XR video games, XR tech devices, Zoom virtual backgrounds

Gig Economy

Workers in the Gig Economy are freelancers, part-time workers, independent contractors, temporary workers, etc. **Examples include:** Freelance writing, Web developing, Digital marketing

Hyperautomation

According to Gartner, a technological research and consulting firm, hyperautomation is a business-driven, disciplined approach that organizations use to rapidly identify, vet and automate as many business and IT processes as possible. It involves the orchestrated use of multiple technologies, tools or

platforms, including AI, machine learning, robotic process automation, etc. **Examples include:** Automating billing cycles, customer communication and collection in healthcare

Lossless audio

Lossless audio is all about the streaming process not affecting the quality of the sound. According to **Apple Music**, who announced in May 2021 that they're adding a lossless streaming service that will deliver uncompromised sound quality at no extra charge, most audio compression techniques lose some amount of data contained in the original source file. In short: Lossless compression is a form of compression that preserves all of the original data.

Metaverse

A virtual-reality space in which users can interact with a computer-generated environment and other users. Also known as a network of 3D virtual worlds focused on social connection.

Examples include: Ernest Cline's 2011 science fiction novel, *Reader Player One*, Fortnite Concerts, Augmented Reality (AR)

Mixed Reality (MR)

Mixed Reality, or MR, is the merging of the real and virtual worlds to produce new environments and visualizations, where physical and digital objects co-exist and interact in real time. MR is a combination of multiple advanced technologies, primarily AR and VR.

Examples include: Microsoft's Hololens, experiential education

Listen to the Future Females podcast: Lily Wu shares "Everything you need to know about NFT's and why we need more female representation in Web3" **here**.

Non-fungible token (NFT)

An NFT is a non-interchangeable unit of data, or a digital asset, stored on a blockchain that can be sold and traded. NFTs can't be exchanged for another

asset of the same type.

Examples include: Art, music, videos, real estate

ALSO SEE: NFTs: Learn from Lily Wu

Quantum Computing

A type of computation that harnesses the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations. Devices that perform quantum computations are known as quantum computers. Where conventional computers use bits, quantum computers use quantum bits known as qubits.

Examples include: AI, since quantum computers can analyze large amounts of data to provide AI machines feedback for improving performance

Robotics

The interdisciplinary branch of technology that deals with the design, construction, operation and application of robots. The goal of robotics is to design machines that can help and assist humans.

Examples include: AI powered robot assistants, drones, robotic toys, automotive industry robots, NASA's Robonaut

The Internet of Behaviors (IoB)

IoB refers to the gathering of data (from IoT as well as other sources) in order to predict human behavior, interests and preferences. It seeks to understand how, why and when people use technology when purchasing things.

Examples include: Digital marketing and personalized advertisements on social media

The Internet of Things (IoT)

The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data.

Examples include: Smart home security systems, wearable health monitors (Fitbit, Apple Watch, etc.), connected cars

Virtual Reality (VR)

Virtual Reality, or VR, is a simulated experience (making use of computer technology) that can be either similar to the real world, or completely different.

Examples include: VR as a treatment for mental health issues such as PTSD and anxiety, body-scanning technology in VR, gambling in VR

Voice-user interface (VUI)

A voice-user interface, or VUI, makes spoken human interaction with computers possible.

Examples include: Apple's Siri, Amazon's Alexa

ALSO SEE: 5 tips on how to pay yourself a salary

Web3

Web3, or Web 3.0, is an idea (or a work-in-progress) for a new iteration of the web known as the upcoming third generation of the internet. It will be based on blockchain technology, which will incorporate concepts such as decentralization and token-based economics. Information will be processed in a smart, human-like way through technologies such as machine learning and Big Data.

Did you know? Web 3.0 was previously known as the "semantic web"

White paper

White paper is a long piece of written content (such as a report or guide) viewed in eBook format. These white papers are used to explain a subject better.

ENGLISH-ENGLISH AUDIO VOCABULARY

SUPPLEMENTARY READING

An Introduction of Computer Forensics

An Introduction of Computer **Forensics** plays a vital role within the investigation and prosecution of cyber criminals the method includes acquisition, inspection, and news of data hold on across computers and networks related to a civil or criminal incident. Incident responders should be properly trained to extract, analyze, report, and investigate cases that involve technology because of the source or the victim of a crime.

This section discusses computer forensics and its role in incident handling provides an outline of pc forensic method, and explains the phases concerned in pc **forensics Investigation** method.

Computer Forensics

Computer Forensic may be a digital forensic division that deals with crimes committed across computing devices like networks, computers, and digital storage media. It refers to a group of method procedures and techniques to determine, gather, preserve, extract, interpret, document, and gift proof from computing instrumentation in such a manner that the discovered proof is appropriate throughout a legal and/or body continuing within the court of law.

In short, PC **forensics** deals with the method of finding proof associated with a digital crime to search out the culprits and take legal actions against them.

Listed below are the objectives of PC forensics:

– Identify, gather, and preserve the proof of a **cybercrime**.

– Track and prosecute the perpetrators within the court of law.

– Gather proof of cyber crimes in a very forensically sound manner.

– Find vulnerabilities and security loopholes that facilitate attackers.

– Understanding the usage of correct tools for varied forensic functions.

Role of laptop Forensics in Incident Handling

The incident response could be a method of developing a method to deal with the incidence of any security breach within the system or network. the method includes the formulation of security policy and goals of incident response; creation of incident response team; analysis of threats; establishing ways for detection a breach; and making ready to combat threats and mitigate damages within the event of a security breach.

Organizations produce incident response plans to accomplish goals such as:

– Develop and implement a powerful security policy

– Effectively monitor and analyze the systems and network traffic

– Ensure operational logs and work mechanisms

– Handle the incidents in a very manner that minimizes the injury and reduces recovery time and prices

– Map the pathway for extracting proof in a legally sound and acceptable manner

Define the role of an occurrence response skilled, like distinctive however breach occurred, a way to find the strategy of the breach, and the way to mitigate the breach On the opposite hand, laptop forensics could be a legal method of finding, gathering, analyzing, and presenting the proof in a very court of law to work out the perpetrator behind the incident. Organizations typically embrace laptop forensics as a part of the incident response commit to track and prosecute perpetrators of an occurrence.

There has been an associate exponential increase within the range of cybercrimes and litigation involving giant organizations. This has highlighted the **requirement** for laptop forensics. Organizations have to be compelled to use the services of a laptop forensics agency or rent laptop forensics professional to protect against laptop incidents or solve crimes that involve the utilization of computers and connected technologies. The staggering monetary losses caused

by laptop crimes have conjointly contributed to the revived interest in laptop forensics.

The most role of laptop forensics in incident handling is to:

– Prepare for incidents ahead to make sure integrity and continuity of network infrastructure.

– Identify and gather proof of laptop crimes in a very forensically sound manner.

– Determine the precise cause, nature, and impact of the incident.

– Generate a timeline for the incident that helps in correlating completely different incidents.

– Conduct a rhetorical analysis of the affected system that helps in deciding the character of incidents and impact of the incident.

– Identify and track the perpetrators of the crime or incident.

– Extract, process, and interpret the factual proof so it proves the attacker's actions within the court.

– Offer ample protection to information resources and guarantee regulative compliance.

– Protect organizations from similar incidents in future.

– Counteract on-line crimes like abuse, bullying, and name injury.

Minimize the tangible and intangible losses to a company or a person.

– Support prosecution of the offender of an occurrence.

– Save organizations cash and time by conducting an injury assessment of the exploited network.

– Save organizations from legal liabilities and lawsuits.

Digital forensics can be defined as a branch of forensic science dedicated to recovery and investigation of digital or electronic data. These data can be from any digital asset or data storing entity which includes a computer system, mobile device, cloud service, and so on. **Infosavvy gives training** on **incident handling** in how digital forensic work. **Accreditation by EC-Council**.

Questions related to this topic

1. What is Computer Forensics?
2. What are the objectives of Computer forensics?
3. What is the Role of laptop Forensics in Incident?

An Introduction of Computer Forensics | Info-savvy.com https://info-savvy.com/an-introduction-of-computer-forensics/

Anti-phishing Tools Guide

What are some easy anti-phishing tools?

An Anti-phishing Tools Guide toolbar is a outstanding way to assist alongside these who are much less computer-savvy. You can strive and train them how to become aware of and keep away from phishing attempts, however the truth is, they may also in no way turn out to be adept at it.

Doing a speedy search on the **web** can yield you many respectable free results. A free anti-phishing toolbar can also be enough for everyday day-to-day browsing, however we advocate you to additionally seem at anti-phishing carrier for your enterprise.

Toolbar at Netcraft

The Netcraft Toolbar provides updated information about the sites users visit regularly and blocks dangerous sites. The toolbar provides you with a wealth of data about the sites you visit. This information will assist you make an informed choice about the integrity of these sites.

Features:

- Protect your savings from Phishing attacks
- Observes the hosting location and risk rating of each website visited (as well as other information)
- Helps in defending the web community from fraudsters
- Checks if a web site supports Perfect Forward Secrecy (PFS)

- Observes if a web site is laid low with the aftermath of the Heartbleed **vulnerability**

PhishTank

PhishTank is a collaborative clearinghouse for **data and information** about phishing on the Internet. It provides an open API for developers and researchers to integrate anti-phishing data into their applications. learn more about **Anti-phishing tools in CEH from Infosavvy.**

Learning Good Ways To Protect Yourself From Identity Theft

Common Social Engineering Targets and Defense Strategies

Attackers implement various **social engineering** techniques to trick people into providing sensitive information about their organizations, thus helping the attackers in launching malicious activities. These techniques are used on privileged individuals, or those who have important information.

The table below shows common social engineering targets, various social engineering techniques an attacker uses, and the defense strategies to counter the attacks.

Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees / help desk never to Reveal passwords or other information by phone. Enforce policies for the front office and help desk personnel
Technical support and System administrators	Impersonation, persuasion, intimidation, fake SMS, phone calls, and emails	Train technical support executives and system administrators never to reveal passwords or other information by phone or email
Perimeter security	impersonation, reverse social engineering, piggybacking, tailgating, etc.	Implement strict badge, token or biometric authentication, employee training, and security guards
Office	Shoulder surfing, eavesdropping, ingratiation, etc.	Employee training, best practices and checklists for using passwords. Escort all guests.

Vendors of the target organization	Impersonation, persuasion, intimidation	Educate vendors about social engineering.
Mail room	Theft, damage or forging of mails	Lock and monitor mail room, including employee training
Machine room/Phone closet	Attempting to gain access remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment
Company's Executives	Fake SMS, phone calls and emails to grab confidential data	Train executives to never reveal identity, passwords or other confidential information by phone or email
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas, shred important data, erase magnetic media

Questions related to this topic

1. What are the three methods used in social engineering to gain access to information?
2. What are examples of social engineering techniques?
3. What is the term used for the technique used by phishing attacks to trick users into sharing confidential data?
4. What is the best defense against phishing?

Anti-phishing Tools Guide | Infosavvy Security and IT Management Training https://info-savvy.com/anti-phishing-tools-guide/

Concept of Security, Cyber Space & Cyber Crime

Concept of Security Cyber Space & Cyber Crime in this Cybercrime refers to the series of social group attacking each cyber space and cybercrime security. Cybercrime refers to criminal activity done exploitation computers and

also the net. It conjointly involves criminal access (unauthorized access, transmissions of pc knowledge, to, from or at intervals a computing system.

Understanding Security as a process

Security is a process, not an end state.

Security is the process of maintaining standard level of apparent risk. No organization can be considered "secure" for any time beyond the last verification of adherence to its security policy. If your manager asks, "Are we secure?" you should answer, "Let me check." If he or she asks, "Will we have a tendency to be secure tomorrow?" you should answer, "I don't know." Such honesty will not be popular, but this mind-set will produce greater success for the organization in the long run.

concept security is a part ***Certified Ethical Hacking v10(CEH v10)*** *training you learn the* ***cyber security attacks*** *and their impact.*

Security Features

• **Confidentiality:** It is roughly equivalent to privacy. Measures undertaken to confirm confidentiality are designed to stop sensitive data from reaching the incorrect folks, whereas ensuring that the proper folks will actually get it: Confidentiality is assurance that data is shared solely among approved persons or organizations.

