

Краснодарский университет МВД России



**ПРОФЕССИОНАЛЬНО-ОРИЕНТИРОВАННЫЕ МАТЕРИАЛЫ
ДЛЯ УГЛУБЛЕННОГО ИЗУЧЕНИЯ АНГЛИЙСКОГО ЯЗЫКА
В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ
ТЕХНОЛОГИЙ**



Краснодар
2025

Краснодарский университет МВД России

**Профессионально ориентированные материалы
для углубленного изучения английского языка в сфере
информационно-телекоммуникационных технологий**

Учебное пособие

Краснодар
2025

УДК 811.111(075.8)
ББК 81.2Англ-9
П841

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

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

Рецензенты:

Б. Н. Селин, кандидат педагогических наук (Белгородский юридический институт МВД России имени И. Д. Путилина);

Н. Н. Серостанова, кандидат педагогических наук (Воронежский институт МВД России).

Профессионально ориентированные материалы для
П841 углубленного изучения английского языка в сфере информационно-телекоммуникационных технологий: учебное пособие / сост.: С. В. Борисова, В. А. Гончарова. – Краснодар: Краснодарский университет МВД России, 2025. – 324 с.

ISBN 978-5-9266-2170-6

Содержатся современные аутентичные профессионально ориентированные материалы для углубленного изучения английского языка обучающимися по специальности «Информационно-телекоммуникационные технологии в правоохранительной сфере». Особое внимание уделяется профессиональной лексике, необходимой для деятельности будущих сотрудников органов внутренних дел в сфере безопасности информационных технологий.

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

УДК 811.111(075.8)
ББК 81.2Англ-9

ISBN 978-5-9266-2170-6

© Краснодарский университет
МВД России, 2025
© Борисова С. В., Гончарова В. А.,
составление, 2025

Оглавление

Введение.....	4
UNIT 1. Computer and computer processing systems.....	6
UNIT 2. Software and Internet technologies.....	27
UNIT 3. Computer networks.....	40
UNIT 4. Programming: languages, methods and technologies.....	71
UNIT 5. The concept and problems of information security.....	79
UNIT 6. Types and methods of data security. Cryptographic data security...	119
UNIT 7. Malicious computer programs and protection from their effects...	134
UNIT 8. Classification of crimes. Computer crimes.....	151
UNIT 9. Cybercrime. Cyberterrorism and extremism: definition, types.....	156
UNIT 10. Information and telecommunication computer technologies in investigating crimes.....	236
REFERENCES.....	243
APPENDIX 1.....	244
APPENDIX 2.....	245
APPENDIX 3.....	248
APPENDIX 4.....	251

ВВЕДЕНИЕ

Ключевым фактором совершенствования и оптимизации правоохранительной деятельности, как и любого федерального органа исполнительной власти, являются информационно-коммуникационные технологии, что особенно актуально в условиях информационно-технического прогресса.

Методическая организация пособия предусматривает выполнение целевых установок программы – научить будущих профессионалов – сотрудников полиции понимать и обсуждать англоязычную литературу, связанную со всеми аспектами деятельности, направленной на борьбу с высокотехнологичными преступлениями, воспринимать на слух иноязычную речь и объясняться в определенных ситуациях профессионального характера на изучаемом языке по данной теме.

Пособие состоит из 10 разделов (*1. Компьютер и компьютерные технологии обработки информации, 2. Программное обеспечение. Интернет технологии, 3. Средства и системы связи, 4. Программирование: языки, методы, технологии, 5. Понятие и проблемы информационной безопасности, 6. Виды и способы защиты информации. Криптографическая защита информации, 7. Вредоносные компьютерные программы и защита от их воздействия., 8. Понятие «преступления». Компьютерные преступления, 9. Киберпреступность – понятие, виды и методы защиты, 10. Информационно-телекоммуникационные компьютерные технологии в расследовании преступлений*) и нескольких приложений (*инструкций по написанию эссе, составлению презентаций и реферированию текста*).

Цель данного пособия состоит в развитии навыков разных видов чтения - изучающего, просмотрового, поискового и аналитического.

Каждый раздел включает в себя различные тексты, содержащие ряд лексических единиц, а также упражнения, направленные на расширение,

закрепление и активизацию как специальной, так и общеупотребительной лексики.

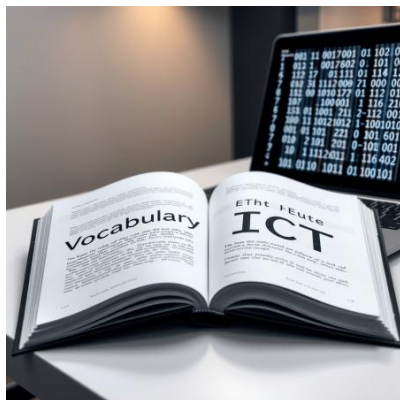
Данное пособие может быть использовано в качестве дополнения к общезыковым учебникам по данной специальности и для самоконтроля обучающихся.

Аутентичные профессионально-ориентированные тексты на английском языке могут быть использованы профессорско-преподавательским составом, адъюнктами, курсантами и слушателями образовательных организаций МВД России. Уделяется особое внимание на профессиональную лексику, необходимую для будущих сотрудников ОВД по специальности 10.05.05 – безопасность информационных технологий в правоохранительной сфере, желающими совершенствовать навыки чтения и перевода оригинальной литературы на английском языке по данной специальности.

UNIT 1. Computer and computer processing systems



Text 1



Study this vocabulary:

IBM (International Business Machine) – фирма по производству компьютеров

to enter the fray – ввязаться в драку

computer of choice – лучший компьютер

to fall by the wayside – остаться в стороне;
уступить дорогу

to survive onslaught – выдержать конкуренцию

siliconchip - кремнёвый кристалл; чип

K - единица ёмкости памяти, равная 1024 байтам, словам или битам

wordsize - размер слова; разрядность двоичного слова

soft-copyoutput - вывод электронной; программно-управляемой копии

hard-copyoutput - вывод «твёрдой» печатной копии

a cathode-ray tube - катодно-лучевая трубка

floppy disks – гибкий диск

Read the text “PERSONAL COMPUTERS”

Personal computers are supposed to appear in the late 1970s. One of the first and most popular personal computers was the Apple II, introduced in 1977 by Apple Computer. During the late 1970s and early 1980s, new models and competitive operating systems seemed to appear daily. Then, in 1981, IBM entered the fray with its first personal computer, known as the IBM PC. The IBM PC quickly became the personal computer of choice, and most other personal computer manufacturers fell by the way-side. One of the few companies to survive IBM's onslaught was Apple Computer, which is sure to remain a major player in the personal computer marketplace. In less than a decade the microcomputer has been transformed from a calculator and hobbyist's toy into a personal computer for almost everyone.

What is a personal computer? How can this device be characterized?

— First, a personal computer being microprocessor-based, its central processing unit, called a microprocessor unit, or MPU, is concentrated on a single silicon chip.

— Second, a PC has a memory and word size that are smaller than those of minicomputers and large computers. Typical word sizes are 8 or 16 bits, and main memories range in size from 16 K to 512 K.



— Third, a personal computer uses smaller, less expensive, and less powerful input, output and storage components than do large computer systems. Most often, input is by means of a keyboard, soft-copy output being displayed on a cathode-ray tube screen. Hard-copy output is produced on a low-speed character printer.

— A PC employs floppy disks as the principal online and offline storage devices and also as input and output media.

— Finally, a PC is a general-purpose, stand-alone system that can begin to work when plugged in and be moved from place to place.

Probably the most distinguishing feature of a personal computer is that it is used by an individual, usually in an interactive mode. Regardless of the purpose for which it is used, either for leisure activities in the home or for business applications in the office, we can consider it to be a personal computer.

Ex.1. Answer the questions:

1. When did the first personal computer appear?
2. What was one of the first PC model?
3. What is a personal computer?
4. What are the four main characteristics of a PC?
5. What does the term “microprocessor-based” mean?
6. What are the typical word sizes of a PC?
7. How is input carried out in personal computers?
8. What principle storage devices do PC use?
9. What kind of a system is a PC?
10. What differs personal computers from large computer systems?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. The Apple II was introduced in 1977 by Apple Computer.
2. IBM entered the personal computer market in 1980 with its first PC.
3. Most personal computer manufacturers survived IBM’s entry into the market.
4. A personal computer is microprocessor-based.
5. Personal computers have larger word sizes than minicomputers.

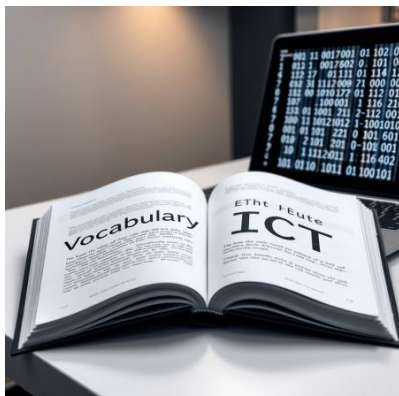
6. Hard-copy output for PCs is usually produced on a high-speed printer.
7. Floppy disks were used as storage devices in personal computers.
8. Personal computers are not portable.
9. A personal computer can be used only in business environments.
10. One of the most distinguishing features of a PC is that it is used interactively by an individual.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. appear			
2. introduce			
3. enter			
4. become			
5. fall			
6. survive			
7. transform			

Text 2



Study this vocabulary:

conduct - проводить

err on the side of caution – действовать с наименьшим риском

gaming consoles – игровая приставка

hazardous - опасный

illustrate - иллюстрировать; показывать

longtermexposure - долговременное воздействие

potential - потенциальный

Read the text “MOBILE PHONES”

Is talking on a mobile phone hazardous to your health? It is difficult to know for sure. Some research suggests that heavy users of mobile phones are at a greater risk of developing brain tumours. However, many other studies suggest there are no links between cancer and mobile phone use.

The main problem with the current research is that mobile phones have only been popular since the 1990s. As a result, it is impossible to study the long term exposure of mobile phone use. This concerns many health professionals who point out that many cancers take at least ten years to develop. Another concern about these studies is that many have been funded by those who benefit financially from the mobile phone industry.



Many cancers take 10 years to develop.

Over three billion people use mobile phones on a daily basis, and many talk for more than an hour a day. Mobile phone antennas are similar to microwave ovens. While both rely on electromagnetic radiation, the radio waves in mobile phones are lower in radio frequency (RF). Microwave ovens have enough RF to cook food and are therefore known to be dangerous to human tissues. However, the concern is that the lower frequency radio waves that mobile phones rely on

may also be dangerous. It seems logical that holding a heat source near your brain for a long period of time is a potential health hazard.

Mobile phones get hot when they are used for a long period of time.

Some researchers believe that other types of wireless technology may also be dangerous to human health, including laptops, cordless phones, and gaming consoles. Organizations that are concerned about the effects of Electromagnetic Radiation (EMR) suggest replacing all cordless devices with wired ones. They say that many cordless phones emit dangerous levels of EMR even when they are not in use. They even suggest keeping electronic devices, such as computers and alarm clocks out of bedrooms, or at least six feet from your pillow.

Other wireless technology may also be hazardous to our health.

A growing number of health professionals worldwide are recommending that mobile phone users err on the side of caution until more definitive studies can be conducted. They recommend that adults use head sets or speaker phones and that children and teens, whose brain tissue are still developing, use mobile phones only for emergencies. Concerned medical experts use the example of tobacco to illustrate the potential risks. Many years ago, people smoked freely and were not concerned about the effects of cigarettes on their health. Today, people know that cigarettes cause lung cancer, though it is still unknown exactly how or why. Some doctors fear that the same thing will happen with devices such as mobile phones.

Ex. 1. Answer the questions:

1. According to the text, do mobile phones lead to brain tumours?
2. The text mentions the 1990s because this was when the mobile phones were invented.
3. Why does the article mention microwave ovens?
4. How is mobile phone use compared to tobacco use in this article?
5. Do you think that prolonged use of mobile phones can affect our health (for example cause fatigue and headaches, emit radiation, excite brain cells, etc.)?