• **Integrity:** Assurance that the information is authentic and complete. Integrity In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

• **Availability:** Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them. Availability of knowledge refers to making sure that approved parties are able to access the data once required.

Concept of Cyberspace:

With the arrival and growth of electronic transmission, the word "cyberspace" has entered into everyday formulation. But what does this word

signify? I begin by sketching equivalence between physical area and Internet, showing that they share the ideas of place, distance, size and route in common. With this mutual framework in place, I'm going on to look at numerous theories substantial, relational, physicist and Kantian concerning the character of physical area. We see that, whereas Internet shares a number of the properties of physical area isolated by every of those theories, still it cannot be subsumed under any one theory. We also see that cyberspace exhibits several novel properties, projecting it far beyond the scope of any existing theory and setting it apart as an exciting Cyberspace is "the environment in which communication over computer network happens." And almost everybody in one way or the other is connected to it.

Steps to Cyber Security

Certified Ethical Hacker | CEH Certification

Concept of Cybercrime

Computer crime, or cybercrime, is any offence committed over a computer and a network. Computers are utilized in the commission of a criminal offense, or it may be the target.

To better cybercrime understand, you can refer to below example.

Commonwealth bank, Australia – march 2011:- automatic teller machines (atms) spat outtens of thousands of free dollars in Sydney Tuesday after a computer glitch turned into a nightmare for the commonwealth bank. It security believe that it is a consequence of hacking.

As per University of Maryland, Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. The state of being protected against the criminal or unauthorized use of electronic information, or the measures taken to achieve this. 'Some folks have argued that the threat to cyber security has been somewhat inflated'.

Cyber security

Cyber security endeavors to confirm the realization and maintenance of the safety properties of the association and user's assets against relevant security risks within the cyber setting.

If you wish to learn ***Cyber security*** *and build a colorful career in* ***cybersecurity,*** *then check out our* ***Cyber security Certification & Training with infosavvy in Banglore Location*** *which comes with instructor-led live training and real-life project experience.* ***CEHv10 training*** *will help you understand* ***cyber security in depth*** *and help you achieve mastery over the subject.*

Questions related to this topic

1. What is cyber space security?
2. What are different methods of cyber security?
3. What is cybercrime introduction?
4. Who is responsible for cyber security in a company?
5. What is Concept of Security Cyber Space & Cyber Crime?

Concept of Security, Cyber Space & Cyber Crime | Info-savvy https://info-savvy.com/concept-of-security-cyber-space-cyber-crime/

Defend Against Key loggers

Defend against Key loggers are an increasingly common variety of malware threatening consumers today. Key logger programs record every keystroke the user makes, and **hackers** can use this data to decipher your passwords and other tip. Unfortunately, key loggers are very difficult to detect this suggests your information will be compromised for an extended time without you knowing it. Read on for more information on what key loggers are,

how they work, and the way you'll be able to prevent them from accessing your computer.

The following are some more ways to defend against key loggers:

– Use pop-up blockers and avoid opening junk emails – Install anti-spyware antivirus programs and keep the signatures up to now. – Install professional firewall software and anti-key logging software. – Recognize phishing emails and delete them. – Update and patch system software regularly to defend against key loggers – Do not click on links in unwanted or doubtful emails which will point to malicious sites – Use keystroke interference software, which inserts randomized characters into every keystroke – Antivirus and anti-spyware software is ready to detect any installed software, but it's better to detect these programs before installation. Scan the files thoroughly before installing them onto the pc and use a registry editor or process explorer to see for keystroke loggers.

– Use the Windows onscreen keyboard accessibility utility to enter the **password** or the other tip. you'll maintain your information confidentially because you employ mouse to enter any information like passwords and master card numbers into the keyboard, rather than typing the passwords using the keyboard.

– Use automatic form-filling password manager or a virtual keyboard to enter user names and passwords because they avoid exposure through key loggers, This automatic form-filling password manager will remove the utilization of typing your personal, financial, or confidential details like master card numbers and passwords through keyboards. – Keep your hardware systems secure in a very locked environment and regularly check the keyboard cables for the attached connectors, USB port, and computer games like the P52 that are accustomed install key logger software. – Use software that regularly scans and monitors the changes within the system or **network**.

– Install host-based IDS, which may monitor your system and disable the installation of key loggers.

Hardware Key logger Countermeasures

– Restrict physical access to sensitive computer systems. – Periodically check your keyboard interface to make sure that no extra components are plugged to the keyboard cable connector. – Use encryption between the keyboard and its driver. – Use an anti-key logger that detects the presence of a hardware key logger like Oxygen Key Shield. – Use an on-screen keyboard and click on thereon by employing a mouse.

Anti-Key loggers

. Anti-key loggers, also called anti-keystroke loggers, detect and disable keystroke logger software. Anti-key logger's special design helps them to detect software key loggers. Many urge organizations, financial institutions, online gaming industries, also as individuals use anti-key loggers for shielding their privacy while using systems. This software prevents a key logger from logging every keystroke typed by the victim and thus keeps all personal information safe and secure. An anti-key logger scans a **computer**, detects, and removes keystroke logger software. If the software (anti-key logger) finds any keystroke logging program on your computer, it immediately identifies and removes the key logger, whether it's legitimate keystroke logging program or an illegitimate keystroke logging program.

Some of the anti-key loggers detect the presence of hidden key loggers by comparing all files within the computer against a signature database of key loggers and checking out similarities. Other anti-key loggers detect the presence of hidden key loggers by protecting keyboard drivers and kernels from manipulation. A virtual keyboard or touch screen makes the keystroke capturing job of malicious spyware or Trojan programs difficult. Anti-key loggers secure your system from **spyware**, key loggers.

Zemana Anti Logger

Zemana Anti Logger may be a software application that blocks hackers. It detects any attempts to change your computer's settings; record your activities, hook to your PCs sensitive processes, or inject malicious code in your system. It protects your computer from key logger and malware attacks, thereby protecting your identity. The Anti Logger detects the malware at the time it **attacks** your system instead of detecting it supported its signature fingerprint. It'll prompt you if any computer virus is attempting to record the keystrokes of your system, capture your screen, gain access to your clipboard, microphone, and webcam, or inject itself into any sensitive areas of your system.

Defend Against Spyware

Zemana Anti-logger provides protection against various threats like SSL logger, webcam logger, Key loggers, clipboard and screen logger, spyware, Trojans, and so on.

In **cybersecurity** there are so many different attacks are there in which one of the most happen attack is stealing user data using of **keylogger**. keylogger captures all the data which you type with your keyboard and hacker trace that data. mostly data can be login id or password. **Infosavvy gives Training** on **CEHv10 Course** in which you will learn in details of these types of attacks.

Questions related to this topic

1. Can a key logger be detected?
2. Will a key logger record passwords?
3. Is Key logger a malware?
4. What type of malware is a key logger program?

Defend Against Key loggers | Info-savvy https://info-savvy.com/defend-against-key-loggers/

Defend Against Spyware

Spyware

Spyware is defended any computer virus installed into a user's system without the user's knowledge and gathers tip like personal data and access logs.

Spyware comes from three basic sources:

Free downloaded software, email attachments, and websites that automatically install **spyware** once you browse them.

Here are ways to defend against spyware:

- Try to avoid using any computing system which isn't totally under your control.
- Never adjust your Internet **security** setting level too low because it provides many chances for spyware to put in on your computer. So, always set your Internet browser security settings to either high or medium to defend your computer from spyware.
- Don't open suspicious emails and file attachments received from unknown senders. there's an excellent likelihood that you simply will get an epidemic, freeware, or spyware on the pc. Don't open unknown websites present in Spam mail messages, retrieved by search engines, or displayed in pop-up windows because they'll mislead you to download spyware.
- Enable a Firewall to boost the protection level of your computer
- Update the **software** regularly and use a firewall with outbound protection
- Regularly check task manager report and MS configuration manager report
- Update virus definition files and scan the system for **spyware** regularly
- Install anti-spyware software. Anti-spyware protects against spyware. Anti-spyware is the first line of defense against **spyware**. This

software prevents spyware installed on your system. It periodically scans your system and protects your system from spyware.

- Keep your OS up so far.
- For other users, using other operating systems or software products, ask the knowledge given by the operating system vendors, and take essential steps against any **vulnerability** identified.
- Perform web surfing safely and download cautiously
- Before downloading any software, confirm that it's from a trusted website. Read the 'license agreement, security warning, and privacy statements related to the software thoroughly to urge a transparent understanding before you download.
- While downloading freeware or shareware from an online site, make sure that the location is safe. Likewise, take care of software programs obtained through PP file-swapping software. Before installing such programs, perform a scan using anti-spyware software
- Do not use administrative mode unless it's necessary because it's going to execute malicious programs like spyware within the administrator mode. As a result, attackers may take complete control over your system,
- Do not download free music files, screensavers, or smiley faces from the web because after you download such free programs, there's a chance that spyware comes beside them invisibly.
- Beware of pop-up windows or sites, Never click anywhere on the windows that display messages like your computer could also be infected, or that they will help your computer to run faster. once you click on such windows your system may get infected with spyware.
- Carefully read all disclosures, including the license agreement and privacy statement before installing any application
- Do not store personal or financial information on any computing system that's not totally under your control, like in an online cafe.

Anti-Spyware

There are many anti-spyware applications available within the market, which scan your system and check for spyware like malware, Trojans, Dialers, worms, **key loggers**, and rootkits, and take away them if found. Anti-spyware provides real-time protection by scanning your system at regular intervals, either weekly or daily. it scans to confirm the pc is free from malicious software.

SUPER Anti Spyware

SUPER Anti Spyware may be a software application which might detect and take away spyware, adware, Trojan horses, rogue security software, computer worms, rootkits, parasites, and other potentially harmful software applications.

Features:

– Defend and take away Spyware, Adware and take away Malware, Trojans, Dialers, worms, key loggers, hijackers, Parasites, Rootkits, Rogue Security Products and lots of other sorts of **threats**.

– Repair broken Internet Connections, Desktops, Registry Editing and more with our unique Repair System.

– Real-lime Blocking of threats. Prevent potentially harmful software from installing or re-installing.

– Configure SUPER Anti Spyware to send you an e-mail with the results from specific actions. Schedule either quick, complete or custom scans Daily or Weekly to confirm your computer is free from harmful software. Remove spyware automatically.

Some of the anti-spyware programs are listed below:

- Kaspersky Internet Security 2018
- Secure Anywhere Internet Security Complete
- Adaware antivirus free
- MacScan
- NortonAntiVirusBasic

- Spybot -Search&Destroy
- SpyHunter
- Malwarebytes for Windows
- ZemanaAntimalware
- HitmanPro
- EmsisoftAntimalware
- DigitalCareAntiVirus
- SpywareTerminator 2015

Questions related to this topic

1. What is the best free anti-malware software?
2. What is the best software to remove viruses?
3. How do I scan for malware with Windows Defender?
4. What is the best free malware protection for Windows 10?

Different types of tools with Email Foot printing

Email Foot printing

Different types of tools with Email Foot printing, So far we have discussed foot printing through search engines. foot printing using Google, foot printing through **social networking sites**, and website foot printing. Now we will discuss email foot printing. This section describes how to track email communications, how to collect information from email headers, and email tracking tools.

EC-Council Certified Incident Handler | ECIH v2

Tracking Email Communications

Email tracking monitors the emails of a particular user. This kind of tracking is possible through digitally time stamped records that reveal the time and date when the target receives and opens a specific email. Email tracking tools allows an attacker to collect information such as IP addresses, mail servers,

and service provider involved in sending the mail. Attackers can use this information to build a hacking strategy and to perform **social engineering** and other attacks. Examples of email tracking tools include ervlailTrackerPro, Yesware, Contactrvlonkey and so on.

Information gathered about the victim using email tracking tools:

Recipient's system IP address: Allows to track the recipients IP address

Geo location: Estimates and displays the location of the recipient on the map and may even calculate the distance from the attacker's location

Email received and Read: Notifies when the email is received and read by the recipient

Read duration: The duration of time spent by the recipient on reading the mail sent by the sender

Proxy detection: Provides information about the type of server used by the recipient

Links: Checks whether the links sent to the recipient through email have been checked

Operating system and Browser information: Reveals information about the operating system and the browser used by the recipient. The attacker can use this information to find loopholes in that version of operating system and browser, in order to launch further attacks

Forward Email: Determines whether the email sent to the user is forwarded to another person

Device Type: Provides information about the type of device used to open and read the email e.g., desktop computer, mobile device, or laptop. Email is one of our main forms of communication in the business world. Learn why email addresses and company directories are coveted target for a **hacker**. Lisa Bock reviews why it is important to limit your exposure of your company email lists because of Spearfishing, spoofing and identity theft risks.

Secure email by streak

Secure Gmail encrypts and crypts emails you send in Gmail. This happens all on your machine, and the encrypted text never reaches Google servers. This is useful if you don't want anyone but the intended recipient to ever read your email (i.e. companies, governments, etc.)

How secure is it?

Secure Gmail uses symmetric encryption to encrypt and decry-pt each message. The password is decided by the user and assumes the recipient already knows it. Secure Gmail is only as good as your password, pick an easy to guess password and it will be easy to break. Shared knowledge can be a useful and convenient password. Remember to never email or IM your password for others to intercept.

– Secure Gmail – send encrypted email.

– Enter **"Secure"** compose mode. Entering secure mode is easy, its right next to the compose button.

-Easy Security. Encrypting your messages are simple, you just need to enter a password that your recipient will know.

Email Tracking Tools

Email tracking tools allow an attacker to track an email and extract information such as sender identity, mail server, sender's IP address, location and so on. These tools send notifications automatically when the recipients open the mail and gives status information about whether the email was successfully delivered or not. **Attackers** use the extracted information to attack the target organization's systems by sending malicious emails.

Questions related to this topic

1. How do I find the IP address of an email sender in Gmail?
2. Can you trace a Gmail account?
3. How can you find an IP address from an email?
4. what are the Different types of tools with Email Foot printing?

Enterprise Information Security Architecture

Information Security Architecture

Enterprise Information Security Architecture is a set of requirements, processes, principles, and models that determine the current And/or future structure and behaviour of an organization's security processes, information security systems, personnel, and organizational sub-units. It ensures that the security architecture and controls are in alignment with the organization's core goals and strategic direction. Though Enterprise **Information Security** Architecture deals with information security, it relates more broadly to the security practice of business. Optimization. Thus, it also addresses **business** security architecture, performance management and security process architecture. The main objective of implementing EISA is to make sure that IT security is in alignment with business strategy.

Enterprises are struggling nowadays to achieve the balance between implementing the **security** controls in the enterprise while allowing the employees to increase the productivity and communicate the information easily. Enterprise security is not only about protecting the infrastructure of the enterprise, but also the sensitive data flowing among the organization. Security of enterprise is done in a generic manner by applying three ways [1, 2]:

Prevention – This involves preventing the networks from intruders by avoiding security Breaches. This is normally done by the implementation of firewalls.

Detection – This process focuses on the detection of the **attacks** and the breaches that are done over the network.

Recovery – Once an attack occurs, recovery is essential for preventing the information asset of the enterprise that may damage due to the attack. For this, some recovery mechanisms are being employed by the enterprises. Till date,

most of the researches and works have been done in the area of prevention and detection of the attack.

Enterprise Information Security Architecture (EISA) could be a key component of an information security program. the first function of **EISA** is to document and communicate the artifacts of the safety program during a consistent manner. As such, the first deliverable of EISA could be a set of documents connecting business drivers with technical implementation guidance. These documents are developed iteratively through multiple levels of abstraction.

EC-Council Security Analyst v10 | ECSA

Motives behind enterprise security

Enterprise security is getting difficult primarily due to the following reasons A. Increasing threats- Enterprise organizations are continuously attacked by newer With the aim of stealing the confidential information. **Cybercriminals**, hackers are growing in a large number. It has been reported that in recent years, malware are worse than previous attacks. Further, crime is getting more sophisticated these days. All these factors need to be managed. B. Technology Complexity – **Security experts** are dealing with threats as well as maintaining the change with the effect of the new technologies like cloud computing, mobile computing, Internet of things and virtualization. These new technologies are creating a gap within the system which need to be addressed. C. Legacy security procedures and techniques: From the past, many security techniques have been used in the enterprises starting from firewalls, **Intrusion Detection System/ Intrusion Prevention System (IDS/IPS)**, to host security software (i.e., antivirus software), and to security monitoring and compliance tools (i.e., SIEM, log management, etc.). These procedures are incapable of dealing with the multidimensional threat.

What is an Information Security Incident?

There exist multiple security standards for securing and protecting the assets of the enterprises. Some organizations use the published security standards while others implemented their own security architecture depending on their requirement. There is no single uniform standard that can be applied to all enterprises. By incorporating the recommended policies and programs, effective and consistent security architecture can be developed.

Trends in enterprise security

Due to the incorporation of cloud and mobile applications, the security needed by the enterprise has been increased at a wider level. The attacks are changing day by day and so this necessitates more secure information environment. Thus these trends suggest that further improvement is needed in the security architectures of the enterprises.

- Encrypted data
- DDoS (Distributed Denial of Service Attack
- Managed Security Service
- Single platforms forsecure
- Increased Customer expectation
- Data collection and process
- Malware analytic
- Intelligent algorithm

The following are the goals of EISA:

– To help in monitoring and detecting network behaviors in real time acting upon internal and externals security risks.
– To help an organization detect and recover from security breaches.
– To aid in prioritizing resources of an organization and pay attention to various threats.
– To benefit the organization in cost prospective when incorporated in security provisions such as **incident response**, disaster recovery, and event correlation, etc.

– To help in analyzing the procedures needed for the IT department to identify assets and function properly.
– To help perform **risk assessment** of an organization's ET assets with the cooperation of IT staff.

Questions related to this topic

1. What is Enterprise Information Security Architecture ?
2. What is Trends in enterprise security ?
3. What is Motives behind enterprise security?

Essential Terminology in Cyber security

Here are some terms and their definition, you must know before you start studying ethical hacking. As cyber security technology grows and expands, so does the vocabulary associated with it.

Hack Value:

It is the notion among hackers that one thing is price doing or is interesting. Hack value will be a playful disruption. It's additionally maintenance for the imagination, surprise the far side tedium of living in a client, dominated culture.

It crossovers between different fields and practices, regard their achievements and approaches in hacking instead of specific genres. Like alternative chapters a number of the artworks and comes exist their own right, inside and outside of gallery context.

Alternative examples either play with or disrupt things through cultural enactments of communication with others. These embody publications, farming, food distribution and public heritage sites. All the comes and works studied are social. Some are political and a few are participatory.

This includes works that use digital networks and physical environments also as written matter. What binds these examples along isn't solely the

adventures. They initiate once experimenting with alternative ways that of seeing, being and thinking.

They additionally share common intentions to loosen the restrictions, distractions and interactions dominating. The cultural interfaces, facades and structures in our everyday surroundings. Hack value is the notion among hackers to evaluate something that is worth doing or is interesting. Hackers derive great satisfaction from breaking down the toughest network of cyber security . They consider it their accomplishment as no one can do.

6 Quick Methodology For Web Server Attack

Vulnerability:

Vulnerability is the existence of weakness, design when exploited, leads to an unexpected and undesirable event compromising. Simply that allows an attacker to enter the system by bypassing various user authentications. Vulnerability comes from the Latin word for “wound,” values. Vulnerability is that the state of being open to injury, or showing as if you’re. It would be emotional, like admitting that you are loving with somebody who would possibly solely such as you as a friend, or it will be literal, just like the vulnerability of a soccer goal that is unprotected by any defensive players. Vulnerability is that the existence of a weakness (design or implementation error) which will result in a surprising event compromising the protection of the system.

Exploit:

An exploit is breach of IT system security through vulnerabilities, in the context of an attack on system or network. Exploitation is that the next step in an attacker’s playbook when finding a vulnerability. Exploits are the means that through that a vulnerability may be leveraged for malicious activity by hackers; these include pieces of software system, sequences of commands, or maybe open supply exploit kits. An exploit could be a code that takes advantage of a software vulnerability or security flaw.

It’s written either by cyber security researchers as a proof-of-concept threat or by malicious actors to be used in their operations. When used, exploits enable an intruder to remotely access a network and gain elevated privileges, or move deeper into the network. It also refers to malicious software or commands that can cause unanticipated behavior of legitimate software or hardware through attackers taking advantage of the vulnerabilities. Exploit could be a breach of an IT system of cyber security through vulnerabilities.

Payload:

Payload is the part of a malware or an exploit code that performs the intended malicious actions, which can include creating backdoor access to a victim’s machine, damaging or deleting files, committing data theft and hijacking computer. Hackers use various methods to execute the payload. Payload is that the part of an exploit code that performs a supposed malicious action. For example, they can activate a logic bomb, execute an infected program, or use an unprotected computer connected to a network.

In computing, a payload is that the carrying capability of a packet or different transmission information unit. The term has its roots within the military and is usually related to the capability of practicable malicious code to try and do injury. Technically, the payload of a particular packet or different protocol information unit (PDU) is that the actual transmitted information sent by act endpoints; network protocols additionally specify the most length allowed for packet payloads.

Certified Ethical Hacker | CEH Certification

Zero-Day Attack:

in a Zero-Day attack, the attacker exploits vulnerabilities in a computer application before the software developer can release a patch for them. A Zero-Day attack is an attack that exploits the PC vulnerability before software engineer releases a patch. Based on common usage of exploit terms, an exploit

is said as a zero-day exploit once it's wont to attack a vulnerability that has been identified however not yet patched, additionally called a zero-day vulnerability.

Daisy Chaining:

It involves gaining access to one network and/or computer and then using the same information to gain access to multiple networks and computers that information. Daisy chaining involves gaining access to a network and /or laptop and so exploitation constant data to realize access to multiple networks and computers that contain desirable data.

Doxing:

Doxing is publication in person identifiable data concerning a private or organization. It refers to gathering and publishing personally identifiable information such as an individual's name and email address, or other sensitive information pertaining to an entire organization. People with malicious intent collect this information from publicly accessible channels such as the databases, social media and the Internet.

Bot:

A "bot" (a contraction of "robot") is a software application or program that can be controlled remotely to execute or automate predefined tasks. Hackers use buts as agents that carry out malicious activity over the Internet. Attackers use infected machines to launch distributed denial-of-service (DDoS) attacks, key logging, spying, etc. bot could be a software system application which will be controlled remotely to execute or alter predefined tasks.

Warfare:

Warfare or info war refers to the use of data and communication technologies to require advantage of an opponent.

Hacking:

Hacking is unauthorized attempts makes an attempt tries to bypass the protection mechanisms of a data system or network.

Hacker:

Hacker is a person with wonderful computer skills, with the flexibility to create and explore computer code and hardware.

Ethical hacking:

is that the use of hacking tools and tricks to spot vulnerabilities therefore on guarantee system security.

People also ask Questions

1. What software do hackers use to hack?
2. What is the most dangerous hacker tool?
3. Has your computer been hacked?
4. How does a hacker get your password?

TEN Different Types Of Hackers

Hackers

TEN Different Types Of Hackers In computing, a hacker is any skilled computer expert that uses their technical knowledge to overcome a problem. While "hacker" can refer to any skilled computer programmer, the term has become associated in popular culture with a **"security hacker"**, someone who, with their technical knowledge, uses bugs or exploits to break into computer systems. Hacker usually fall into one of the **following categories**, according to their activities:

1. Black Hats Hackers

Taking credit for the negative persona around "hacking," these guys are your culprits. A black hat hacker is that the sort of hacker you ought to be worried. Heard a news a few new cybercrime today? one among the black hat hackers could also be behind it. While their agenda could also be monetary most of the time, it's not always just that. These hackers search for vulnerabilities in individual PCs, organizations and bank systems. Using any loopholes they'll find, they will hack into your network and obtain access to your personal,

business and financial information. Black hats are individuals who use their extraordinary computing skills for illegal or malicious purposes. This category of hacker is often involved with criminal activities. They are also known as crackers.