6. Another word for dangerous is
7. The device used for playing video games is a gaming
8. The term "funded" means
9. Microwaves are a type of.....
10. A synonym for "to show" is

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

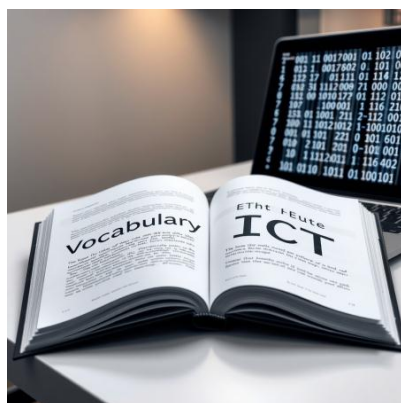
1. Some studies suggest a link between heavy mobile phone use and brain tumours.
2. All studies agree that mobile phone use causes cancer.
3. Mobile phones have been widely used since the early 1980s, which allows for long-term health studies.
4. Many cancers take at least ten years to develop.
5. Radio waves from mobile phones are more powerful than those from microwave ovens.
6. Mobile phones can become hot during extended use.
7. Laptops and cordless phones are considered safe and emit no electromagnetic radiation.
8. Cordless phones emit EMR even when not in use.
9. Health professionals recommend keeping electronic devices away from your.
10. Doctors compare mobile phone use to tobacco, suggesting that future research may show serious health risks.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. suggest			
2. point out			
3. rely			
4. may be dangerous			
5.fear			
6. recommend			
7. compare			

Text 3



Study this vocabulary:

handling - оперирование
assembly - сборка
gripper - зажимное устройство
spotwelding - точечная сварка
spindle - вал; шпиндель
arcwelding – дуговая сварка

grinding - шлифовка

spraying - окраска распылением

frame - обрамлять

rod - стержень

seam - шов

pickup – забрать, собрать

conveyor - конвейер

arrangement – устройство, оборудование

gripper – захват, манипулятор

grasp – уловить, схватить

spotwelding – точечная сварка

arc welding – электродуговая сварка

Read the text “ROBOTS IN INDUSTRY”

Today most robots are used in manufacturing operations. The applications of robots can be divided into three categories:

1. material handling
2. processing operations
3. assembly and inspection.

Material-handling is the transfer of material and loading and unloading of machines. Material-transfer applications require the robot to move materials or work parts from one to another. Many of these tasks are relatively simple: robots



pick up parts from one conveyor and place them on another. Other transfer operations are more complex, such as placing parts in an arrangement that can be calculated by the robot. Machine loading and unloading operations utilize a robot to load and unload parts. This requires the robot to be equipped with a gripper

that can grasp parts. Usually the gripper must be designed specifically for the particular part geometry.

In processing operations robot manipulates a tool to perform a process on the work part. Examples of such applications include spot welding, continuous arc welding and spray painting. Spot welding of automobile bodies is one of the most common applications of industrial robots. The robot positions a spot welder against the automobile panels and frames to join them. Arc welding is a continuous process in which robot moves the welding rod along the welding seam. Spray painting is the manipulation of a spray-painting gun over the

surface of the object to be coated. Other operations in this category include grinding and polishing in which a rotating spindle serves as the robot's tool.

Ex. 1. Answer the following questions:

1. How can robots be used in industry?
2. How can robots load and unload parts?
3. What are examples of processing operations a robot performs?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

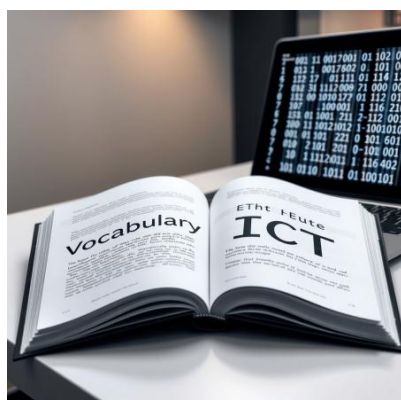
1. Most robots today are used in manufacturing operations.
2. There are four main categories of robot applications.
3. Material handling includes transferring materials and loading/unloading machines.
4. Robots used for material transfer only perform complex tasks.
5. In machine loading and unloading, robots require a special tool called a gripper to grasp parts.
6. Grippers must be designed specifically for the part's shape.
7. In processing operations, robots move parts between machines.
8. Spot welding is one of the most common applications of industrial robots.
9. Arc welding is a process where the robot moves the welding rod along the seam.
10. Spray painting involves moving a spray gun over the surface to coat it.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. require			
2. pick up			
3. place			
4. utilize			
5. grasp			
6. manipulates			
7. positions			
8. moves			

Text 4



Study this vocabulary:

interface – интерфейс
 methods of external communication – методы
 внешней коммуникации
 outside entities – внешние объекты
 programming language – языки
 программирования

network interface – сетевой интерфейс

user interface – пользовательский интерфейс

physical interface – физический интерфейс

Interface in Computer Science

An interface defines the communication boundary between two entities, such as a piece of software, a hardware device, or a user. It generally refers to an abstraction that an entity provides of itself to the outside. This separates the methods of external communication from internal operation, and allows it to be internally modified without affecting the way outside entities interact with it, as

well as provide multiple abstractions of itself. It may also provide a means of translation between entities which do not speak the same language, such as between a human and a computer. Because interfaces are a form of indirection, some additional overhead is incurred versus direct communication. Supporting Languages. Certain programming languages have different methodologies for allowing the construction of interfaces. In general, any programming language can implement an interface, but the following programming languages provide specific interface constructs of some kind or another: ActionScript in Flash, Ada, C++ (using nonstandard extensions), C#, ColdFusion, D, Delphi, Eiffel, Java, Logtalk, Mesa, ML, Modula, Modula-2, Modula-3, Oberon, Objective-C, REALbasic, Unified Modeling Language, Visual Basic, Clarion Interface may refer to: in computer science:

- Interface (computer science), an abstraction of a software component

- Interface (Java), an abstract type which is used to specify an interface that classes must implement

- Network interface, a point of interconnection between a terminal and a network or between two networks

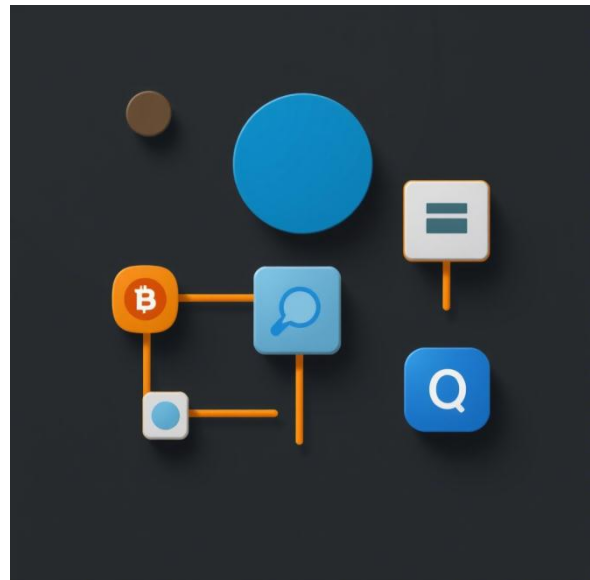
- User interface, the aggregate of means by which people interact with a machine, device, computer program, or other complex tool
- Graphical user interface in other fields:

- Interface (chemistry), a surface forming a boundary between two phases

- Interface (music group), an electronic music artist based in New York

- Interface (novel), a 1994 novel by Neal Stephenson and George Jewsbury

- Interface" (TNG episode), a seventh season episode of Star Trek: The Next Generation



- Interface Inc., a carpet company focused on environmental sustainability
- Physical interface, a device for joining electric circuits together

Ex. 1. Answer the questions:

1. What does interface define?
2. What can interface refer to?
3. What separates the methods of external communication from internal operation?
4. What affects the way outside entities interact with interface?
5. What can interface provide for?
6. Why is some additional overhead incurred versus direct communication?
7. What supporting languages are listed in the text?
8. Why do certain programming languages have different methodologies?
9. Why does any programming language can implement an interface

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

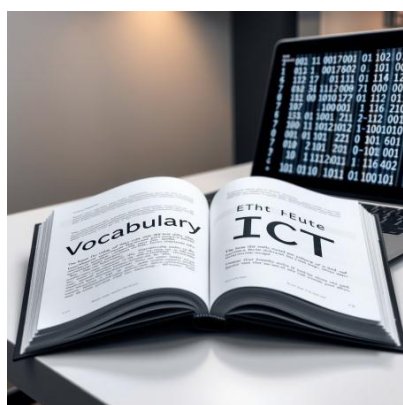
1. An interface defines the communication boundary between two entities.
2. Interfaces allow internal modifications without affecting external interactions.
3. Interfaces cannot be used to translate between different languages, such as between humans and computers.
4. Using interfaces reduces communication overhead compared to direct communication.
5. Only certain programming languages can implement interfaces.
6. Java provides specific constructs for creating interfaces.
7. The term "interface" is only used in computer science.
8. A user interface is how people interact with machines or software.
9. An interface in Java is a concrete class that contains implemented methods.
10. Interface Inc. is a company known for making video games.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. defines			
2. provide			
3. incurs			
4. construct			
5. support			
6. implement			
7. refers			
8. allows			

Text 5



Study this vocabulary:

transistors – транзистор

vacuum tubes – вакуумная лампа

semiconductor – полупроводник

integrated circuit – интегральная схема

switch - переключатель

discrete components – дискретные компоненты

chip – электронный чип

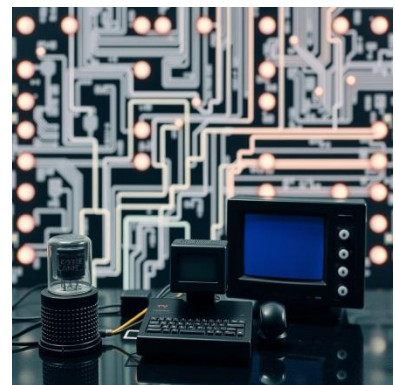
software – программное обеспечение

STEPS IN THE DEVELOPING OF COMPUTERS

1. In 1948 due to the invention of transistors there appeared the possibility to replace vacuum tubes. The transistor occupied an important place on the way to computer development. The potential advantage of the transistor over the vacuum tube was almost as great as that of the vacuum tube over the relay. A transistor can switch flows of electricity as fast as the vacuum tubes used in computers, but the transistors use much less power than equivalent vacuum tubes, and are considerably smaller. Transistors are less expensive and more reliable. They were mechanically rugged, had practically unlimited life and could do some jobs better than electronic tubes. Transistors were made of crystalline solid material called semiconductor.

With the transistor came the possibility of building computers with much greater complexity and speed.

2. The integrated circuit constituted another major step in the development of computer technology. Until 1959 the fundamental logical components of digital computers were the individual electrical switches, first in the form of relays, then vacuum tubes, then transistors. In the vacuum tubes and relay stages, additional discrete components, such as resistors, inductors, and capacitors were required in order to make the whole system work. These components were generally each about the same size as packaged transistors. Integrated circuit technology permitted the elimination of some of these components and integration of most of the others on the same chip of semiconductor that contains the transistor. Thus the basic logic element — the switch, or "flip-flop", which required two separate transistors and some resistors and capacitors in the early 1950s, could be packaged into a single small unit in 1960. The chip was an important achievement in the accelerating step of computer technology.



3. In 1974 a company in New Mexico, called Micro Instrumentation Telemetry System (MITS) developed the Altair 8800, a personal computer (PC) in a kit. The Altair had no keyboard, but a panel of switches with which to enter the information. Its capacity was less than one per cent that of the 1991 Hewlett-Packard handheld computer. But the Altair led to a revolution in computer electronics that continues today. Hardware manufacturers soon introduced personal computers, and software manufacturers began developing software to allow the computers to process words, manipulate data, and draw. During the 1980s computers became progressively smaller, better and cheaper.

Today the personal computer can serve as a work station for the individual. A wide array of computer functions are now accessible to people with no technical background.

1. Answer the questions:

1. What occupied an important place on the way to computer development?
2. What constituted another major step in the development of computer technology?
3. What were transistors made of?
4. What did a company in New Mexico develop in 1974?
5. Can the personal computer serve as a work station for the individual?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Transistors replaced vacuum tubes because they were smaller, used less power, and were more reliable.
2. Transistors cannot switch electricity as fast as vacuum tubes.
3. The integrated circuit was introduced before 1959.
4. Before the integrated circuit, computers required many separate components like resistors and capacitors.

5. The integrated circuit allowed multiple components to be placed on a single chip.
6. The Altair 8800 was the first personal computer available only pre-assembled.
7. The Altair 8800 had a keyboard for entering information.
8. The Altair 8800 started a revolution in computer electronics.
9. Personal computers became smaller, better, and cheaper during the 1980s.
10. Today's personal computers can be used by people without technical backgrounds.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. replace			
2. eliminate			
3. permit			
4. integrate			
5. develop			
6. switch			
7. occupy			
8. constitute			

Text 6



Study this vocabulary:

voltage – напряжение

data bases – база данных

digitization – оцифровка

central processing unit (CPU) – центральный процессор

input devices устройства ввода

output devices – устройства вывода

hardware – аппаратное обеспечение

auxiliary storage units – дополнительное запоминающее устройство

DIGITAL COMPUTERS

There are two fundamentally different types of computers: analog and digital. In current usage, the term "computer" usually refers to high-speed digital computers. These computers are playing an increasing role in all branches of the economy.