Certified Ethical Hacker | CEH Certification

2. White Hats Hackers

Meet the right guys on the **dark web**. White hat hackers, also referred to as **ethical hackers** are the cyber security experts who help the govt. and organizations by performing penetration testing and identifying loopholes in their **cyber security**. They even do other methodologies and ensure protection from black hat hackers and other malicious cyber crimes. Simply stated, these are the right people that are on your side. they're going to hack into your system with the great intention of finding vulnerabilities and help you remove virus and malware from your system.

3. Gray Hats Hackers

Gray hat hackers fall somewhere in between white hat and black hat hackers. While they'll not use their skills for personal gain, they can, however, have both good and bad intentions. as an example , a hacker who hacks into a corporation and finds some vulnerability may leak it over the web or inform the organization about it. It all depends upon the hacker. Nevertheless, as soon as hackers use their hacking skills for personal gain they become black hat hackers. there's a fine line between these two. So, let me make it simple for you. Because a gray hat hacker doesn't use his skills for personal gain, he's not a black hat hacker. Also, because he's not legally authorized to hack the organization's **cyber security**, he can't be considered a white hat either.

4. Blue Hats Hackers

These are another form of novice hackers very similar to script kiddies whose main agenda is to require revenge on anyone who makes them angry. they need no desire for learning and should use simple cyber attacks like

flooding your IP with overloaded packets which can result in **DoS attacks**. A script kiddie with a vengeful agenda are often considered a blue hat hacker.

5. Suicide Hackers

Suicide hackers are individuals who aim to bring down critical infrastructure for a **"cause"** and are not worried about facing jail terms or any other kind of punishment. They are similar to suicide bombers, who sacrifice their life for an attack and are thus not concerned with the consequences of their actions.

6. Script Kiddies Hackers

A derogatory term often used by amateur hackers who don't care much about the coding skills. These hackers usually download tools or use available hacking codes written by other developers and hackers. Their primary purpose is usually to impress their friends or gain attention. However, they don't care about learning. By using off-the-shelf codes and tools, these hackers may launch some attacks without bothering for the quality of the attack. Commonest cyber attacks by script kiddies might include **DoS and DDoS attacks**.

7. Malicious Insider or Whistle blower

A malicious insider or a whistle blower could also be an employee with a grudge or a strategic employee compromised or hired by rivals to garner trade secrets of their opponents to remain on top of their game. These hackers may take privilege from their quick access to information and their role within the corporate to hack the system.

8. Red Hat Hackers

Red Hat Hackers have an agenda almost like white hat hackers which in simple words is halting the acts of Black hat hackers. However, there's a serious difference within the way they operate. they're ruthless when it involves dealing with black hat hackers. instead of reporting a malicious attack, they believe taking down the black hat hacker completely. Red hat hacker will launch a series

of aggressive cyber attacks and malware on the hacker that the hacker may also have to replace the entire system.

8 Most Common Types of Hacker Motivations

9. State/Nation Sponsored Hackers

State or Nation sponsored hackers are those that have been employed by their state or nation's government to snoop in and penetrate through full security to realize tip from other governments to stay at the highest online. they have an endless budget and extremely advanced tools at their disposal to target individuals, companies or rival nations.

10. Hacktivist Hackers

Hacktivist is when hackers break into government or corporate computer systems as an act of protest. Hacktivists use hacking to increase awareness of their social or political agendas, as well as themselves, in both the online and offline arenas. They are individuals who promote a political agenda by hacking, especially by defacing or disabling websites. Common hacktivist targets include government agencies, multinational corporations, or any other entity that they perceive as a threat. It remains a fact, however, that gaining unauthorized access is a **crime**, irrespective of their intentions.

Questions related to this topic

1. What is a red hat hacker?
2. What are the 3 types of hackers?
3. What is a good hacker called?
4. What software do hackers use?
5. What are the TEN Different Types Of Hackers?

Top 8 Cyber security Skills You Must Have

Last updated on Apr 11, 2022

Table of Contents

With businesses increasingly moving online and shifting to cloud storage, the demand for cyber security is currently at its peak. With that milestone comes a high demand for cyber security experts who can safeguard digital data. A good cyber security professional must possess a rich and diverse skill set. In this tutorial, we will explore the top eight cyber security skills (expanded from five, due to popular new advances!) that will help you get into the field of cyber security.

Top 5 Cyber security Skills

1. Networking and System Administration

- An in-depth understanding of networking is required to start a career in cyber security. Learning networking will help you understand data transmission's technical aspects, which will help you secure your data. Taking up networking certifications like CompTIA Security+ and Cisco CCNA is advisable.
- Another skill that will be beneficial for you is to master system administration. It is all about configuring and maintaining computers. You must be curious to know every aspect of your computer features and settings and play around a bit.

2. Knowledge of Operating Systems and Virtual Machines

- A cyber security professional must have a strong knowledge of operating environments such as Windows, Linux, and Mac OS. As a cyber security expert, you should be comfortable working on any OS. VMs allow you

to train and research in an isolated environment and help you maximize your skills.

- The next point to remember is to know Kali Linux as it is the most widely known Linux distribution for ethical hacking and penetration testing. It comes with several hundred tools related to Penetration Testing, Malware Analysis, Security research, Computer Forensics, and so on.

3. Network Security Control

- Network Security Control refers to the different measures which are employed to enhance the security of a network. You need to know how your network works, how routers, firewalls, and other devices work. A firewall is a hardware or software that blocks outgoing or incoming traffic from the internet to your computer. As a cyber security expert, you must leverage a firewall to filter and prevent unauthorized traffic onto the network.
- Additionally, you must know about Intrusion detection systems, Intrusion Prevention Systems, Virtual Private Networks (VPNs), and remote access. For example, you should operate the IDS and recognize any security policy violations and malicious traffic on the network.

4. Coding

- Having zero coding knowledge may limit your cyber security opportunities in the future. Hence, it is advised to acquaint yourself with a few coding languages.
- Given below are the list of a few coding languages you can learn to have a successful career in cyber security:

1. C and C++: C and C++ are low-level programming languages you need to know as a cyber security professional.
2. Python: It is a well-known high-level programming language that is becoming popular among cyber experts today. It will help you identify and fix vulnerabilities.

3. JavaScript: A good advantage of knowing JavaScript is that you can prevent cross-site scripting attacks.

4. PHP: Most websites are created using PHP, learning it will help defend against intruders.

5. HTML: HTML is yet another language cyber security professionals should understand, as most websites use it, and it is one of the easiest languages to learn.

6. Go lang. It is great for cryptography; you can solve various cyber security problems with it.

7. SQL: Attackers use this language to damage the stored data; one example is the SQL injection attack. Hence, having a good understanding of SQL(Structured Query Language) is beneficial.

8. Assembly Language: Assembly will help you understand how malware functions work and thereby help you defend against it.

5. Cloud Security

- Companies are looking for professionals with security skills applicable to public and hybrid cloud platforms such as AWS and Azure. More organizations look to cloud infrastructure to store data and run applications. This includes the implementation of policies and technologies that protect cloud-based systems and devices.
- Like Application Development Security, Cloud Security also involves building secure systems from the start. People with the experience and knowledge in managing big platforms, such as Microsoft Azure, AWS, and the Google Cloud Platform, are in high demand.

6. Blockchain Security

- Blockchain's popularity is increasing, thanks in part to the level of security it offers. Consequently, cyber security professionals should become familiarized with block chain and how it handles security issues. Consider it preparing for the future.

- Blockchain will likely make security inroads into areas like Internet of Things devices (more on this later), network control, supply chain integration, identity control, and mobile computing.
- Blockchain's complex nature makes it difficult for intruders to compromise. For a cybercriminal to corrupt or destroy a blockchain, they would have to eliminate the data found on each user's computer that's connected to the targeted global network.

7. The Internet of Things (IoT)

- According to Statista, there will be over 30 billion Internet of Things devices connected worldwide by 2025. With such a huge number of devices comes many more opportunities for security vulnerability. Therefore, IoT security will become a higher priority in the near future, and an essential part of maintaining the integrity and security of the overall Internet system.
- Many IoT devices are sensors that collect personal data, which raises the stakes in maintaining secure networks and preserving consumer confidence.
- IoT security emphasizes protecting connected devices and networks over the Internet, especially since most of these devices access networks without human intervention or oversight. Therefore, it becomes important to make sure that proper security measures are in place so that IoT devices can be left alone to perform their functions automatically, without cyber security experts having to be concerned about keeping out unauthorized intruders.

8. Artificial Intelligence (AI)

- Like blockchain, Artificial Intelligence is a relatively young innovation that's been enjoying widespread use. AI is perfect for the cybersecurity sector, as it brings reliability and consistency to cybersecurity measures, as it helps security professionals identify suspicious activity and impart a greater understanding of the cyber environment.

- AI brings a level of automation and support that is unmatched by human capabilities, catching threats that may otherwise go unnoticed and unaddressed.
- Artificial Intelligence can also be trained to learn and evolve, making it better equipped to handle new emerging threats and hacking techniques.

Additional Cybersecurity Skills

Now, go through a set of additional skills that can help you get into the cybersecurity field:

1. Risk Analysis: Cybersecurity professionals are required to identify, manage and mitigate risks. Risk management and mitigation are a skill set that will be in high demand in the coming years.
2. Information Security: Companies require skilled professionals who can protect their electronic data from unauthorized access.
3. Security Incident Handling & Response: As a cybersecurity expert, you must be prepared to handle any genuine threat of violating an organization's security policy. With security incident management, you are required to identify, manage, record, and analyze security threats in real-time. As a security practitioner, you must also manage and analyze the security information and event management (SIEM) tools and services.
4. Security Audit: It is an internal check that is carried out to find flaws in the organization's information system. Security audit and compliance knowledge are very crucial because any missed area of regulatory compliance might incur significant fines and penalties for the organization.
5. Laws and Regulations: This is an often-overlooked cybersecurity aspect. There are several cybersecurity laws and regulations that you should be aware of. These laws define how you can use the internet and protect people from becoming victims of cybercrimes.

Apart from these additional cybersecurity skills, make sure you stay updated with new hacks and learn new tools, as cybersecurity is an ever-evolving field. Apart from the technical skills, there is another important set of skills you should have under your belt, and they're known as "soft skills." Having a set of good soft skills will help you bag your dream job. You can watch this video on the top five soft skills that will help you grow in your career and to incorporate those skills:

Vulnerability Assessments Top 8 Most Useful

Vulnerability assessments top 8 most useful analysis the method of recognizing, categorizing and characterizing the safety holes among the network infrastructure, computers & package, etc. Few samples of such vulnerabilities resort of a misconfiguration of parts in network infrastructure. A defect in associate degree software system, any ambiguity during a marketable product, etc.

Given below are the different types of vulnerability assessments:

Active Assessments

Active evaluation are a type of vulnerability assessment that uses network scanners to scan the **network** to identify the hosts, services, and vulnerabilities present in that network. This network scanners have the capability to reduce the intrusiveness of the checks they perform.

Passive Assessments

Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerability assessments. Even passive assessments provide a list of the users who are a recently using the network.

External Assessments

External assessment assesses the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world. These types of assessments use external devices like firewalls, routers, and servers. An external assessment estimates the threat of network security **attacks** external to the organization. it determines how secure the external network and firewall are.

The following are some of the possible steps in performing an external assessments:

1. Determine the set of rules for firewall and router configurations for the external network.
2. Check whether external server devices and network devices are mapped.
3. Identify open ports and related services on the external network.
4. Examine patch levels on the server and external network devices.
5. Review detection systems such as IDS, firewalls, and application-layer protection systems.
6. Get information on **DNS** zones.
7. Scan the external network through a variety of proprietary tools available or the Internet.
8. Examine web applications sickish as e-commerce arc shopping cart software for vulnerability

Internal Assessments

An internal assessment involves scrutinizing the internal network to find exploits and vulnerability assessments.

The following are some of the possible steps in performing an internal assessments:

1. Specify the open ports aria related services on network devices, servers, and systems.
2. Check for router configurations and tire wall rule sets.