Digital computers are based on manipulating discrete binary digits (1s and 0s). They are generally more effective than analog computers for four principal reasons: they are faster; they are not so susceptible to signal interference; they



can transfer huge data bases more accurately; and their coded binary data are easier to store and retrieve than the analog signals.

For all their apparent complexity, digital computers are considered to be simple machines. Digital computers are able to recognize only two states in each of its millions of switches, "on" or "off", or high voltage or low voltage. By assigning binary numbers to there states, 1 for "on" and 0 for "off", and linking many switches together, a computer can represent any type of data from numbers to letters and musical notes. It is this process of recognizing signals that is known as digitization. The real power of a computer depends on the speed with which it checks switches per second. The more switches a computer checks in each cycle, the more data it

can recognize at one time and the faster it can operate, each switch being called a binary digit or bit.

A digital computer is a complex system of four functionally different elements: 1) the central processing unit (CPU), 2) input devices, 3) memory-storage devices called disk drives, 4) output devices. These physical parts and all their physical components are called hardware.

The power of computers greatly on the characteristics of memory-storage devices. Most digital computers store data both internally, in what is called main memory, and externally, on auxiliary storage units. As a computer processes data and instructions, it temporarily stores information internally on special memory microchips. Auxiliary storage units supplement the main memory when programmes are too large and they also offer a more reliable method for storing data. There exist different kinds of auxiliary storage devices, removable magnetic disks being the most widely used. They can store up to 100 megabytes of data on one disk, a byte being known as the basic unit of data storage.

Output devices let the user see the results of the computer's data processing. Being the most commonly used output device, the monitor accepts video signals from a computer and shows different kinds of information such as text, formulas and graphics on its screen. With the help of various printers information stored in one of the computer's memory systems can be easily printed on paper in a desired number of copies.

Programmes, also called software, are detailed sequences of instructions that direct the computer hardware to perform useful operations. Due to a computer's operating system hardware and software systems can work simultaneously. An operating system consists of a number of programmes coordinating operations, translating the data from different input and output devices, regulating data storage in memory, transferring tasks to different processors, and providing functions that help programmers to write software. In large corporations software is often written by groups of experienced programmers, each person focusing on a specific aspect of the total project.

1. Answer the questions:

1. How many fundamentally different types of computers are there?
2. What are digital computers based on?
3. What are digital computers able to recognize?
4. What is called software?
5. What is often written by groups of experienced programmers?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Digital computers are the same as analog computers.
2. Today, the word 'computer' usually refers to a digital computer.
3. Digital computers use continuous signals to represent information.
4. Digital computers are more effective than analog ones because they are slower and have less storage.
5. A digital computer can recognize only two states: "on" and "off".
6. The binary number 1 represents "off" and 0 represents "on" in digital computers.
7. The CPU is one of the four main components of a digital computer.
8. All physical parts of a computer are called software.
9. Main memory is used only to store programmes permanently.
10. Auxiliary storage devices are used when programmes are too large for the main memory.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

INFINITIVE (BASE FORM)	PAST SIMPLE	PAST PARTICIPLE	PRESENT PARTICIPLE / -ING
refer			
play			
base			
manipulate			
depend			
check			
operate			
call			
store			
retrieve			
supplement			
offer			
use			
print			
direct			
work			
coordinate			
translate			
regulate			
transfer			
provide			

UNIT 2. Software and Internet technologies



Text 1



Study this vocabulary:

Social connectedness — социальная
связанность/присутствие
interaction - общение; взаимодействие
facilitate - облегчать
excel - превосходить; отличаться
explicitly - точно; ясно; явно

bulletinboards - информационные доски/стенды

hashtag - тематическая метка в социальных сетях; хэштег

reachout - связаться; устанавливать контакт; обращаться; держать связь

resist - сопротивляться

Read the text “INTERACTIVITY”

Humans have a strong need for social connectedness and interaction. It is one of our deepest and strongest desires. Most individuals in high-tech societies are part of social networks that contain, collectively, hundreds of social ties that represent a variety of strengths (from weak to strong) and purposes (from instrumental to expressive).

A prime use of the internet and digital media is socializing—making new friends, reconnecting with old ones, and spending time with family both physically near and far away. As with physical places, individuals like to invite family, friends, coworkers, and acquaintances to join them in digital spaces. Because it is so easy to



feel the presence of others online, it is common to spend time in social interaction with them there.

The internet and digital media thus facilitate and encourage social connectedness. Some social networking sites explicitly help individuals find and associate with one another, and many specialize and excel at this. Like email, texting, and speaking on the phone, these sites create a space for people to get to know one another and to potentially become involved in one another's lives. They also allow friends who know one another offline to stay in touch and maintain their friendships.

People exhibit extraordinary creativity in finding ways to interact and connect online.

They develop and join groups of all kinds, from Facebook and Google groups to internet forums and bulletin boards. They invent ways to identify one another and form groups online, such as the hashtag, and invent platforms and apps that constantly reimagine the ways that people can interact.

With mobility, this kind of connectivity can take place almost constantly. Cell phones, tablets, and other mobile/portable media make it easy to reach out to others anytime, anywhere.

With a phone at one's side—always there, always on—social interaction can be nearly always enabled. It can be difficult to resist the temptation to check for messages, updates, and news. Some worry that media-enabled communication and relationships will somehow replace or substitute for face-to-face relationships. But research has indicated precisely the opposite. In general, use of the internet tends to prompt—not substitute for—face-to-face interaction. It is very common to use the internet, cell phones, and mobile media to make dates to get together with others. Mobile phones even allow people to make plans on the go and are often used to do so. And, along with social media, they are used to support and maintain relationships with faraway others—to keep bonds strong in between physical meetings and make those meetings far more likely. Social interaction is well supported by the internet and digital media.

Ex. 1. Answer the following questions:

1. What is the prime use of the internet and digital media?
2. How do social networking sites help individuals find and associate with one another?
3. What allows friends to stay in touch and maintain their friendships?
4. What can replace or substitute for face-to-face relationships?
5. What gadgets allow people to make plans?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Humans have a strong need for social connectedness and interaction.
2. Most individuals in high-tech societies are part of social networks with only a few weak connections.

3. One of the main uses of the internet is socializing.
4. People do not enjoy inviting others into digital spaces.
5. The internet makes it harder to feel the presence of others.
6. Social networking sites help people find and connect with each other.
7. Digital communication replaces face-to-face interaction completely.
8. People use hashtags and online groups to identify each other and form communities online.
9. Mobile devices make it more difficult to stay in touch with others.
10. Mobile phones are never used to make plans on the go.

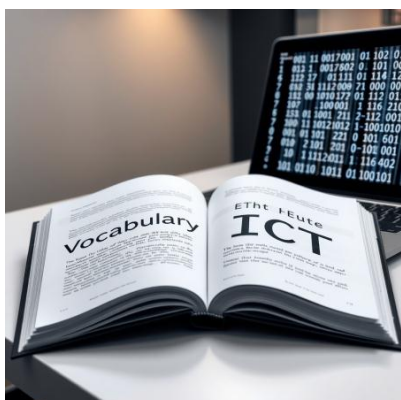
Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

INFINITIVE (BASE FORM)	PAST SIMPLE	PAST PARTICIPLE	PRESENT PARTICIPLE / - ING
spend			
facilitate			
encourage			
help			
associate			
create			
allow			
develop			
join			
invent			
make			
reach out			

check			
worry			
indicate			
prompt			
substitute			
support			

Text 2



Study this vocabulary:

virtual reality – виртуальная реальность

invention – изобретение

helmet – шлем

lenses - линзы

illusion – иллюзия

surgeon – хирург

simulator - симулятор

Read the text “COMPUTER GAMES AND VIRTUAL REALITY”

Computer games are gaining more and more popularity nowadays. Some people claim that teenagers get a lot of benefits playing them. But other people argue that young people should spend



their free time going in for sport. Let`s look upon this problem objectively and try to understand it. To begin with, computer games develop memory, because when you play it you try to remember all details. Moreover, it develops logical

thinking, language and basic computer skills. Apart from that, you can make virtual friends. So it is another way of communication. And if you like each other, you can meet in the future and become close friends. In addition, playing computer games is a good way of entertainment. To start with, computer games have a harmful effect on health. First of all, you can spoil your eye sight. Besides, you sit in the same place and don't move so you can gain weight. Another point to be made is that a lot of games have aggressive moments and this makes teenagers cruel and causes violent behavior. Furthermore, young people spend too much time on this and it can ruin relationships with people.

Not long ago computers were considered an amazing invention. Today they form part of our everyday life. The latest thing today is Virtual Reality. A Virtual Reality system can transport the user to exotic locations such as a beach in Hawaii or the inside of the human body. The Virtual Reality system is still in the early stages of its development. At the moment it is necessary to put a large helmet on your head to see the simulated world and you have to wear a special glove on your hand in order to manipulate the objects you see there. Lenses and two miniature display screens inside the helmet create the illusion that the screen surrounds you on every side.

You can «look behind» computer— generated objects, pick them up and examine them, walk around and see things from a different angle. Already today Virtual Reality is used in medicine. In hospitals, surgeons could plan operations by first «travelling» through the brain, heart or lungs without damaging the body. It is also used in police training schools. In schools pupils could explore the Great Pyramid or study molecules from the inside. Developers of Virtual Reality say its potential is powerful.

Ex1. Answer the following questions:

1. What can computer games develop?
2. What kind of communication do you have with the help of computer?
3. What is Virtual Reality?

4. Why do you need to wear helmet and special glove?
5. What are the possible uses of Virtual Reality?
6. What are some of the disadvantages of Virtual Reality?
7. Do you think Virtual Reality is an important invention or not?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

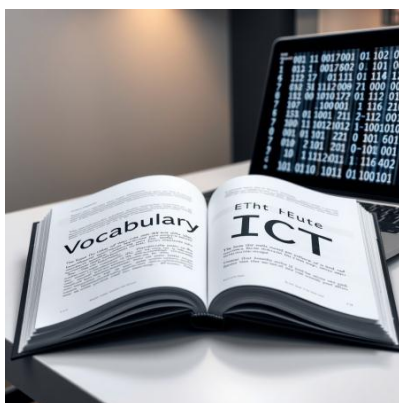
1. Computer games are becoming more popular nowadays.
2. Playing computer games can help develop memory and logical thinking.
3. Computer games improve physical health because they make players more active.
4. Virtual Reality systems are already widely used by everyone today.
5. Some people believe that teenagers should spend their free time playing sports instead of playing computer games.
6. Playing computer games helps improve language skills and basic computer skills.
7. All computer games help build strong real-life friendships.
8. Virtual Reality allows users to explore places like a beach in Hawaii or the inside of the human body.
9. Computer games always cause violent behavior in teenagers.
10. Virtual Reality is currently used in medicine and education.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

INFINITIVE (BASE FORM)	PAST SIMPLE	PAST PARTICIPLE	PRESENT PARTICIPLE / -ING
claim			
argue			
look			
try			
develop			
remember			
make			
meet			
spoil			
sit			
move			
cause			

Text 3



Study this vocabulary:

network – сеть

to embrace - охватывать; окружать

to design - задумывать; придумывать;
разрабатывать

to survive - выжить

nuclear war – ядерная война

to pollute – загрязнять

path - путь; маршрут

available - доступный; имеющийся в распоряжении; наличный

packet switching - пакетное переключение

invention - изобретение

accurate - точный

to count - считать; сосчитать

approximately - приблизительно; примерно

to receive - получать

to provide - снабжать; доставлять; обеспечивать

reliable – надежный

provider - провайдер; поставщик

router — маршрутизатор

to intercept - перехватить (сигнал и т. д.)

to encode - кодировать; шифровать

notwithstanding - тем не менее; однако; все же

to crack - взломать

to circulate - передвигаться/двигаться в пределах чего-то

tremendous - разг. огромный; гигантский; громадный; потрясающий

Read the text “INTERNET AND MODERN LIFE”

The Internet has already entered our ordinary life. Everybody knows that the Internet is a global computer network, which embraces hundred of millions of users all over the world and helps us to communicate with each other.