3. List the internal vulnerabilities of the operating system and **server**.

4. Scan for Trojans that may be present in the internal environment.

5. Check the patch levels on the organization's internal network devices, servers, and systems.

6. Check for the existence of malware, **spyware**, and virus activity and document them.

7. Evaluate the physical security.

8. Identify and review the remote management process and events.

9. Assess the file-sharing mechanisms if or example, NFS and SMB/CIFS shares) 0 Examine the antivirus implementation and events.

Top vulnerability scanning tools

Host-based Assessments

Host-based assessments are a type of **security** check that involves carrying out a configuration-level check through the command line. These assessments check the security of a particular network or server. Host-based scanners assess systems to identify vulnerabilities such as incorrect registry and file permissions, as well as software configuration errors. Host-based assessment can use many commercial and open-source scanning tools.

Network Assessments

Vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Network assessment professionals use firewall and network scanners such as Nessus. These scanners find open ports, recognize the services running on those parts, and find vulnerabilities associated with these services. These assessments help organizations determine how vulnerable systems are to Internet and Intranet attacks. And how an **attacker** can gain access to important information. A typical network assessment conducts the following tests on a network:

1. Checks the network typologies for inappropriate firewall configuration.

2. Examines the router filtering rules.
3. Identities inappropriately configured database servers.
4. Tests individual services and protocols such as HTTP, SNMP, and FTP.
5. Reviews HTML source code for unnecessary information.
6. Performs bounds checking on variables.

Application Assessments

An application assessment focuses on transaction web applications, traditional client-server applications, and hybrid systems. It analyzes all elements of an application infrastructure, including deployment and communication within the client and server. This type of assessment tests the web server infrastructure for any misconfiguration, outdated content, and known vulnerabilities. Security professionals use both commercial and open-source tools to perform as, assessments.

Wireless Network Assessments

Wireless network assessment determines the vulnerabilities in an organization's wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Wireless network standards have evolved, but many networks still use the weak and outdated security mechanisms and are open for attack. Wireless network assessments try to attack wireless authentication mechanisms and get unauthorized access. This type of assessment tests wireless networks and identifies rogue wireless networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access once they get access to the wireless network.

1. Identify open ports and related services on the external network
2. Examine patch levels on the server and external network devices

3. Review detection systems such as IDS, firewalls, and application-layer protection systems

4. Get information on DNS zones

5. Scan the external network through a variety of proprietary tools available or the Internet

6. Examine web applications sickish as e-commerce arc shopping cart software for vulnerability.

EC-Council Security Analyst v10 | ECSA

Questions related to this topic

1. How do I scan my network for vulnerability?
2. What are the types of vulnerability scans?
3. What are the 4 main types of vulnerability in cyber security?
4. Which of these are examples of security tools that can scan computer systems and networks for vulnerabilities?

What is an Information Security Incident?

Information Security Incident

Information Security Incident may be a network or host activity that potentially threatens. The security's of knowledge keep on network devices and systems with regard to confidentiality, integrity, and accessibility. It'd be any real or suspected adverse event in regard to the safety of laptop systems or networks. It's a violation at hand threat that has the potential to impact laptop security policies, acceptable use policies practices. Discussed below square measure the various varieties of data **security incidents:**

What is a Security Incident?

A security incident is any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information. This includes

interference with information technology operation and violation of campus policy, laws or regulations.

Examples of security incidents include:

- Computer system breach
- Unauthorized access to, or use of, systems, software, or data
- Unauthorized changes to systems, software, or data
- Loss or theft of equipment storing institutional data
- Denial of service attack
- Interference with the intended use of IT resources
- Compromised user accounts

It is important that actual or suspected security incidents are reported as early as possible so that campus can limit the damage and cost of recovery. Include specific details regarding the system breach, vulnerability, or compromise of your computer and we will respond with a plan for further containment and mitigation.

Malicious Code or corporate executive Threat Attacks:

Malicious code attack could be a kind of attack that's generated by malicious programs like viruses, worm, and worms. Insiders can even use the malicious code to realize body privileges, capture passwords, and alter. The audit logs to hide their tracks. Malicious code attacks also are referred to as as program threats. The intention behind this sort of **attacks** is to change info, steal knowledge. And acquire unauthorized access and harm resources of the system or network. Insider threats to your network generally involve those who work as staff or contractors of your company. They belong in your facilities and that they usually have user accounts in your networks.

They understand things concerning your organization that outsiders. Sometimes don't–the name of your network administrator, that specific applications you utilize. What type of network configuration you've got, that vendors you're employed with. External **cyber attackers** sometimes ought to

fingerprint your network, analysis info concerning your organization. Socially engineer sensitive knowledge from your staff, acquire malicious access to any user account. Even those with the smallest {amount} amount of privileges. Thus internal attackers have already got benefits that external attackers lack.

Unauthorized Access:

Unauthorized access refers to the process of obtaining illegal access to the systems or network resources to harm data. Associate aggressor can do this by **victimization network** sniffers to capture network traffic. To spot and procure encrypted usernames, passwords, and so on. Unauthorized access incidents embody secret attacks, session hijacking, and network sniffing. Unauthorized access may additionally occur if a user makes an attempt to access district system they must not be accessing. Once trying to access that space, they might be denied access Associate in nursing probably see an unauthorized access message. Some system directors came upon alerts to allow them to grasp once. There's Associate in nursing unauthorized access try, so they will investigate the explanation. These alerts will facilitate stop **hackers** from gaining access to a secure or confidential system. Several secure systems can also lock associate degree account that has had too several unsuccessful login makes an attempt.

Unauthorized Usage of Services:

In this kind of incidents, Associate in nursing assailant uses another user's account to attack the system or network. It's the violation of associate degree **organization's system policies** by misusing .The resources provided to the users or workers. This might embody victimization associate degree workplace laptop to transfer movies or to store pirated computer code. Removing the contents announce by another- user, harassing alternative users, gaining credentials or personal data of different use-s, a-id so on. Inappropriate usage **incidents** embrace privilege increase, insider attacks, and sharing of critical data.

If you report loss of a debit card inside two business days after you notice the card missing, your liability is proscribed to $50. If you don't, your potential liability will increase to $500. You risk unlimited liability (up {to all to all or Associate in Nursing to any or all} the money in your account and your draft protection). If you fail to report an unauthorized card dealings. That seems on your statement among sixty days of that statement being mail-clad to you. If your credit or debit card is lost or stolen, contact the card establishment immediately—you will notice the quantity on your monthly statement. Check your account statements once you receive them—or additional typically online—to catch any transactions you didn't create and report them directly.

Email-based Abuse:

during this kind of incidents, Associate in nursing attacker creates a pretend web site mimicking the legitimate web site and sends the ….website links to the users to steal sensitive data like user credentials, checking account details, and credit card details. This sort of incidents includes unsought business email known as Spam, and phishing mails. **Espionage:** undercover work involves stealing the proprietary data of any organization and spending a similar to different organizations with the motive of negatively impacting its name or for a few monetary profit.

Information Security Incidents

Fraud and Theft:

this sort of incidents involves thieving or loss of quality or instrumentality that Contains hint. The motive behind fraud and thieving is to achieve management over and misuse the data systems like access management systems, **inventory systems**, monetary information, and phone phone equipment. Employee Sabotage Associate in Nursing Abuse: The actions performed l:PV an worker to abuse systems embody removing hardware or services of a computing system, deliberately creating incorrect information

entry, deliberately deleting information or altering data, inserting logic bombs to delete data, applications., and system files, crashing systems, and so on.

Network and Resource Abuses:

during this variety of incidents. Associate in nursing aggressor uses the network and resources for getting crucial organization details, or in some situations they even create the network services or resources out of stock to the legitimate users by flooding a lot of traffic to the servers or applications. Network and resource abuse incidents embody **denial-of-service (DoS) attacks,** network scanning, and so on. Resource misconfiguration Abuses: during this kind of incidents, Associate in Nursing attacker exploits resource misconfiguration like vulnerable code configurations, open proxy servers and anonymous file transfer protocol servers, misconfigured internet forms and journal. Sites, and so on. Resource misconfiguration abuses embody SQL injection attacks, bypassing authentication, malicious code execution, and so on.

EC-Council Certified Incident Handler | ECIH v2

What should I do if I suspect a serious Security Incident?

A security incident is considered serious if the campus is impacted by one or more of the following:

- potential unauthorized disclosure of sensitive information
- serious legal consequences
- severe disruption to critical services
- active threats
- is widespread
- is likely to raise public interest

Sensitive information is defined in the UCB Data Classification Standard and includes personally identifiable information that is protected by laws and regulations, as well as confidential research protected by data use agreements, such as:

- Social security number
- Credit card number
- Driver'slicensenumber
- Student records
- Protected health information (PHI)
- Human subject research

If All businesses should have some processes or technologies in place to help prevent **security incidents** and breaches. These systems should include methods of detecting unusual activity and blocking threats and attacks. Some primary technologies might include firewalls, network security **monitoring tools**, web vulnerability scanning tools and encryption tools. **Infosavvy** gives Training on **Incident Handling(ECIH v2)** Processes with Certification in **Mumbai Location** and **Accreditation by EC-Council.**

Questions related to this topic

1. What are the 3 types of access control?
2. What authorizes a user to access resources on a network?
3. What are the six main categories of access control?
4. Is it safe to allow apps to access your contacts?
5. What is an Information Security Incident?

What is Information Security & types of Security policies

Information Security

What is **Information Security** & types of Security policies form the foundation of a security infrastructure. Data security policy defines the fundamental security needs and rules to be implemented so as to protect and secure organization's data systems. While not them, it's attainable} to protect the corporate from possible lawsuits, lost revenue, and bad publicity, to not mention the fundamental **security attacks**.

A **security policy** could be a high-level document or set of documents that describes, in detail, the safety controls to implement in order to protect the corporate. It maintains confidentiality, availability, integrity, and asset values. A security policy also protects the corporate from threats like unauthorized access, theft, fraud, vandalism, fire, natural disasters, technical failures, and accidental damage. Additionally, it protects against **cyber-attack**, malicious threats, international criminal activity foreign intelligence activities, and terrorism.

Policies are not technology specific and accomplish 3 things;

• They reduce or eliminate legal liability of employees and third parties.

• They protect confidential and proprietary data from theft, misuse, unauthorized disclosure, or modification.

• They forestall stage of the company's computing resources.

What is Information Security & **types of Security policies** All security policies should documented properly and that they should focus on the security of all departments in a company. Management should take into consideration the areas in which security is most significant, and prioritize its actions accordingly, however it's important to appear into every department for doable security breaches and ways that to safeguard against them.

The following data security systems in a company would possibly need a lot of attention in terms of security:

• Encryption mechanisms – Antivirus systems

• Access control devices – web sites

• Authentication systems – Gateways

• Firewalls – Routers and switches

There are **2 types of security policies:** technical security and administrative security policies. Technical **security** policies describe the configuration of the technology for convenient use; body security policies address however all persons should behave. All workers should conform to and sign each the policies.

In a company the high-level management is responsible for the implementation of the organization's security policies. High-level officers concerned within the implementation of the policies embody the following:

1. Director of data Security
2. Chief Security Officer

The following are the goals of security policies:

- To maintain an outline for the management and administration of **network security**
- To protect an organization's computing resources
- To eliminate legal liabilities arising from workers or third parties
- To prevent wastage of company's computing resources
- To prevent unauthorized modifications of the data
- To scale back risks caused by illegal use of the system resource
- To differentiate the user's access rights
- To protect confidential, proprietary data from theft, misuse, and unauthorized disclosure

Information Security of Threat

Types of Security Policies

A security policy is a document that contains data about the way the company plans to protect its data assets from known and unknown threats. These policies help to keep up the confidentially, availability, and integrity of data. The four major forms of security policy are as following:

Promiscuous Policy:

This policy doesn't impose any restrictions on the usage of system resources. for example, with a promiscuous net policy, there's no restriction on net access. A user will access any web site, transfer any application, and access a laptop or a network from a foreign location. whereas this may be helpful in company businesses wherever people that travel or work branch offices need to access the **structure networks**, several malware, virus, and Trojan threats are

present on the internet and because of free net access, this malware will return as attachments while not the data of the user. Network directors should be very alert whereas selecting this kind of policy.