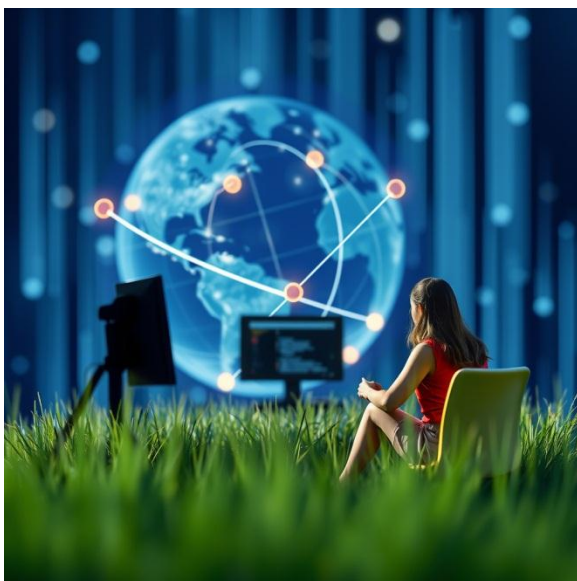
The history of Internet began in the United States in 1969. It was a military experiment, designed to help to survive during a nuclear war, when everything around might be polluted by radiation and it would be dangerous to get out for any living being to get some information to anywhere. Information sent over the Internet takes the shortest and safest path available from one computer to another. Because of this, any two computers on the net will be able to stay in touch with each other as long as there is a single route between them. This technology was called packet switching.

Invention of modems, special devices allowing your computer to send the information through the telephone line, has opened doors to the Internet for millions of people.

Most of the Internet host computers are in the United States of America. It is clear that the accurate number of users can be counted fairly approximately, nobody knows exactly how many people use the Internet today, because there are hundred of millions of users and their number is growing.

Nowadays the most popular Internet service is e-mail. Most of the people use the network only for sending and receiving e-mail messages. They can do it either they are at home or in the internet clubs or at work. Other popular services are available on the Internet too. It is reading news, available on some dedicated news servers, telnet, FTP servers, etc.

In many countries, the Internet could provide businessmen with a reliable, alternative to the expensive and unreliable telecommunications systems its own system of communications. Commercial users can communicate cheaply over the Internet with the rest of the world. When they send e-mail messages, they only have to pay for phone calls to their local service providers, not for international calls around the world, when you pay a good deal of money.



But saving money is only the first step and not the last one. There is a commercial use of this network and it is drastically increasing. Now you can work through the internet, gambling and playing through the net.

However, there are some problems. The most important problem is security. When you send an e-mail, your message can travel through many different networks and computers. The data is constantly being directed towards its destination by special computers called routers. Because of this, it is possible

to get into any of the computers along the route, intercept and even change the data being sent over the Internet. But there are many encoding programs available. Notwithstanding, these programs are not perfect and can easily be cracked.

Another big and serious problem of the net is control. Yes, there is no effective control in the Internet, because a huge amount of information circulating through the net. It is like a tremendous library and market together. In the future, the situation might change, but now we have what we have. It could be expressed in two words—an anarchist's dream.

Ex.1. Answer the following questions:

1. What is the Internet?
2. When and where did the history of Internet begin?
3. Why was the Internet designed?
4. What is modem?
5. Where are most of the Internet host computers?
6. What is the accurate number of internet users?
7. What is the most popular Internet service today?
8. What are other popular services available on the Internet?
9. What is the most important problem of the Internet?
10. Why is there no effective control in the Internet today?
11. Is there a commercial use of the network today?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. The Internet is a global computer network that connects millions of users worldwide.
2. The Internet was originally created as a military experiment in 1969.
3. The Internet was designed to help people survive during natural disasters.

4. Information on the Internet travels along the longest and safest path between computers.
5. Packet switching allows computers to stay connected even if only one route exists between them.
6. Modems allowed people to connect to the Internet through telephone lines.
7. The exact number of Internet users is known and easy to count.
8. E-mail is the most popular service offered by the Internet.
9. People can only use e-mail at home.
10. You have to pay international rates when sending e-mail through the Internet.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

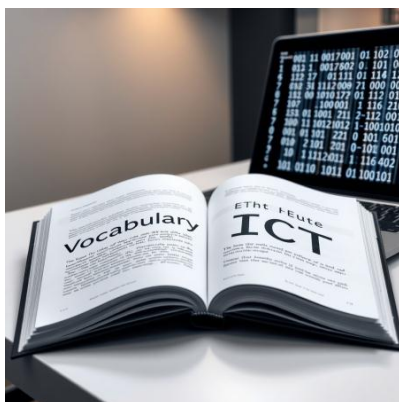
INFINITIVE (BASE FORM)	PAST SIMPLE	PAST PARTICIPLE	PRESENT PARTICIPLE / -ING
use			
provide			
pay			
save			
increase			
work			
gamble			
play			
travel			
direct			
get			

intercept			
change			
encode			
crack			
describe			

UNIT 3. Computer networks



Text 1



Study this vocabulary:

network – сеть

to captivate – пленить

to log on - входить; подключаться

to last - длиться

overload - перегрузка

to grow - расти; увеличиваться

breakthrough - крупное достижение; прорыв

voicemail - голосовое послание

videoconferencing - видео-конференц-связь

Web TV - веб-телевидение

to browse - просматривать

cellularphone - сотовый телефон

to dial up - набирать номер, звонить

answering machine - автоответчик

to handle - обращаться; иметь дело с
amount – количество
fiber optic cables - оптоволоконный кабель
opposed - зд. вместо
binary code - бинарный код, двоичный код
amount of bandwidth - пропускная способность
fast modem - быстрый модем
coaxial cable - коаксиальный кабель
to increase 1,000 fold - увеличить(ся) в 1000 раз
satellite dish - спутниковая тарелка
lane - линии движения
clog - засорение; препятствие
customer - клиент; покупатель
business time - бизнес-время

Read the text “THE FUTURE OF THE INTERNET”

Everywhere we go, we hear about the Internet. It's on television, in magazines, newspapers, and in schools. One might think that this network of millions of computers around the globe is as fast and captivating as television, but with more and more users logging on everyday and staying on longer and longer, this «Information Superhighway» could be perhaps more correctly referred to as an expressway of big city centre at rush hour.

It is estimated that thirty five to forty million users currently are on the Internet. According to a recent statistics, an average Internet call lasts five times as longer as the average regular telephone call. 10 percent of the Internet calls last 6 hours or longer. This can cause an overload and, in turn, cause telephone network to fail.

The local network was designed for short calls which you make and then hang up, but Internet calls often occupy a line for hours. With so many users in the Internet and their number is growing by 200 percent annually, it certainly

provides new challenges for the telephone companies. The Internet, up to the beginning of the 90s, was used only to read a different texts. Then in the early 90's, a way was made to see pictures and listen to a sound on the Internet. This breakthrough made the Internet to be most demanded means of communication, data saving and transporting.

However, today's net is much more than just pictures, text, and sound. The Internet is now filled with voice messages, video conferencing and video games. With voice messages, users can talk over the Internet for the price of the local phone call.

Nowadays we no longer have to own a computer to access the Internet. Now, -devices such as Web TV allow our television to browse the Web and use Electronic Mail. Cellular phones are now also dialing up the Internet to provide E-mail and answering machine services. The telephone network was not designed and built to handle these sorts of things. Many telephone companies are spending enormous amounts of money to upgrade the telephone lines.

K. Kao and G. Hockman were the first to come up with the idea of using fiber optic cables, as opposed to copper wire, to carry telephone signals. Fiber optics uses pulses of light to transmit binary code, such as that used in computers and other electronic devices. As a result the amount of bandwidth is incredibly raised. Another solution for the problem is fast modems which satisfy the need for speed.

By accessing the Net through the coaxial cable that provides television to our homes, the speed can be increased 1,000 fold. However, the cable system was built to only send information one way. In other words, they can send stuff to us, but we can't send anything back, if there is no modem available.



Yet another way is being introduced to access the Internet, and that is through the use of a satellite dish just like the TV dishes currently used to deliver television from satellites in space to your home. However, like cable connection, the information can only be sent one way.

Faster ways of connecting to the Internet may sound like a solution to the problem, but, just as new lanes on highways attract more cars, a faster Internet could attract many times more users, making it even slower than before.

To help solve the problem of Internet clogs, Internet providers are trying new ways of pricing for customers. So, in business time any connection to Net cost more than your connection in the night.

In conclusion, I should add that if we want to keep the Internet usable and fairly fast, we must not only improve the telephone lines and means of access, but also be reasonable in usage.

Ex.1. Answer the following questions:

1. How many users are currently in the Internet?
2. How long does an average Internet call last?
3. What can cause the overload of the telephone system?
4. What was the main purpose of the Internet up to the 90s?
5. Do we need to have a computer to get access to the Internet today?
6. Who was the first to come up with the idea of using fiber optic cables?
7. What is the alternative way to get access to the Internet today?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. The Internet is discussed in many media, including television, magazines, newspapers, and schools.
2. The Internet can be compared to a busy city expressway during rush hour because of heavy traffic.

3. There are currently about 20 million users on the Internet.
4. An average Internet call lasts five times longer than an average regular telephone call.
5. Ten percent of all Internet calls last six hours or more.
6. Local telephone networks were designed for long Internet calls.
7. The number of Internet users is growing by 200% annually.
8. Until the early 1990s, the Internet was used only for reading texts.
9. The Internet became more popular after it started supporting images and sound.
10. Today, the Internet supports voice messages, video conferencing, and online games.
11. Voice messages over the Internet cost as much as international phone calls.

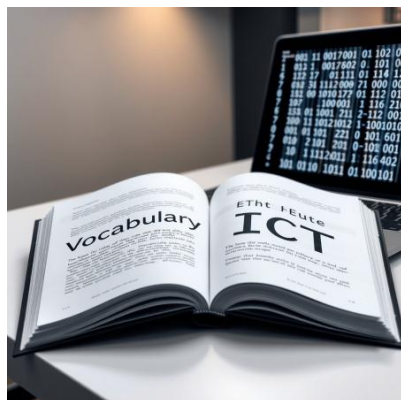
Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

INFINITIVE (BASE FORM)	PAST SIMPLE	PAST PARTICIPLE	PRESENT PARTICIPLE / -ING
go			
hear			
think			
log			
hang			
grow			
use			

make			
provide			
send			

Text 2



Study this vocabulary:

unauthorized access – несанкционированный доступ

misuse – неправильное использование

confidentiality – конфиденциальность

transmission – передача

storage – хранилище

processing – обработка

hardware – аппаратное обеспечение

destruction – разрушение

triangle – треугольник

tangible object – материальный объект

essential – существенный

intentional – преднамеренный

vulnerabilities – уязвимости

gain – выгода, доход

inherent – свойственный

asset – объект, ценный вклад

subordinate – второстепенный

convict – осужденный

Read the text: What Is Security?

In general, security is “the quality or state of being secure — to be free from danger.” In other words, protection against adversaries — from those who would do harm, intentionally or otherwise — is the objective. National security, for example, is a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people. Achieving the appropriate level of security for an organization also requires a multifaceted system.

A successful organization should have the following *multiple layers of security* in place to protect its operations:

- *Physical security*, to protect physical items, objects, or areas from unauthorized access and misuse.

- *Personnel security*, to protect the individual or group of individuals who are authorized to access the organization and its operations.

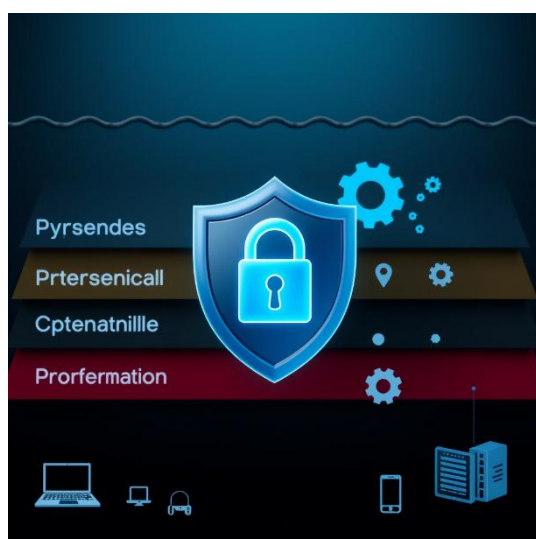
- *Operations security*, to protect the details of a particular operation or series of activities.

- *Communications security*, to protect communications media, technology, and content.

- *Network security*, to protect networking components, connections, and contents.

- *Information security*, to protect the confidentiality, integrity and

availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.



The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the

systems and hardware that use, store, and transmit that information. Information security includes the broad areas of information security management, computer

and data security, and network security. The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A. triangle. The C.I.A. triangle has been the industry standard for computer security since the development of the mainframe. It is based on the three characteristics of information that make it valuable to organizations: confidentiality, integrity, and availability. The security of these three characteristics of information is as important today as it has always been, but the C.I.A. triangle model no longer adequately addresses the constantly changing environment. The threats to the confidentiality, integrity, and availability of information have evolved into a vast collection of events, including accidental or intentional damage, destruction, theft, unintended or unauthorized modification, or other misuse from human or nonhuman threats. This new environment of many constantly evolving threats has prompted the development of a more robust model that addresses the complexities of the current information security environment. The expanded model consists of a list of critical characteristics of information.

Key Information Security Concepts

A number of terms and concepts are essential to any discussion of information security.

— ***Access***: A subject or object's ability to use, manipulate, modify, or affect another subject or object. Authorized users have legal access to a system, whereas hackers have illegal access to a system. Access controls regulate this ability.

— ***Asset***: The organizational resource that is being protected. An asset can be logical, such as a Web site, information, or data; or an asset can be physical, such as a person, computer system, or other tangible object. Assets, and particularly information assets, are the focus of security efforts; they are what those efforts are attempting to protect.

— ***Attack***: An intentional or unintentional act that can cause damage to or otherwise compromise information and/or the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect. Someone casually reading sensitive information not intended for his or her use is a passive attack. A hacker attempting to break into an information system is an intentional attack. A lightning strike that causes a fire in a building is an unintentional attack. A direct attack is a hacker using a personal computer to break into a system. An indirect attack is a hacker compromising a system and using it to attack other systems, for example, as part of a botnet (slang for robot network). This group of compromised computers, running software of the attacker's choosing, can operate autonomously or under the attacker's direct control to attack systems and steal user information or conduct distributed denial-of-service attacks. Direct attacks originate from the threat itself. Indirect attacks originate from a compromised system or resource that is malfunctioning or working under the control of a threat.

— ***Control, safeguard, or countermeasure***: Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve the security within an organization.

— ***Exploit***: A technique used to compromise a system. This term can be a verb or a noun. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain. Or, an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or is created by the attacker. Exploits make use of existing software tools or custom-made software components.

— ***Exposure***: A condition or state of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.

— ***Loss***: A single instance of an information asset suffering damage or unintended or unauthorized modification or disclosure. When an organization's information is stolen, it has suffered a loss.

— ***Protection profile or security posture***: The entire set of controls and safeguards, including policy, education, training and awareness, and technology, that the organization implements (or fails to implement) to protect the asset. The terms are sometimes used interchangeably with the term security program, although the security program often comprises managerial aspects of security, including planning, personnel, and subordinate programs.

— ***Risk***: The probability that something unwanted will happen. Organizations must minimize risk to match their risk appetite — the quantity and nature of risk the organization is willing to accept.

— ***Subjects and objects***: A computer can be either the subject of an attack — an agent entity used to conduct the attack — or the object of an attack — the target entity. A computer can be both the subject and object of an attack, when, for example, it is compromised by an attack (object), and is then used to attack other systems (subject).

Threat: A category of objects, persons, or other entities that presents a danger to an asset. Threats are always present and can be purposeful or undirected. For example, hackers purposefully threaten unprotected information systems, while severe storms incidentally threaten buildings and their contents.

— ***Threat agent***: The specific instance or a component of a threat. For example, all hackers in the world present a collective threat, while Kevin Mitnick, who was convicted for hacking into phone systems, is a specific threat agent. Likewise, a lightning strike, hailstorm, or tornado is a threat agent that is part of the threat of severe storms.

— ***Vulnerability***: A weaknesses or fault in a system or protection mechanism that opens it to attack or damage. Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door. Some well-known vulnerabilities have been examined, documented, and published; others remain latent (or undiscovered).

Ex.1. Answer the following questions:

1. Does personnel security protect the details of a particular operation or series of activities?
2. Does network security protect communications media?
3. What is CNSS?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Security is defined as the state of being free from danger.
2. National security includes protecting a country's people, assets, and resources.
3. The C.I.A. triangle stands for Confidentiality, Integrity, and Authorization.
4. Information security focuses only on protecting digital data.
5. The C.I.A. model still fully covers all modern information security challenges.
6. Access refers to a subject or object's ability to use or affect another subject or object.
7. An asset can be either logical (like data) or physical (like a computer).
8. A hacker trying to break into a system is an example of a passive attack.

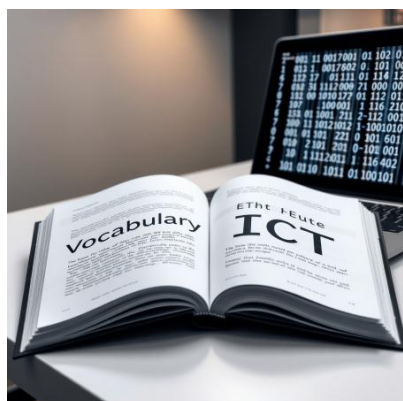
9. A lightning strike that causes damage is considered an unintentional threat.
10. Controls, safeguards, and countermeasures help reduce risk and improve security.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. protect			
2. access			
3. define			
4. include			
5. cause			
6. compromise			
7. modify			

Text 3



Study this vocabulary:

span – промежуток, период

layering on – наложение

overlapping of – дублирование, перегрузка

implementation – выполнение, осуществление

prudent – благоразумный

diligence – усердие, старательность

stockholders – акционеры

Read the text @Information security

Information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information. The information must be protected while in motion and while at rest. During its life time, information may pass through many different information processing systems and through many different parts of information processing systems. There are many different ways the

information and information systems can be threatened. To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms. The building up, layering on and



overlapping of security measures is called defense in depth. The strength of any system is no greater than its weakest link. Using a defense in depth strategy, should one defensive measure fail there are other defensive measures in place that continue to provide protection.

The three types of controls (administrative controls, logical controls, and physical controls) can be used to form the bases upon which to build a defense in depth strategy. With this approach, defense in depth can be conceptualized as three distinct layers or planes laid one on top of the other. Additional insight into defense in depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people as the outer layer of the onion, and network security, host based security and applications security forming the inner layers of the onion. Both perspectives are equally valid and each provides valuable insight into the implementation of a good defense in depth strategy.

Information security as a process The terms reasonable and prudent person, due care and due diligence have been used in the fields of Finance,

Securities and Law for many, many years. In recent years these terms have found their way into the fields of computing and information security. USA Federal Sentencing Guidelines now make it possible to hold corporate officers liable for failing to exercise due care and due diligence in the management of their information systems.

In the business world, stockholders, customers, business partners and governments have the expectation that corporate officers will run the business in accordance with accepted business practices and in compliance with laws and other regulatory requirements. This is often described as the “reasonable and prudent person” rule.

A prudent person takes due care to insure that everything necessary is done to operate the business by sound business principles and in a legal ethical manner.

A prudent person is also diligent (mindful, attentive and ongoing) in their due care of the business.

In the field of Information Security, Harris offers the following definitions of due care and due diligence:

“Due care are steps that are taken to show that a company has taken responsibility for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees.” And, [Due diligence are the] “continual activities that make sure the protection mechanisms are continually maintained and operational.”

Attention should be paid to two important points in these definitions. First, in due care, steps are taken to show — this means that the steps can be verified, measured, or even produce tangible artifacts. Second, in due diligence, there are continual activities — this means that people are actually doing things to monitor and maintain the protection mechanisms and, these activities are ongoing.

Ex.1. Answer the following questions:

1. What does each aspect of information security process consist in?

Assess

Protect

Detect

Respond

Review

2. How do you understand the following: “The strength of any system is no greater than its weakest link”?

3. What types of information security controls are mentioned in the text?

4. What does information security as a process involve?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Information security must protect information only during its creation and disposal.
2. Information needs to be protected both while it is being transmitted and when it is stored.
3. Information may pass through many different systems during its life cycle.
4. Defense in depth means using a single strong protective mechanism to secure information.
5. In defense in depth, if one security measure fails, others continue to provide protection.
6. The three types of controls used in defense in depth are administrative, logical, and physical.
7. Defense in depth can be compared to layers of an onion, with data at the core.

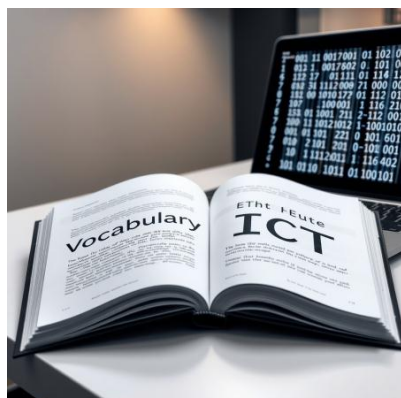
8. "Reasonable and prudent person" is a concept not related to information security.
9. Due care refers to steps taken to show that a company is responsible for its activities.
10. Due diligence involves continuous efforts to maintain and monitor protection mechanisms.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. create			
2. dispose			
3. pass			
4. threaten			
5. build			
6. layer			
7. maintain			

Text 4



Study this vocabulary:

conduct - проводить

err on the side of caution – действовать с наименьшим риском

gaming consoles - игровая приставка

hazardous - опасный

illustrate - иллюстрировать; показывать

longterm exposure - долговременное воздействие

potential - потенциальный

Read the text: How Strong is Your Information Security Program?

Traditionally, documented security policies have been viewed as nothing more than a regulatory requirement. While this may have been true in the past, building a strong information security program (ISP) is a business imperative as you fight to keep the customers you have and work to attract new ones. Your information security policies can either work to help you grow your business or signal a red flag that security is not a top priority.



No matter how strong your security posture is now, if you don't document it, it won't last. You must assume that people instrumental in building your security environment will eventually move on. In that respect, training the replacement is a lot less painful and much more effective with a written guide. Without a policy manual, the new employee would eventually learn what to do but would you really want to risk a security incident while they are trying to figure it out? It's important to understand that there is no procedure, policy, or technology that will ever be 100% secure. It just doesn't exist. You can, however, endeavor to get as close to perfect as possible.

Lack of a documented security policy is a huge red flag when determining liability in the event of an incident. You do not know when the next attack will happen and if someone is aggressively targeting you, they will cause pain. When time comes to defend yourself, no matter the strength of your security environment, the lack of a documented information security program is a

message that management has not taken data security seriously. This perception becomes increasingly dangerous when we're talking about a court of law and an untold number of potential customers in the court of public opinion.

Ex.1. Answer the following questions:

1. What is the purpose of building an information security programme of an organisation?
2. Why do you think the author refers to it as *a business imperative*?
3. Why should your security posture be documented?
4. What is the role of training in maintaining a strong security posture of a company, according to the author?
5. What does a documented security policy imply?
6. What is the lack of a documented information security programme fraught with?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Documented security policies used to be considered only as a regulatory requirement.
2. A strong information security program can help attract new customers and retain existing ones.
3. If your security posture is strong, there is no need to document it.
4. Written policies make training new employees easier and more effective.
5. Without documented policies, new employees will never learn how to perform their duties.
6. It is possible to create a completely 100% secure system with the right policy or technology.

7. The absence of a documented security policy may signal that management does not take data security seriously.
8. In case of an incident, having no written security policy may increase legal liability.
9. The author suggests that even the strongest technical security measures are enough to protect an organization.
10. Public perception of a company's security practices has no real impact on its business.

Ex. 4. Write down ten word-combinations with a verb.

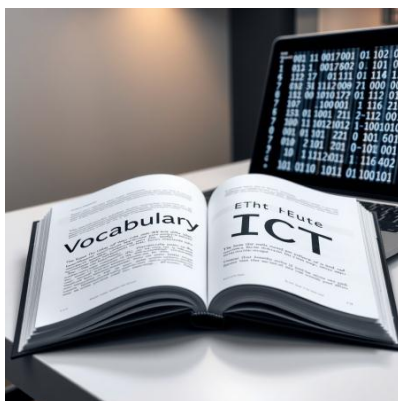
Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. view			
2. build			
3. work			
4. last			
5. train			
6. learn			
7. endeavor			

UNIT 4. Programming: languages., methods and technologies



Text 1



Study this vocabulary:

bitmap images – растровые изображения

characters – символы

paper transactions – бумажные транзакции

translates – преобразование

accuracy – точность

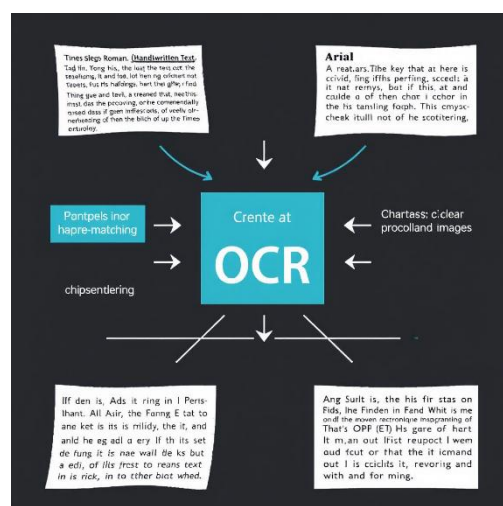
delays – задержки

Read the text: OCR Technology

Optical Character Recognition (OCR) – used extensively throughout business and government – examines scanned bitmap images of machine-printed text and translates the characters into ASCII text files that can be edited. For instance, paper checks contain number series written in machine print designed

to minimize recognition errors. These codes contain bank routing numbers, the holder's account numbers and other information required to process paper transactions. Machine print conversion is largely a solved problem in this application, as OCR software was included in the first commercial systems that automated machine print text recognition.