Permissive Policy:

Policy begins wide-open and only the known dangerous services/attacks or behaviors are blocked. for instance, in a very permissive net policy, the bulk of net traffic is accepted, however many proverbial dangerous services and **attacks** square measure blocked. as a result of solely proverbial attacks and exploits are blocked, it's not possible for directors to stay up with current exploits. directors are perpetually enjoying catch-up with new attacks and exploits. This policy ought to be updated often to be effective.

Prudent Policy:

A prudent policy starts with all the services blocked. The administrator permits safe and necessary services singly. It logs everything, like system and network activities. It provides most security whereas permitting only proverbial however necessary dangers.

Paranoid Policy:

A paranoid policy forbids everything. There's a strict restriction on all use of company computers, whether or not it's system usage or network usage. There's either no net association or severely restricted net usage. Because of these to a fault severe restrictions, users typically try and notice ways that around them.

Examples of Security Policies:

Given below square measure samples of security policies that organizations use worldwide to secure their assets and vital resources.

Access management Policy:

Access management policy outlines procedures that facilitate in protective the structure resources and also the rules that management access to them. It permits organizations to trace their sets.

Remote-Access Policy:

A remote-access policy contains a collection of rules that define authorized connections. It defines who will have remote access, the access medium and remote access security controls. This policy is critical in larger organizations during which networks are geographically unfold, and people during which employees work from home.

Firewall-Management Policy:

A firewall-management policy defines a standard to handle application traffic, like net or e-mail. This policy describes the way to manage, monitor, protect, and update firewalls within the organization. It identifies network applications, **vulnerabilities** related to applications, and creates an application-traffic matrix showing protection strategies.

Network-Connection Policy:

A network-connection policy defines the set of rules for secure network connectivity, including standards for configuring and extending any part of the network, policies related to private networks, and detailed information about the devices attached to the network. It protects against unauthorized and unprotected connections that allow hackers to enter into the **organization's network** and affect data integrity and system integrity. It permits only authorized persons and devices to connect to the network and defines who can install new resources on the network, as well as approve the installation of new devices, and document network changes, etc.

Questions related to this topic

1. What types of things would you suggest to a manager be included in a network access policy?
2. What are the three types of security policies?
3. What do organizational BYOD bring your own device policies typically include?
4. What are security policies and procedures?

5. What is Information Security & types of Security policies?

What is “Anonymizer” & Types of Anonymizers

/ CEH / By TusharPanhalkar

Anonymizer

What is “Anonymizer” & Types of Anonymizers An associate degreeonymizer is an intermediate server placed between you because the user and also the website to accesses the web site on your behalf and build your web water sport untraceable. Anonymizers enable you to bypass net censors. associate degree anonymizer eliminates all the distinctive info (**IP address**) from your system whereas you’re surf riding the net, thereby making certain privacy. Most anonymizers will anonymize the net (HTTP:), fireplace transfer protocol (FTP :), and gopher (gopher net services. What is “Anonymizer” & Types of Anonymizers.

To visit a page anonymously, you’ll be able to visit your most well-liked anonymizer web site, and enter the name of the target website within the Anonymization field. Alternately, you’ll set your browser home page to purpose to an anonymizer, so as to anonymize sequent net access. with the exception of this, you’ll be able to like better to anonymously give passwords and different info to sites without revealing any extra information, like your IP address. Nuts might set up associate degree anonymizer as a permanent proxy server by creating the positioning name the setting for the HTTP, FTP, Gopher, and different proxy choices in their applications configuration menu, thereby cloaking their malicious activities. What is “Anonymizer” & Types of Anonymizers.

Why Use an Anonymizer?

The reasons for victimization anonyrnizers include:

• **Ensuring privacy:** defend your identity by creating your net navigation activities untraceable. Your privacy is maintained till and unless you disclose your personal data on the net, for instance, by filling out forms.

• **Accessing government-restricted content:** Most governments stop their citizenship accessing bound websites or content deemed inappropriate or containing sensitive data. However, these sites will still be accessed victimization an anonymizer settled outside the target country.

• **Protection against on-line attacks:** associate degree anonymizer will defend you from all instances of online phrasing attacks by routing all client web traffic via its protected DNS server.

• **Bypassing IDS and firewall rules:** Firewalls are usually bypassed by workers or students accessing websites that they're not alleged to access. associate degree anonymizer service gets around your organization's firewall by fixing a association between your pc and also the anonymizer service. By thus doing, firewalls see solely the affiliation from your pc to the anonymizer's net address. The anonymizer can then hook up with any web site (e.g., Twitter) with the assistance of a web affiliation, and so direct the content back to you. To your organization, your system seems to be merely connected to the anonymizer's net address, however to not the particular web site to that you have got browsed.

The 10 Secrets You Will Never Know About Cyber Security & Its Important?

In addition to protective users' identities, anonymizers also can be wont to attack a web site while not being derived.

Types of Anonymizers

An anonymizer could be a service through that one will hide their identity once victimization sure web services. It encrypts the information from your pc to the net service supplier. Anonymizers are of two basic types; Networked anonymizers and Single-point anonymizers.

Networked Anonymizers

A networked anonymizer 1st transfers your data through a network of Internet-connected computers before passing it on to the web site. as a result of the data passes through many web computers, it becomes a lot of cumbersome for anyone making an attempt to trace your data to determine the association between you and also the anonymizer.

Example: if you wish to go to any website, you have got to form an invitation.

Advantage: Complication of the communications makes traffic analysis advanced.

Disadvantage: Any multi-node network communication incurs a point of risk of compromising confidentiality at each node.

Single-Point Anonymizers

Single-point anonymizers 1st transfer your data through a web site before causation it to the target website, so pass back data gathered from the targeted web site, to you via the web site to shield your identity.

Advantage: Arms-length communication protects **information** address and connected distinctive info.

Disadvantage: Effects less resistance to stylish traffic analysis.

Anonyntizers

An anonymizer assists you to mask your scientific discipline address to visit websites while not being tracked or known whereas keeping your activity and identity protected. It uses varied techniques like SSH, VPN, and HTTP proxy that permit you to access blocked or censored content on the net with omitted advertisements.

Certified Ethical Hacker | CEH Certification

Whonix

Whonix may be a desktop OS designed for advanced security and privacy. It mitigates the threat of common attack vectors whereas maintaining usability. on-line obscurity is completed via fail-safe, automatic, and desktop-wide use of

the Tor network.

Features:

– A heavily reconfigured Debian base is run within multiple virtual machines, providing a considerable layer of protection from malware and science address leaks.

– Usually used applications are pre-installed and safely pre-configured for immediate use.

– It's below active development, and it's the sole OS designed to be run within a Vivi and paired with Tor.

Some of the anonymizers are as follows:

- Tunnelbear
- InvisiblenetProject (I2P)
- Proxify
- Psiphon
- AnonymizerUniversal
- Anonymousnetsurfriding
- Guardster
- Ultrasurf
- netProxyServer

AnonymizerforMobile

Orbot

Orbot may be a proxy app that enables alternative apps to use the web additional firmly. It uses Tor to inscribe net traffic, and so hides it by bouncing through a series of computers round the world. Tor may be a free package that gives associate open network to assist defend your system against any type of network police work that threatens personal freedom and privacy, confidential business activities and relationships, and a form of state security observance called **"traffic analysis."** Orbot creates a really non-public web affiliation.

Psiphon

Psiphon may be a evasion tool from Psiphon INC. that utilizes VPN, SSH, and HTTP Proxy technology to supply you with open and uncensored access to web content. However, Psiphon doesn't increase online privacy and isn't a web **security** tool.

Features:

1. Browser or VPN (whole-device) mode: one will select whether or not to tunnel everything or simply the net browser.
2. In-app stats: This helps you to acumen abundant traffic you have got been victimization.

Questions related to this topic

1. What is Web Proxy address?
2. Should I use a proxy server?
3. What is proxy server how it works?
4. How do I get a proxy server?
5. What is "Anonymizer" & Types of Anonymizers?

Overview of Digital evidence

Leave a Comment / CTIA / By TusharPanhalkar

Digital evidence

Overview of Digital evidence, face many challenges during the investigation of a digital crime, like extracting, preserving, and analyzing the digital proof. Digital evidences play an essential role while investigation cyber-crimes. Digital proof helps incident res-ponders in tracing out the wrongdoer. This section provides a summary of digital proof, styles of digital proof, **characteristics** of digital proof, roles of digital proof, and kinds of proof.

Digital proof

Digital proof is outlined as "any info of significant worth that's either hold on or transmitted during a digital form" and helps incident responders/investigators notice the wrongdoer. Digital devices are of times employed in cyber-attacks and different security breaches that store information regarding the session, like login user, time, form of affiliation, and **IP addresses**. Therefore, these devices like servers and routers act as a supply for digital evidence that may be employed by incident responders to prosecute the attacker.

Certified Threat Intelligence Analyst | CTIA

Digital proof is gift across computing devices, servers, routers, and so on. it's revealed throughout forensics investigation whereas examining digital storage media, watching the network traffic, or creating duplicate copies of **digital** knowledge.

Incident responders/investigators ought to take utmost care whereas gathering and extracting the digital proof because it is specific and fragile in nature. This makes it tough for an occurrence res-ponder/investigator to trace the criminal activities. **Incident** responders/investigators ought to be trained and trained to extract, handle, and analyze such fragile proof.

Listed below are the various sources of digital evidence:

• Desktop computers, laptops, network storage devices, and servers.
• DVDs, ports like USB, Firewire, and PCMCIA.
• Thumb drives, flash disks, memory disks, magnetic disks, optical disks.
• Portable devices like PDAs, digital cameras, audio/video players, and cell phones.
• Various styles of laptop and network logs Types of Digital Evidence.

Based on the fragility and period of time, it has of 2 types:

•Volatile Evidence

Volatile proof refers to the temporary info on a digital device that needs a relentless power offer and is deleted if the ability offer is interrupted. as an

example, the RAM stores most volatile information and discards it once the device is converted.

Important volatile information includes system time, logged-on user(s), open files, network info, method info, process-to-port mapping, method memory, writing board contents, service/driver info, and command history.

- **Nonvolatile Evidence**

Nonvolatile proof refers to the **permanent information** hold on on auxiliary storage devices, like onerous disks and memory cards. Nonvolatile information doesn't rely on power offer and remains intact even once the device is converted.

Information holds on in nonvolatile type includes hidden files, slack area, swap file, index files, unallocated clusters, unused partitions, hidden partitions, written record settings, and event logs.

Types of Threat Intelligence

Characteristics of Digital proof

The digital proof should have some characteristics to be disclosed within the court of law. the most characteristic of the digital proof is its connection and weight (influence). The term "relevance" refers to the affiliation between digital proof and also the fact that is to be established. The digital proof is accepted in a very court of law once it's relevant. If the collected digital proof doesn't amendment chance of the very fact, the proof is orthogonal. The term "**weight of the digital proof**" refers to what proportion the digital evidence changes the chance of the very fact.

- **Admissible:** Incident res-ponders have to be compelled to gift proof in an admissible manner, which suggests that it ought to be relevant to the case, act in support of the consumer presenting it, and be communicated and non-prejudiced.
- **Authentic:** it's terribly simple to govern digital proof, that raises queries of its possession. Therefore, incident responders should give supporting documents

relating to the believably of the proof with details like supply and its connection to the case. If necessary, they need to additionally furnish details like author of the proof or path of transmission.

• **Complete:** The proof should be complete, which suggests it should either prove or contradict the accordant truth in the litigation. If the proof fails to try to, therefore, the court is prone to dismiss the case citing lack of sturdy proof.

• **Reliable:** The forensic experts ought to extract and handle the proof whereas maintaining a record of the tasks performed throughout the method to prove that the proof is dependable. forensic investigations should be conducted solely on the copies of the proof as a result of the court must have the first proof for future reference.

• **Believable:** Incident res-ponders and prosecutors should gift the proof in a very clear and accessible manner to the members of jury. they need to justify the facts clearly and acquire an expert opinion on the same to confirm the **investigation** method.