Optical Character Recognition (OCR) systems recognize only machine print. Using pattern-matching technology, OCR translates the shapes and patterns of machine-made characters into corresponding computer codes. Though most advanced systems are able to recognize multiple fonts, they can process only standard fonts such as Times Roman and Arial. Once all characters in a given word are recognized, the word is compared against a vocabulary of potential answers for the final result.



Character recognition then segments lines of text or words into separate characters that are recognized by the makeup of their component shapes. Machine-printed letters are evenly spaced across, and up-and-down, a given page, allowing the OCR system to read the text one character at a time. Segmentation into single characters represents a critical recognition failure point for forms processing organizations, because OCR recognition technology requires high-quality images with excellent contrast, character and clarity. Any text that is less than perfect will cause even the most sophisticated OCR systems to return significant reductions in accuracy when processing degraded images. For example, when characters break apart due to poor image quality, or if multiple characters merge due to blurred or dark backgrounds between them, recognition accuracy may be reduced by as much as 20 percent.

The most commonly accepted OCR accuracy measurement is represented by the percentage of characters correctly read on a given page of text, and systems vary widely, achieving 95 to 99 percent accuracy. But accuracy rates at anything below 100 percent can translate into huge productivity losses. An entire application or verification process could be compromised if even 5 percent of the data is either entered incorrectly or misread. Therefore, OCR systems must have the ability to ‘proofread’ results, mark characters the system does not recognize, and send rejected text to human operators for manual processing. Needless to say, such human intervention increases costs and delays.

Intelligent Character Recognition (ICR) converts hand printed characters to their machine print (ASCII) equivalents, representing a significant step forward in technology when compared to older OCR systems that only read machine print. The ability to recognize handprint significantly broadens the range of applications that benefit from automated ICR solutions, saving time and increasing accuracy to levels not attainable by OCR or human intervention.

ICR software is based on the science of neural networks that behave like the human brain when processing information. Because ICR can handle variations in character shape, the term 'intelligent' is combined with 'character recognition' to describe handprint recognition.

Ex.1. Answer the questions:

1. What is the difference between OCR, ICR and Intelligent Recognition?
2. Why isn't OCR just enough?
3. Why is it so difficult to automatically recognize handwriting?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. OCR stands for Optical Character Recognition.
2. OCR technology is used only in government institutions and not in business.

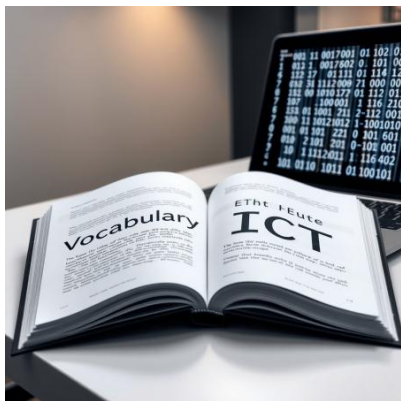
3. OCR translates scanned images of printed text into editable ASCII files.
4. Paper checks often contain machine-printed numbers that can be read by OCR systems.
5. OCR systems can recognize both machine-printed and handwritten text equally well.
6. OCR uses pattern-matching technology to translate characters into computer codes.
7. Most advanced OCR systems can recognize all fonts, including unusual handwriting styles.
8. After recognizing individual characters, OCR compares the word with a vocabulary list.
9. Segmentation of characters is not important for OCR accuracy.
10. OCR systems perform well even when image quality is poor.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. examine			
2. translate			
3. contain			
4. minimize			
5. recognize			
6. process			
7. represent			

Text 2



Study this vocabulary:

handwriting – почерк

misinterpreted – неверно истолкованный

eliminates – исключить

Read the text: Intelligent Recognition technology

The basic principle of Parascript® Intelligent Recognition states that handwriting, when reduced to its most basic components, is essentially motion, or a series of movements, made by a writing instrument. According to this theory, any handwriting can be described using elements of a special description language. The eight elements that make up the trajectories of all cursive letters (Figure 1 below) form a ring that illustrates the possible transitions of neighbor elements. Figure 2 - An example of the letter 'd' described using motion theory. The order of elements in the letter description follows the trajectory of a pen. Horizontal lines show the vertical position on the image associated with each element in the letter description.



Both OCR and ICR deliver high accuracy when analyzing constrained text (OCR with machine print and ICR with handprint) but are ineffective when dealing with cursive, where letters are linked together, and

may be poorly written or even illegible. Consider a situation where the symbol segmentation of an image is ambiguous. In Figure 3 below, an OCR/ICR recognition system could determine that the first symbol is a 'd' or a combination of a 'c' and an 'l'. Depending on the segmentation, the reading

result produced by a letter-based recognition technology may be completely different: ‘clear’ in the first case and ‘dear’ in the second. As accurate character segmentation is critical, Intelligent Recognition can often recognize poor-quality text that would be impossible for OCR and ICR systems to recognize. Intelligent Recognition dynamically uses context in a process similar to the one humans employ when reading and interpreting text to compensate for the inherent ambiguity of human handwriting. The context is used during the recognition process rather than after recognition, when results might already have been misinterpreted, thus improving the accuracy of results. Again, going back to Figure 3, it is not clear if the first symbol is a ‘d’ or a combination of a ‘c’ and an ‘l’.

The dynamic vocabularies contained in Intelligent Recognition systems do not analyze and store all possible hypotheses of segmentation. If the dynamic vocabulary does not contain a combination of ‘c’ and an ‘l’ at the beginning of the word, the only possible segmentation solution is ‘d’. The dynamic usage of context eliminates all impossible combinations from the solution set, enabling the evaluation of results ‘on the fly’ during the recognition process. Dynamic context, therefore, provides the highest possible recognition accuracy, because it eliminates the impossible results in real time, during the recognition process.

Intelligent Recognition technology often recognizes text that is considered to be of poor quality or even completely unacceptable for OCR and ICR technologies, therefore further improving the recognition rates when compared to other systems. Working with high quality machine print, OCR provides recognition accuracy of nearly 100 percent (99.9 %), a level of accuracy acceptable for many forms processing applications. ICR cannot guarantee the same levels of accuracy that OCR systems deliver on machine print due to the inherent problems of reading handprint spacing variations, diversity of human writing styles, etc. Instead, state of the art ICR systems provide the same recognition accuracy for a certain part of the data stream, while the data that cannot be reliably read continue to be sent for visual verification. The following

mechanism is used by ICRs to ensure the accuracy required by the application. The stream of images is divided into two parts: those that were recognized reliably with a required accuracy (accepted), and those for which the system does not guarantee the required accuracy (rejected).

Intelligent Recognition further improves recognition rates and accuracy when compared to traditional machine print (OCR) and handprint (ICR) engines through field recognition and cross-validation of results.

Intelligent Recognition recognizes a field not a character, and consequently a whole field is either accepted or rejected. Conversely, in the case of a rejected field Intelligent Recognition technology additionally provides information about unreliable characters. Second, the reject mechanism is tuned so thoroughly that it allows accuracy up to 0.1% for the texts of low quality.

Computing power alone is not able to deliver high recognition results without a human-like recognition approach. Intelligent Recognition employs the most advanced methods of single character recognition while using sophisticated algorithms to cross-validate results during the recognition process.

Intelligent Recognition advances the state of recognition technology, exploiting the strengths and capabilities of its predecessors – OCR and ICR systems, while eliminating their inherent limitations. Intelligent Recognition technology delivers highly accurate machine print, handprint and cursive recognition results, helps eliminate laborious human data entry and has become a proven solution for a broad range of the most demanding applications for government posts, commercial mailers, banks, financial institutions and data processing centers.

Ex.1. Answer the questions:

1. What is the difference between OCR, ICR and Intelligent Recognition?
2. Why isn't OCR just enough?
3. Why is it so difficult to automatically recognize handwriting?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

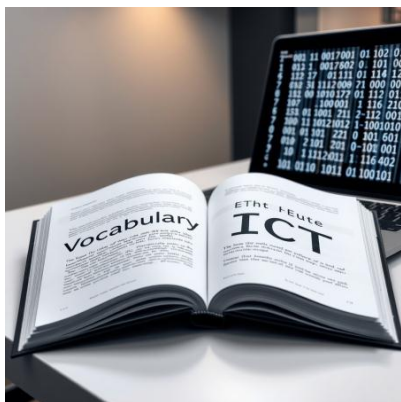
1. According to the motion theory, any cursive letter can be described using eight basic elements.
2. OCR and ICR provide high accuracy when analyzing cursive handwriting.
3. In some cases, OCR/ICR systems may interpret the same symbol differently depending on how it is segmented.
4. Accurate character segmentation is not essential for good recognition results.
5. Intelligent Recognition uses context during the recognition process, similar to how humans read.
6. Dynamic vocabularies in Intelligent Recognition analyze and store all possible hypotheses of segmentation.
7. Dynamic use of context helps eliminate impossible interpretations during recognition.
8. Intelligent Recognition can often recognize poor-quality text that OCR and ICR cannot.
9. OCR provides nearly 100% accuracy only with high-quality machine print.
10. ICR systems achieve the same level of accuracy as OCR even with handwritten text.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. describe			
2. consider			
3. follow			
4. provide			
5. interpret			
6. eliminate			
7. evaluate			

Text 3



Study this vocabulary:

compile – компилятор

functionality – функциональность

postconditions – постусловия

debug versions – версия для отладки

ancestors – предшественник

Interface in Programming

The concept of interface is the cornerstone of modular programming, a forerunner and a standard ingredient of object-oriented programming. In object-oriented programming, an object's interface consists of a set of methods that the object must respond to. Note that the object does not make its instance variables a part of its interface - these are typically accessed by means of accessory methods.

Some object-oriented programming languages mandate that the interface to the object be specified to the compiler separately from the implementation of that object, whilst others relax the requirement. For example, a class in a programming language such as Objective-C consists of its interface, specified in a header file, and the implementation in the source file. Because of the dynamically typed nature of Objective-C, one can send messages to any object, and the interface to the class becomes important as it specifies the methods the class responds to.

Interfaces were historically derived from the header files of the C programming language by restricting their syntactic context and contents, and making them a part of the language semantics (as opposed to a mere preprocessor feature).

The Java programming language takes a different approach to the concept of the interface normally existing in other object-oriented programming languages (i.e. that the interface specified is the interface to the class), in that an interface specifies a set of methods which implement some specific functionality, common to a set of classes.



Some programming languages (e.g. D, Java, Logtalk) allows the definition of interface hierarchies. This allows easy definition of e.g. both minimal and extended versions of an interface.

Some programming languages (e.g. Logtalk) support private and protected implementation of an interface. Thus, the (public) methods declared in an interface can easily become private or protected methods of a class implementing the interface.

The Eiffel language includes in the interface of a class its invariants and the pre-and postconditions of the methods of the class. This is essential to the methodology of design by contract, and may be regarded as an extension of the conditions imposed by the types of the arguments. These rules may be specified in the implementation of a class or in an ancestor which may leave the methods unimplemented. They are extracted by language processors to provide an interface view in the development environment and to generate run-time assertions (checks) in debug versions. The language also ensures that derived classes obey the contracts of their ancestors.

Ex.1. Answer the questions:

1. What is the concept of interface?
2. What is the Java programming language?
3. What does the Eiffel language include?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. The concept of interface is important in modular programming and object-oriented programming.
2. An object's interface includes its instance variables directly.
3. In some programming languages, the interface must be specified separately from the implementation.
4. In Objective-C, interfaces are specified in source files.
5. Interfaces in programming originated from C++ header files.
6. Java uses interfaces in the same way as most other object-oriented programming languages.
7. In Java, an interface defines a set of methods that provide specific functionality shared among several classes.

8. Some programming languages like D, Java, and Logtalk allow interface hierarchies.
9. In Logtalk, methods declared in an interface can be private or protected in a class that implements the interface.
10. The Eiffel language includes method preconditions and postconditions in a class interface.

Ex. 4. Write down ten word-combinations with a verb.

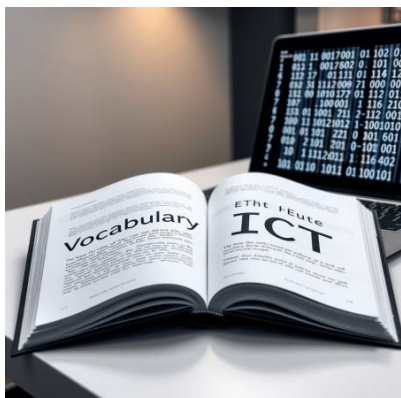
Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. consist			
2. respond			
3. mandate			
4. specify			
5. implement			
6. become			
7. take			

UNIT 5.The concept and problems of information security



Text 1



Study this vocabulary:

Integrity – целостность

Concentration – концентрация

internal systems. – внутренние системы

databases – базы данных

hardware – аппаратное обеспечение

software – программное обеспечение

INFORMATION SECURITY

Information security (InfoSec for short) means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are often interrelated and share the common goals of protecting the confidentiality,

integrity and availability of information; however, there are some subtle differences between them.



These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration.

Information security is concerned with confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print or other forms.

Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory (even a calculator). IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

Information assurance is the act of ensuring that data is not lost when critical issues arise. These issues include but are not limited to: natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists.

One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise. Governments, military, corporations, financial institutions, hospitals, and private

businesses amass a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, not to mention damage to the company's reputation. Protecting confidential information is a business requirement and in many cases also an ethical and legal requirement. For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. There are many ways of gaining entry into the field as a career. It offers many areas for specialization including securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics, etc.

Information Security Attributes: or qualities, i.e., Confidentiality, Integrity and

Availability (CIA). Information Systems are composed in three main portions, hardware, software and communications with the purpose to help identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational.

Essentially, procedures or policies are implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organizations.

Ex.1. Answer the questions:

- 1) What does information security mean?
- 2) What are information security components (attributes)?

- 3) What does computer security focus on?
- 4) What are the most common methods of providing information assurance?
- 5) Why is protecting of confidential information very important?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

Information security means protecting information and systems from unauthorized access, use, and modification.

2. The terms “information security”, “computer security” and “information assurance” are completely different and never overlap.

3. Information security deals only with electronic data.

4. Computer security focuses on securing the information itself rather than the system.

5. A computer is defined as any device with a processor and some memory.

6. IT security specialists are responsible for protecting company technology from cyber attacks.

7. Information assurance is mainly about preventing unauthorized access to data.

8. Off-site backup is one of the methods used in information assurance.

9. Only governments and military organizations deal with confidential information.

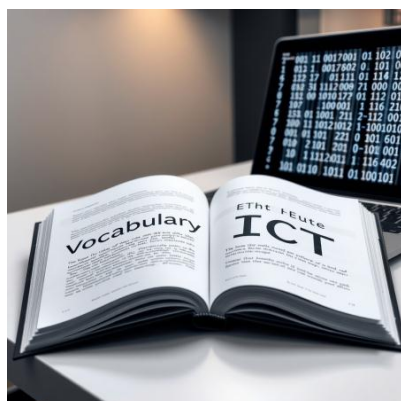
10. If confidential business data falls into the wrong hands, it could lead to financial loss and damage to reputation.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. protect			
2. share			
3. concern			
4. ensure			
5. define			
6. keep			
7. include			

Text 2



Study this vocabulary:

requirement – требование

unclassified – несекретно

Top Secret – совершенно секретно

Labels – метка

SECURITY CLASSIFICATION FOR INFORMATION

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all



information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification. Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

The Business Model for Information Security enables security professionals to examine security from systems perspective, creating an environment where security can be managed holistically, allowing actual risks to be addressed. The type of information security classification labels selected and used will depend on the nature of the organization, with examples being: In the business sector, labels such as: Public, Sensitive, Private, Confidential. In the government sector, labels such as: Unclassified, Sensitive But Unclassified, Restricted, Confidential, Secret, Top Secret and their non-English equivalents. In cross-sectoral formations, the Traffic Light Protocol, which consists of: White, Green, Amber, and Red. All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification of a particular information asset that has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place.

Ex.1. Answer the questions:

- 1) What is an important aspect of information security and risk management?
- 2) Does all information require the same degree of protection?
- 3) What is the first step in information classification?
- 4) What should the classification policy describe and define?
- 5) What factors influence which classification information should be assigned?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Not all information requires the same level of protection.
2. The first step in information classification is to create a classification policy.
3. A classification policy should describe classification labels, criteria, and security controls.
4. All information has the same value to an organization.
5. Information classification is not affected by laws or regulations.
6. The Business Model for Information Security helps professionals manage security from a systems perspective.
7. In the business sector, common classification labels include Secret and Top Secret.
8. Government organizations often use classifications like Confidential, Secret, and Top Secret.
9. Employees do not need training on information classification.
10. Once assigned, the classification of information never needs to be reviewed again.

Ex. 4. Write down ten word-combinations with a verb.

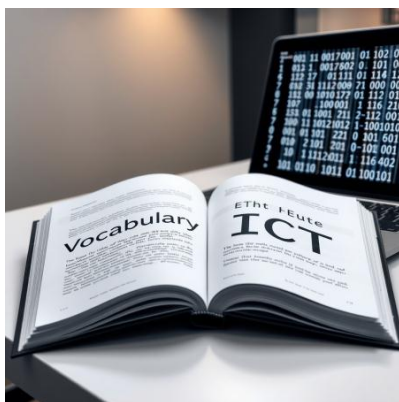
Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. recognize			
2. develop			
3. describe			
4. list			
5.influence			
6. examine			
7. create			

UNIT 6.Types and methods of data security. Cryptographic data security



Text 1



Study this vocabulary:

information assurance – информационная
безопасность, защита
tricky – сложный, хитрый
measures – меры
availability – доступность

integrity – целостность

authentication – аутентификация

confidentiality – конфиденциальность

restoration - восстановление

disruption – нарушение, сбой

The National Institute of Standards and Technology (NIST) -
подразделение Управления по
технологиям США, одного из агентств Министерства торговли США.

achieving – достижение

measures – меры

availability – доступность

compliance – совместимость, согласие

upholding – защита, поддержка, обеспечение

precautions – меры предосторожности

Read the text :Information Protection and Information Assurance

Differentiating between information protection and information assurance can be tricky for some, as the terms are inherently linked and share an ultimate goal of preserving the integrity of information. However, by looking at the scope for each term, there are some important characteristics that should help clarify what IT professionals are commonly referring to when discussing information protection or information assurance. The NIST1 provides definitions for both information assurance and information protection in their Glossary of Key Information Security Terms:

Information Assurance (AI): Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information protection (or information security as defined by the NIST):
The

protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

— integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

— confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and— availability, which means ensuring timely and reliable access to and use of information.

Information protection employs security solutions, encryption, and other technologies, as well as policies and processes, to secure information. Information protection can be thought of as a sub-discipline or component of information assurance. While both share a goal of maintaining the integrity, confidentiality, and availability of information, information protection is specifically focused on achieving this through information security, whereas information assurance powered by TCPDF focuses on ensuring the quality, reliability, and retrievability of information in addition to keeping it protected.

Benefits of Information Protection and Information Assurance



There are many benefits of information protection including maintaining compliance with regulatory standards, preventing costly security incidents, upholding the business' reputation, and preserving the confidence of customers, suppliers, partners, and shareholders. Failure to protect sensitive information can result in fines issued by regulatory agencies

or lawsuits from other companies or individuals should they suffer consequences as a result of their personal data

being breached. Information assurance also offers many benefits in addition to those provided by information protection. In addition to security, information assurance ensures data integrity, usability, non-repudiation, and

authenticity. Confidentiality is achieved as well as availability and reliable and timely access to information.

How Information Protection and Information Assurance Work

Information protection relates to mitigating risks through secure systems and architecture that eliminate or reduce vulnerabilities. IP deals with both operations and technology to try and create a successful method for eliminating vulnerabilities in the system that can be used to gain unauthorized access or compromise or steal data. It may include facets such as vulnerability management, penetration testing, and technological solutions such as firewalls, antivirus, data loss prevention, and encryption. Information assurance identifies ways to control and safeguard critical information in a more effective manner, stressing organizational risk management and overall information quality. Information assurance is typically a broader strategic initiative comprised of a wide range of information protection and management processes. Examples can include security audits, network architecture, compliance audits, database management, and development, implementation, and enforcement of organizational information management policies. Step one to implementing a successful information protection and information assurance program is getting buy-in across the organization. Company leadership must acknowledge that both are vital to an organization's overall business health and profitability. The ultimate goal of both information protection and information assurance is to maintain data integrity, reliability, and accessibility. This includes taking precautions against unauthorized destruction or alteration of information and ensuring non-repudiation and the authenticity of data. These undertakings will assure reliable and timely access to the data while maintaining confidentiality and security and should be priorities for organizations today.

Ex.1. Answer the following questions:

1. How do information protection and information assurance work.

2. What benefits of information protection and information assurance do you know?
3. Can you prove that information protection and information assurance should be priorities for organizations today?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

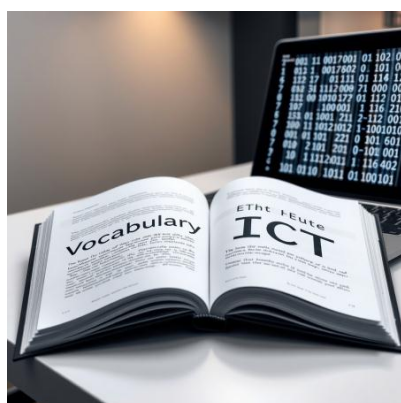
1. Information protection and information assurance have the same meaning and can be used interchangeably.
2. Information assurance includes ensuring availability, integrity, authentication, confidentiality, and non-repudiation of information.
3. Information protection focuses only on data encryption and ignores policies and processes.
4. Information protection is a broader concept than information assurance.
5. One of the benefits of information protection is preventing costly security incidents.
6. Information assurance does not care about the reliability and retrievability of information.
7. Failure to protect sensitive information may lead to fines or lawsuits.
8. Information assurance focuses only on technical aspects of data security.
9. Information protection involves vulnerability management and penetration testing.
10. Company leadership support is not necessary for implementing an effective information protection and assurance program.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. guard			
2. enforce			
3. comprise			
4. stress			
5. control			
6. suffer			
7. create			

Text 2



Study this vocabulary:

defense– защита

malicious – вредоносный

critical – важнейший, ключевой

enterprise– предприятие

sensitive data– конфиденциальные данные

countermeasures – контрмеры, меры

противодействия

firewall – брандмауэр, межсетевой экран

Read the text: Security in Information Technology

Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services. Security is critical for enterprises and organizations of all sizes and in all industries. Weak

security can result in compromised systems or data, either by a malicious threat actor or an unintentional internal threat.

Physical security

Physical security is the protection of personnel, hardware, software, networks and data from physical actions, intrusions and other events that could damage an organization. This includes natural disasters, fire, theft and terrorism, among others. Physical security for enterprises often includes employee access control to the office buildings as well as specific locations, such as data centers. An example of a common physical security threat is an attacker gaining entry to an organization and using a USB storage drive to either copy and remove sensitive data or physically deliver malware directly to systems. Threats to physical security may require less technical savvy on the part of the attacker, but physical security is just as important as information security.

Information security

Information security, also called infosec, encompasses a broad set of strategies for managing the process, tools and policies that aim to prevent, detect and respond to threats to both digital and nondigital information



assets. Infosec includes several specialized categories, including ***application security*** — the protection of applications from threats that seek to manipulate application and access, steal, modify or delete data. These protections use software, hardware and policies, and are sometimes called countermeasures. Common countermeasures include application firewalls, encryption programs, patch management and biometric authentication systems.