Roles of Digital proof

When an intruder bypasses the victim's PC or network, he or she leaves evidence, which might function clues to unravel the attack. samples of cases wherever digital proof could assist the forensic incident respondent in prosecution or defense of a suspect:

• Use/abuse of the net

• Abuse of systems

• Email communication between suspects/conspirators

• Identity theft

• Information run

• Theft of commercial secrets

• Unauthorized transmission of data

• Malicious attacks on the PC systems themselves

• Production of false documents and accounts

• Unauthorized encryption/password protection of documents

Digital pieces of evidence play an essential role while investigation cyber-crimes. Digital proof helps incident res-ponders in tracing out the wrongdoer. In **Infosavvy** you will learn how to find proof in digital evidence in **CTIA course** in **Mumbai Location.**

Questions related to this topic

1. How digital forensics were used in the investigation?
2. What are the different types of digital analysis that can be performed on the captured forensic evidence?
3. How do you handle digital evidence?
4. What are some of the problems traditionally associated with finding digital evidence? Overview of Digital evidence | Info-savvy.com https://info-savvy.com/overview-of-digital-evidence/

REFRENCES

1. Английский язык в сфере информационных технологий - BOOK.ruhttps://book.ru/book/936082 (дата обращения: 21.03.2022)
2. Английский язык для профессионального общения. Вычислительная техника = English for Professional Communication. Computer Engineering https://www.studentlibrary.ru/ru/book/978-985-503-834-5_1.html (дата обращения: 21.03.2022)
3. Английский язык, основы компьютерной грамотности, Радовель В.А., 2006 https://obuchalka.org/20210504131976/angliiskii-yazik-osnovi-komputernoi-gramotnosti-radovel-v-a-2006.html (дата обращения: 21.03.2022)
4. Английский язык для IT-специалистов https://proglib.io/p/eng-for-it (дата обращения: 17.12.2022)
5. Компьютерные технологии и кибертерроризм = Computer Technologies and Cyberterrorism: учеб. пособие по англ. языку / сост.: С. В. Борисова, В. А. Гончарова. - Краснодар: Краснодарский университет МВД России, 2021. - 322 с. - ISBN 978-5-9266-1749-5: 170.69 р. - Текст: непосредственный.
6. Практический курс английского языка по специальности «Безопасность информационных технологий в правоохранительной сфере»: учеб. пособие по англ. яз. / сост. С.В. Борисова, В.А. Гончарова. – Краснодар: Краснодарский университет МВД России, 2017. – 194 с.- ISBN 978-5-9266-1266-7. - Текст: непосредственный.
7. СмирноваТ.В. English for Computer Science Students. Учебное пособие / Т.В. Смирнова, М.В. Юдельсон. - Москва : Флинта, 2012. - 128 с. - ISBN 978-5-89349-203-3. - URL: https://ibooks.ru/bookshelf/27293/reading (дата обращения: 21.03.2022). - Текст: электронный.

8. Учебное пособие по английскому языку для студентов специальности Программирование в компьютерных системах https://www.prodlenka.org/metodicheskie-razrabotki/64982-uchebnoe-posobie-po-anglijskomu-jazyku-dlja-s(дата обращения: 21.03.2022)
9. Учебные пособия для изучения профессионально направленной терминологии для студентов Алатырского технологического колледжа. | Образовательная социальная сеть https://nsportal.ru/user/557746/page/pravoslavnaya-stranichka (дата обращения: 21.03.2022)
10. A BRIEF HISTORY of the INTERNET — Мегаобучалка https://megaobuchalka.ru/5/28665.htm l (дата обращения: 21.03.2022)
11. Computers, Future of | Encyclopedia.com https://www.encyclopedia.com/education/news-wires-white-papers-and-books/computers-future (дата обращения: 21.03.2022)
12. English for Computer Science Student [Электронный ресурс]: учеб. пособие / сост. Т.В. Смирнова, М.В. Юдельсон; науч.ред. Н.А. Дударева. – 9 изд., стер. – М.: ФЛИНТА, 2017. - 126 с.
13. English for law enforcement: навч.-метод. посібник / А. О. Кузьменко. - Дніпропетровськ: Середняк Т. К., 2015. — 183 с. https://core.ac.uk/download/pdf/149277663.pdf (дата обращения: 21.03.2022)
14. Your 2022 Tech Terms Dictionary - Future Females https://futurefemales.co/your-2022-tech-terms-dictionary/ (дата обращения: 21.03.2022)

References for a YouTube Video

1. [1-2] The internet and its components – YouTube https://www.youtube.com/watch?v=nmN-j0pmYsI (дата обращения: 17.12.2022)

2. Classification of Computers – YouTube https://www.youtube.com/watch?v=RQ98_ksHwgY (дата обращения: 17.12.2022)

3. COMPUTER HARDWARE AND SOFTWARE || COMPUTER FUNDAMENTALS FOR CHILDREN – YouTube https://www.youtube.com/watch?v=zlT-Lg_QFTA (дата обращения: 17.12.2022)

4. COMPUTER HARDWARE QUIZ WITH PICTURES || 50 COMPUTER QUIZ ON COMPUTER PARTS FOR CHILDREN || PART 16 – YouTube https://www.youtube.com/watch?v=wfEO3_arXIY (дата обращения: 17.12.2022)

5. Internet and World Wide Web | Introduction to Internet and WWW | Internet Basics – YouTube https://www.youtube.com/watch?v=tq9Yp8kAaTk (дата обращения: 17.12.2022)

6. Introduction to Internet Technologies – YouTube https://www.youtube.com/watch?v=twKznhEIeIY (дата обращения: 17.12.2022)

7. Types of Programming Languages – YouTube https://www.youtube.com/watch?v=aYjGXzktatA (дата обращения: 17.12.2022)

8. TYPES OF SOFTWARE __ APPLICATION SOFTWARE __ SYSTEM SOFTWARE __ UTILITY SOFTWARE __ COMPUTER BASICS – YouTube https://www.youtube.com/watch?v=BTB86HeZVwk (дата обращения: 17.12.2022)

9. What is the Internet? – YouTube https://www.youtube.com/watch?v=Dxcc6ycZ73M (дата обращения: 17.12.2022)

Appendix

Appendix 1

DIRECT SPEECH / REPORTED SPEECH

Direct speech is the exact words someone said. We use quotation marks in Direct the speech.

Reported speech is the exact meaning of what someone said but not the exact words We do not use quotation marks in Reported speech.

Say - Tell

We can use say and tell both in Direct and Reported speech. Tell is always followed by a personal object (told me). Say is used with or without a personal object. When it is used with a personal object say is always followed by to (said to me)

Expressions with say: say good mourning/evening etc, say something, say one's prayers, say a few words, say so etc.

Expressions with tell: tell the truth, tell a lie, tell sb the time, tell sb one's name, tell a story, tell a secret, tell sb the way, tell one from another etc.

Reported Statements

1. To report statements we use a reporting verb (say, tell, explain etc) followed by a that- clause. In spoken English that can be omitted: *He said, "I feel sick." He said that he felt sick.*

2. Pronouns and possessive adjectives change according to the context.

Direct speech: He said, "I'll lend you my car."

Reported speech: He said he would lend me his car.

3. Time words and tenses can change as follows depending on the time reference:

Direct speech	Reported speech
Tonight, today, this	That night, that day, that week /
Now	Then, at that time, at once,
Now that	Since
Yesterday, last	The day before, the previous night/
Tomorrow, next	The following day/ the day after, the
Two days / months / years ago	Two days / month / years before
“Bob escaped yesterday,” he	He said Bob had escaped the day

4. When the reporting verb is in the past, the verb tenses change as follows:

Direct speech	Reported speech
Present Simple	Past Simple/Present Simple
Present Continuous	Past Continuous
Present Perfect	Past Perfect
Past Simple	Past Perfect
Future	Conditional
Present Perfect Continuous	Past Perfect Continuous

5.If the direct verb is already in the Past S., in Reported Speech it can change into the Past Perfect or remain the same.

6.If the direct verb is in the Past Perfect, it remains the same in Reported Speech.

7.Certain words change as follows depending on the context.

Direct Speech: this/ these here come

Reported Speech: that/ those there go

8.There are no changes in the verb tenses in Reported speech when the direct sentence expresses a general truth, a wish or Conditional type 2/3:

“The Earth is a planet,” he said,. He said that the Earth is a planet.

9.When the introductory verb is in the Present, Future or Present Perfect, there are no changes in the verb tenses:

“She can swim", he says.He says that she can swim.

10.The verb tenses can change or remain the same in Reported speech when a sentence expresses something which is up to date or still true. However, the verb tenses usually change when something is not true or out of date:

"I like coffee," he said. He said he likes/liked coffee (still true)

"I am rich," he said. He said he was rich. (we know he isn't; not true)

Reported Questions

In **Reported questions** we use affirmative word order and the question mark is omitted. To report a question we use: a) ask + wh-word (who, what etc) when the direct question begins with such a word; b) ask + if/whether when the direct question begins with an auxiliary verb (do, has, can etc). Pronouns, possessive adjectives, tenses, time expressions etc change as in statements.

Direct speech: He said, "Why is he sentenced?" He said, "Is he guilty?"

Reported speech: He asked why he was sentenced. He asked if he was guilty.

Indirect questions are different from Reported questions. We use Indirect questions when we ask for information, whereas we use Reported questions to report someone else's questions. Indirect questions are introduced with Could you tell me...?, Do you know...?, I wonder..., I want to know...etc and their verb is in the affirmative. There are no changes in the verb tenses as in Reported questions. If the Indirect question starts with I wonder.orI want to know, then the question mark is omitted.

Direct questions	Reported questions	Indirect questions
He asked me, "How old is she?"	He asked me how old she was.	Do you know how old she is?
He asked me, "Where does she come from?"	He asked me where she came from.	I wonder where she comes from.

Reported Commands / Requests/ Suggestions

To report commands, requests, suggestions etc we use a reporting verb (advise, ask, suggest, beg, offer, order, tell etc) followed by a to-infinitive, a not to-infinitive or an -ing form according to the construction of the introductory verb: *He told me not to lie him. He suggested going out.*

Introductory verbs:

Agree, offer, promise, refuse, threaten, advise, ask, beg, command, invite, order, remind, warn, admit, accuse of, apologise for, boast of/about, complain to sb of, deny, insist on, suggest, explain, exclaim, remark.

Modals in Reported Speech

There are changes in the verb tenses of some modal verbs in Reported speech:

Will/shall - would; can - could (present)/would be able to (future); may - might; shall - should (asking for advice)/would (asking for information); must - must/had to (obligation)

Appendix 2

TOO / ENOUGH

Too + adjective/ adverb (negative	He is too boring to listen to him.
Adjective/ adverb + enough	He is rich enough to buy this car.
Enough + noun	He's committed enough crimes to

SO / SUCH

• Such a(n) + (adjective) + singular countable: *It was such an awful day that we had to stay at the hotel.*

• Such is also used with a lot of: *There is such a lot of noise that I can't sleep.*

• Such + (adjective) + uncountable/ plural noun: *It is such a nice weather that I want to do for a walk.*

• So + adjective/ adverb: *I am so hungry that I could eat a horse.*

• So is also used with much/ many, few/ little: *She has got so many dresses that there is no place to keep them all.*

• So + adjective + a(n) + noun: *It was so nice a day!*

• So and such can be used without that.

LIKE / AS

Like is used	As is used
To say what sb or sth looks like	To say what sb or sth is really or to talk about
After verbs (feel, look, smell, sound) + noun	In certain expressions: as usual, as...as, as much, such as, the same as
With nouns / pronouns / -ing	After the verbs: accept, be known, class,

NEITHER…NOR / EITHER…OR

Neither...nor	Either...or
Take both a singular and plural verbs depending on the subject with follows nor, or.	
Neither Fiona nor Ann was calling the police.	*Either John or his friends are calling the police.*

NEITHER / EITHER / SO / TOO

Nick didn't go for a walk yesterday.	**Neither** did I. Neither + auxiliary +	I didn't **either**. Personal pronoun or
They are investigators.	**So** am I. So + auxiliary verb +	I am **too**. Personal pronoun or

Appendix 3

WISH

I wish + PastSimple	Regret about a present situation which we want to be different	I wish I were more patient.
I wish + subject + could + bare infinitive	Wish in the present concerning lack of ability	I wish I could swim
I wish + subject + would + bare infinitive	Wish for a future change unlikely to happen or wish to express dissatisfaction; polite request implying dissatisfaction or lack of hope: • "wish" and "would" shouldhavedifferentsubjects Wish + inanimate subject + would - is used to express speaker's lack of hope or disappointment	I wish he would investigate this case. I wish you would enter the university. I wish it would stop raining.
I wish + PastPerfect	Regret that something happened or didn't happen in the past	I wish I had bought those boots.

Appendix 4

CONDITIONALS

	If-clause	Main clause	use	Example
Type 0 Real	If + any present form	Present Simple	Real - for general truth	If you heat the water, it boils.
Type 1 Real present	If + any present form	Future / Imperative can/ may / might / must/ should + bare inf.	Real - likely to happen in the present or future	If you work hard, you'll be tired.
Type 2 Unreal	If + Past Simple / Past Continuous	Would/ could/ might + bare inf.	Unreal-unlikely to happen in the present or future;	If I were you, I wouldn't judge him.
Type 3 Unreal past	If + Past Perfect/ Past Perfect Continuous	Would/ could/ might + have + past participle	Unreal situation in the past; also used to express regrets and criticism	If you had locked the car, it wouldn't have been stolen.

We do not normally use *will, would* or *should* in an if-clause.

After *if*, we can use *were* instead of was in all persons.

Mixed Conditionals

All types of conditionals can be mixed. Any tense combination is possible if the context permits it.

	If-clause	Main clause	
Type 2	If nobody phoned the militia,	officers will not come to help	Type 1
Type 2	If he knew her,	he would have invited her to	Type 3

Type 3	If you hadn't learnt the poem,	you will not get an A-level.	Type 1
Type 3	If he had found a job,	he wouldn't be searching for	Type 2

Unless means if not: *Unless they are late, we will not miss the train.*

As long as, providing/ provided that can be used instead of if: *As long as he is on time,*

we will not be late for the party

Appendix 5

MODAL VERBS

Modal verbs express the speaker's attitude to the action indicated by the main verb. They express ability, necessity, obligation, duty, request, permission, advice, desire, probability, possibility, etc.

Modal verbs are: can, could, may, might, must, ought to, will, would, shall, should, have to, need. They take no –s in the third singular except for have to and need. They come before the subject in questions and take "not" after them in negations. Except for ought to and have to, modal verbs are followed by an without to: *Sorry, I can't do it.*

Auxiliary	*Uses*	*Present/ Future*	*Past*
May	Polite request	May I borrow your pen?	
	Formal permission	You may leave the room.	
	50% or less certainty	He may be sleeping now.	He might have been at the office.
Might	50% or less certainty	He might be at the library.	He might have been at the library.
	Polite request (rare)	Might I take your car?	
Should	Advisability	I should study tonight.	I should have studied last night.
	90% certainty (expectation)	She should do well on the test tomorrow.	She should have done well on the test.
Ought to	Advisability	You ought to consult the doctor.	You ought to have consulted the doctor.
	90% certainty (expectation)	He ought to pass his driving test tomorrow.	He ought to have passed his driving test.

Had better	Advisability with threat of bad result	You had better be on time, or you miss the beginning of the film.	
Be supposed to	Expectation	The meeting is supposed to begin at 5 p.m.	
	Unfulfilled expectation		The meeting was supposed to begin at 5 p.m.
Must	Strong necessity	I must arrest the offender.	I had to arrest the offender yesterday.
	Prohibition (negative)	You must not smoke here.	
	95% certainty	Mary isn't at work. She must be sick.	She must have been sick.
Have to	Necessity	I have to wear uniform.	I had to wear uniform.
	Lack of necessity (negative)	I don't have to go to class today.	I didn't have to go to class yesterday.
Have got to	Necessity	I have got to go to class.	I had to go to class.
Will	100% certainty	He will be at work at 7.00	
	Willingness	-The phone is ringing. I'll	
	Polite request	Will you please help me?	
Be going to	100% certainty (prediction)	He is going to be at work at 7.00	
	Definite plan (intention)	I'm going to interrogate a witness.	
	Unfulfilled		I was going to move the
	intention		house.

	Ability/ possibility	I can run fast.	I could run fast when I was younger.
	Informal permission	You can use my car tomorrow.	
	Informal polite request	Can I borrow you laptop?	
	Impossibility (negative)	That can't be true!	That can't have been true!
	Past ability		I could run fast when I was a child.
	Polite request	Could I take your book?	
	Suggestion (affirmative)	You could talk to a lawyer.	You could have talked to a lawyer.
	50% or less certainty	He could be at the militia station.	He could have been at the militia station.
	Impossibility (negative)	He couldn't know her!	He couldn't have known her!
	ability	I am able to help you. I'll be able to help you.	I was able to help you.
	Polite request	Would you please help me?	
	Preference	I would rather go to the park than stay home.	I would rather have gone to the park.
	Repeated action in the past		When I was a child I would visit my

	Polite for “want” with “like”	Would you like a cup of tea?	
	Unfulfilled wish		I would have liked a cookie, but there is none left.
	Repeated action in the past		I used to visit my grandparents, when I was a child.
	Past situation that no longer exists		I used to be fat, but now I keep fit.
	Polite question to make a suggestion	Shall I open the door?	
	Future with “I” or “we” as a subject	I shall arrive at nine.	

Appendix 6

Passive Voice

В английском языке, как и в русском, глаголы могут иметь два залога: действительный (ActiveVoice) и страдательный (Passivevoice).

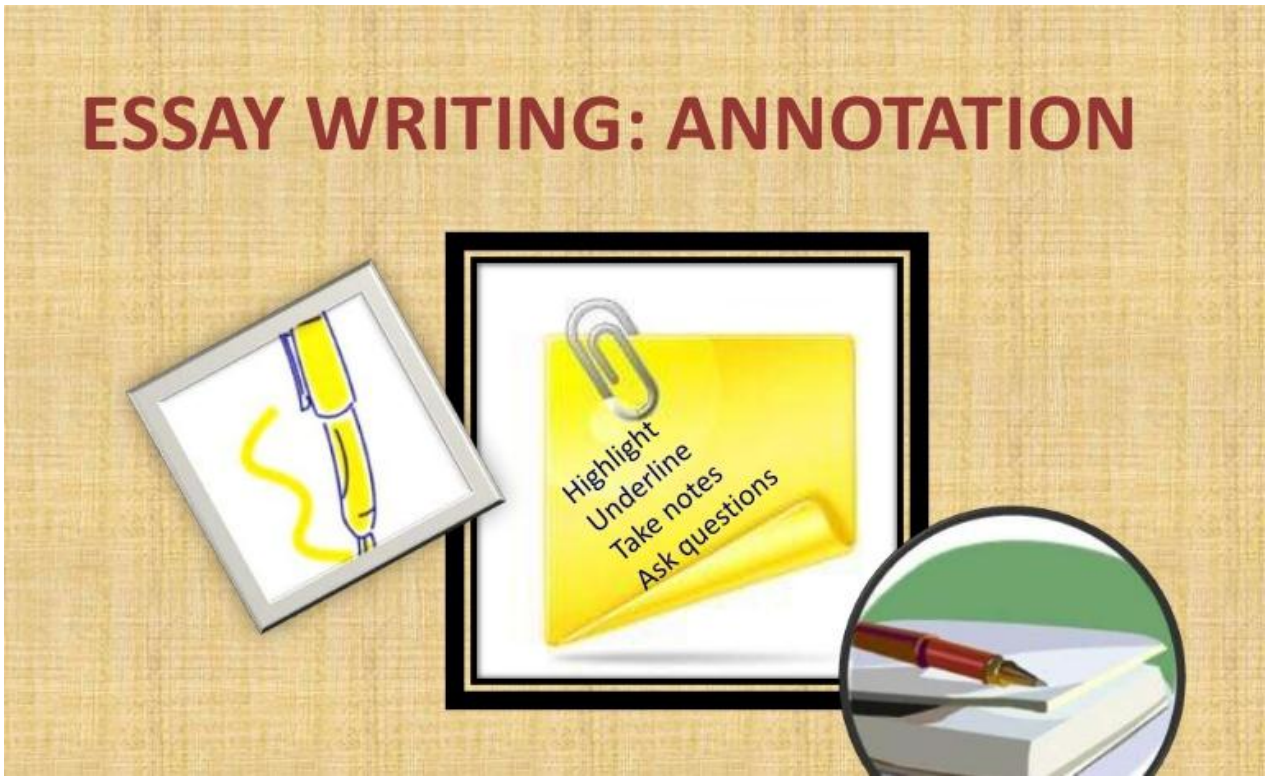
PASSIVE VOICE English: learn, read, enjoy!

	Simple to be V3	Continuous to be being V3	Perfect To have been V3
Present	am / is / are } V3	am / is / are } being V3	have / has } been V3
Past	was / were } V3	was / were } being V3	had been V3
Future	Shall / will } be V3	-----	will have been V3

PASSIVE VERB TENSES

	ACTIVE VOICE	PASSIVE VOICE
Present Simple	He **delivers** the letters.	The letters **are delivered**.
Past Simple	He **delivered** the letters.	The letters **were delivered**.
Future Simple	He **will deliver** the letters.	The letters **will be delivered**.
Present Continuous	He **is delivering** the letters.	The letters **are being delivered**.
Past Continuous	He **was delivering** the letters.	The letters **were being delivered**.
Going to	He **is going to deliver** the letters.	The letters **are going to be delivered**.
Present Perfect	He **has delivered** the letters.	The letters **have been delivered**.
Past Perfect	He **had delivered** the letters.	The letters **had been delivered**.
Infinitive	He **has to deliver** the letters.	The letters **have to be delivered**.
Modals	He **must deliver** the letters.	The letters **must be delivered**.

Appendix 7



SummarizingEnglishScientificLiterature

Языканнотации

Clichés for annotation writing

The article introduces/presents/gives/describes…
The article reveals …
The article contains…
The article points out that …
The publication deals with…
The study/paper presents/discusses…
The paper shows/presents/regards/examines…
The author considers/outlines/concludes/ points out…
The author concentrates on…
The author views/reviews/ presents…
The author analyses how…/ examines why…/

Обратите внимание!

Научная статья обычно состоит из следующих частей:

1. Заголовок (Title). 2. Аннотация (Abstract or Summary). 3. Введение (Introduction). 4. Общая часть (Methods, Materials, Procedures). 5. Результаты, обсуждение результатов, заключение (выводы) и рекомендации (Results, Discussions, Conclusion, Recommendations). 6. Использованная литература (References, Literature, Bibliography).

PLAN OF ANNOTATION

A) **Headline of the text**
I'd like to present the article headlined...
I"m going to speak about the article under the headline...
b) **Source**
- The article is (comes) from...
- The article was carried (published) by...
- It is of the 1-st of October, 2012
- The author of the article is... The article is by...
c) **Theme**
- The article is about...
- It deals with... It covers...
- The text traces (presents, describes, focuses on)...
d) **Idea**
- The author of the article stresses (urges, makes it clear) that...
- The main idea of the author is that...
- The author's aim is... The author aims at...
e) **Judgment**
It seems to me that...
I think (suppose, believe) that...
It is clear to me...It is obvious that..,
To my mind... In my opinion...

Practice yourself in writing an annotation

Оглавление

Учебное издание

АНГЛИЙСКИЙ ЯЗЫК ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ, ИСПОЛЬЗУЮЩИХ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

ENGLISH FOR THE FUTURE INFORMATION TECHNOLOGY SPECIALISTS IN THEIR PROFESSIONAL ACTIVITIES

Учебное пособие
по английскому языку

Составители:
Борисова Светлана Викторовна
Гончарова Виктория Аркадьевна

В авторской редакции

ISBN 978-5-9266-1947-5

Подписано в печать 14.04.2023. Формат 60x84 1/16.
Усл. печ. л. 13,5. Тираж 60 экз. Заказ 132.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.