Ex.1. Answer the following questions:

*

1. How does the author define *security in information technology*? What does it include?
2. Why is *security critical* for enterprises and organizations of all sizes and all industries?
3. What does *physical security* imply? What are *threats* to physical security?
4. What does *information security* encompass?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

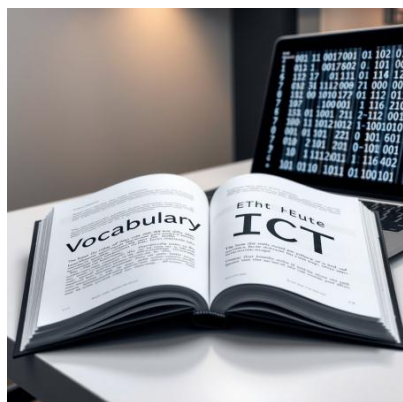
1. Security in IT involves defending digital information and IT assets from threats.
2. Security only concerns large enterprises and not small organizations.
3. Weak security can lead to compromised systems or data.
4. Physical security includes protection from natural disasters, fire, theft and terrorism.
5. Physical security does not include access control to office buildings or data centers.
6. An attacker using a USB drive to steal data is an example of a physical security threat.
7. Physical security threats always require high technical skills.
8. Information security (infosec) deals only with digital information.
9. Application security is a part of information security.
10. Countermeasures in infosec refer to attacks on systems.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. defend			
2. result			
3. protect			
4. require			
5. gain			
6. remove			
7. deliver			

Text 3



Study this vocabulary:

justify – оправдать, объяснить

self-induced – самопроизвольный

expose – разоблачать, выявить

shutdown – прекратить, завершить

enticing ads – привлекательная реклама

duplicate requests – повторяющиеся запросы

scammer – мошенник

pretend – притворяться

embarrassing – затруднительный, неудобный

acquaintances – знакомство

vulnerability – уязвимость

Read the text :Six Common Security Problems

Despite these justify able security concerns about the Web, some of the reasons a person's social media account is compromised are self-induced. Five common mistakes that can expose an account include:

1. Forgetting to Log Out

Increase the security of your social media account by always logging out when you step away from your laptop or computer. It's best to go one step further and close down the browser you were using to view your account. If you leave your account logged in, you set yourself up to be hacked because anyone who can get to your computer can access your account, change the password or even

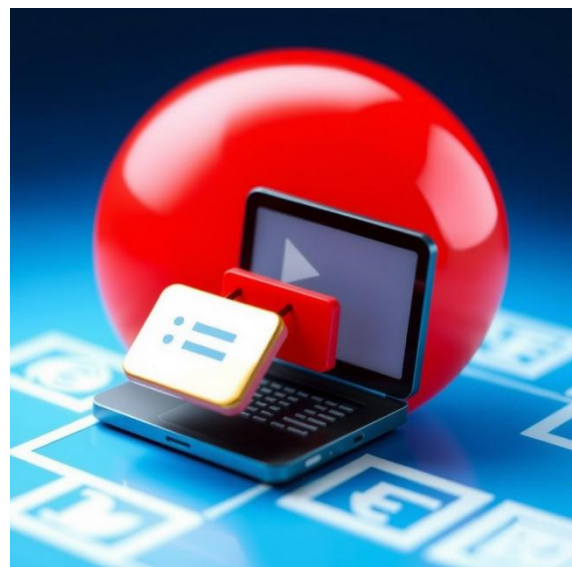
post items and communicate with your friends as if they are you. Logging out and shutting down the browser is even more important if you use a public computer.

2. Clicking on Enticing Ads

Viruses and malware often find their way onto your computer through those annoying, but sometimes enticing ads. However, on the Web, just like in real life, if an offer seems too good to be true, then it probably is. Save yourself a potential security headache — don't click.

3. Connecting With Strangers

Be careful of who you accept invitations from when building your online network. Connecting and sharing information with people you don't know can be dangerous. If you receive friend requests from strangers, it's best to stay away. Further, if you receive friend requests from people you do



know, but are already connected with via the same site, it's possible that someone has set up a fake account. Avoid accepting duplicate requests, instead checking in with the 'real' person to see if the request is legitimate.

You should also be careful when connecting with a celebrity's account, as scammers sometimes pose as famous people. Make sure it is their official, legitimate account and not a stranger pretending to be them before you accept their 'friend' invitation.

4. Using Third Party Apps

Part of the appeal of social media sites are all the various games and apps. Even though a significant number of them are safe, you do grant the app a certain level of permission concerning your information. Make sure you know what the app is viewing and sharing before agreeing to the terms.

5. Exposing Too Much Information

Make sure you understand the level of privacy — or lack of privacy — you are agreeing to when volunteering personal information. Do you really want an app badly enough to allow it to announce where you are? Also, participating in seemingly innocent games, like posting answers to a list of 20 questions, may actually also allow cyber-criminals gather important personal information. For example, the question, "What is your most embarrassing moment?" is probably fine to answer, but answering questions like, "What is your pet's name?" or "Where did you and your significant other meet?" may expose answers you gave to security questions for legitimate sites like Amazon or your bank.

6. Failing to Utilize Security Settings

Social media sites provide you with the ability to restrict who has access to your

information. One practice to increase your account's security is to disable most of the options and then re-open them once you understand what the settings specifically mean to your account. In reality, you probably want different types of content to be displayed to different people, with the most being available to known friends and the least to acquaintances.

What to Do if Your Account Is Hacked

Regardless whether your account is compromised because the social networking site was hacked or just your individual account was infected, you need to take several steps to resolve the issue.

Clean Your Device

The aforementioned hack that compromised Facebook and Google was caused by malware on users machines. In cases like this, use well-known quality malware removal software to scan your machine. The software will contain and/or destroy known and suspicious files. You may even consider reformatting your computer.



Once your machine is clean, the best way to prevent it from becoming infected again is to keep your antivirus software and browsers current. Set them to automatically install updates.

Change Your Passwords

Once an account has been compromised, it is best to presume all your passwords

are compromised. Some security experts advise using a different, strong password for each site.

Get a Password Manager

Since security is dependent on multiple strong passwords, it can become difficult to remember them all -- although there are tricks to make it possible. Consider using a password manager to reduce your vulnerability. You can use the program's password generator to create strong, hard-to-break passwords and you only need to remember one password to access the manager.

Report It

Make sure you report the situation to the social network site. This is especially true if you have been locked out of your account. If this happens, you

may have to prove to the social networking site the account belongs to you, but be persistent and follow through. If you don't, someone could potentially post information as if they are you — which, at the very least, can damage your online reputation. If a crime has been committed, such as banking information stolen, also report the incident to local authorities and appropriate federal law enforcement agencies.

Use Two-Step Verification

If the social media site offers a two-step verification process, use it. The added layer of security makes it much harder for a would-be hacker to access your account. The extra log-in steps will save you time and headaches in the long run.

Staying Safe on Social Media Sites

Each social media site offers tips on how to use their service and still maintain a high level of security. Read their policies, follow their security guidelines and adopt their best practices.

Foursquare: For a better understanding of who can see information associated with your Foursquare account, visit the HelpCenter. This page explains methods for creating security settings for every account scenario. Ensure your check-ins are safe and secure by utilizing these five tips from CIO.

LinkedIn: Visit LinkedIn's Help Center for a wide range of account security articles. A few of the topics covered on the page include methods for protecting your privacy, your identity and your account. They also offer tips for dealing with phishing, spam and malware. If your LinkedIn account is associated with a business, How Not to Have Your Account Hacked provides ways to keep passwords safe even if several people have access to the account.

Pinterest: To keep your Pinterest account secure, you will need to access two main sections on the site: privacy settings and account security. If your account has been hacked or placed in a Safe mode by Pinterest, you will use the account security section to resolve the issue. However, most likely you will only need to use the privacy settings section. This is where you control what others

can view and the degree of personalization desired. Scams are one issue the site has dealt with in the past.

Tumblr: If you use Tumblr, one of the best ways to improve security is to utilize the recently implemented two-factor authentication. For all your settings, though, access the site's security settings page. Here you can learn how to revoke third-party application permissions as well as how to remove spam from your blog. For increased security, according to Entrepreneur magazine, you may want to refrain from using free themes.

Twitter: Visit Twitter's HelpCenter to learn best practices for your Tweets or if you want to know how to connect with or revoke third-party applications. Also visit this page to discover methods for controlling account settings so you can get the level of security you want.

YouTube/Google+: If you have a YouTube and/or Google+ account, bookmark Google's Keeping Your Account Secure page. This page is great source to learn about their two-step verification process, malware and virus issues, general information about your account settings and best practices for protecting your privacy and identity.

One situation people sometimes overlook is what to do if they want to close a social media account. Should the account be deactivated or deleted? According to the Center for Internet Security, you need to take several steps before for your account is deleted from the social media site.

It's All Public Information

Although technically you can post both public and private information on many of the social media sites, due to the onslaught of security breaches in recent years, it is in your best interest to presume anything you post is available for public consumption. Reduce privacy and security risks by only posting information that you would be okay with everyone knowing.

Ex.1. Answer the following questions:

What does the author recommend to do if your account is hacked?

Which of the author's recommendations would you follow to resolve the problem?

What should be done to stay safe on social media site, according to the text?

What would be your solution to the problem?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

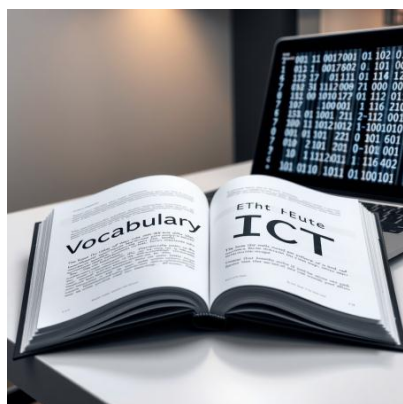
1. People can sometimes be responsible for their own social media account being hacked.
2. You don't need to log out of your account if you're only stepping away for a minute.
3. Closing the browser after using a social media site makes your account more secure.
4. Clicking on suspicious ads is safe because they usually lead to useful websites.
5. If an online offer seems too good to be true, it probably is.
6. It's safe to accept friend requests from strangers on social media.
7. Receiving a friend request from someone you already know on the same site is always safe.
8. Scammers never pretend to be celebrities online.
9. Third-party apps do not have access to your personal information.
10. Posting answers to online games like "What is your pet's name?" can help cybercriminals guess your passwords.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. compromise			
2. expose			
3. close			
4. set			
5. change			
6. click			
7. find			

Text 4



Study this vocabulary:

conduct - проводить

err on the side of caution -

действовать с наименьшим риском

gaming consoles - игровая приставка

hazardous - опасный

illustrate - иллюстрировать; показывать

long term exposure - долговременное воздействие

potential - потенциальный

How Strong is Your Information Security Program?

Traditionally, documented security policies have been viewed as nothing more than a regulatory requirement. While this may have been true in the past, building a strong information security program (ISP) is a business imperative as you fight to keep the customers you have and work to attract new ones. Your

information security policies can either work to help you grow your business or signal a red flag that security is not a top priority.

No matter how strong your security posture is now, if you don't document it, it won't last. You must assume that people instrumental in building your security environment will eventually move on. In that respect, training the replacement is a lot less painful and much more effective with a written guide. Without a policy manual, the new employee



would eventually learn what to do but would you really want to risk a security incident while they are trying to figure it out? It's important to understand that there is no procedure, policy, or technology that will ever be 100% secure. It just doesn't exist. You can, however, endeavor to get as close to perfect as possible.

Lack of a documented security policy is a huge red flag when determining liability in the event of an incident. You do not know when the next attack will happen and if someone is aggressively targeting you, they will cause pain. When time comes to defend yourself, no matter the strength of your security environment, the lack of a documented information security program is a message that management has not taken data security seriously. This perception becomes increasingly dangerous when we're talking about a court of law and an untold number of potential customers in the court of public opinion.

Ex.1. Answer the following questions:

1. What is the purpose of building an information security programme of an organisation?
2. Why do you think the author refers to it as *a business imperative*?
3. Why should your security posture be documented?

4. What is the role of training in maintaining a strong security posture of a company, according to the author?
5. What does a documented security policy imply?
6. What is the lack of a documented information security programme fraught with?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

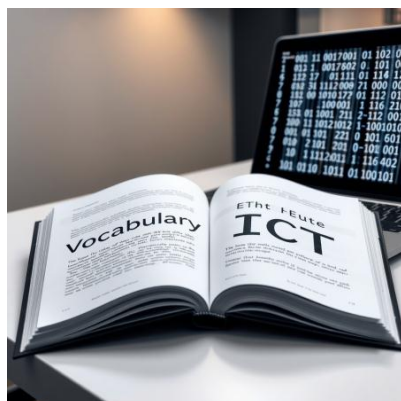
1. In the past, security policies were often seen only as a regulatory requirement.
2. A strong information security program has no impact on customer trust or business growth.
3. Documented security policies are not important if your security system is strong.
4. Security policies help with training new employees about company procedures.
5. An undocumented security policy can be used in court to prove that management took data security seriously.
6. It's possible to create a 100% secure procedure, policy, or technology.
7. If there is no written security policy, a company may face legal consequences after a security incident.
8. You always know exactly when the next cyber attack will happen.
9. Written security policies can act as evidence in a court of law.
10. A good security environment doesn't need documentation because it speaks for itself.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.documetn			
2. assume			
3. train			
4.understand			
5.exist			
6. endeavor			
7. happen			

Text 5



Study this vocabulary:

conduct - проводить

err on the side of caution -

действовать с наименьшим риском

gaming consoles - игровая приставка

hazardous - опасный

illustrate - иллюстрировать; показывать

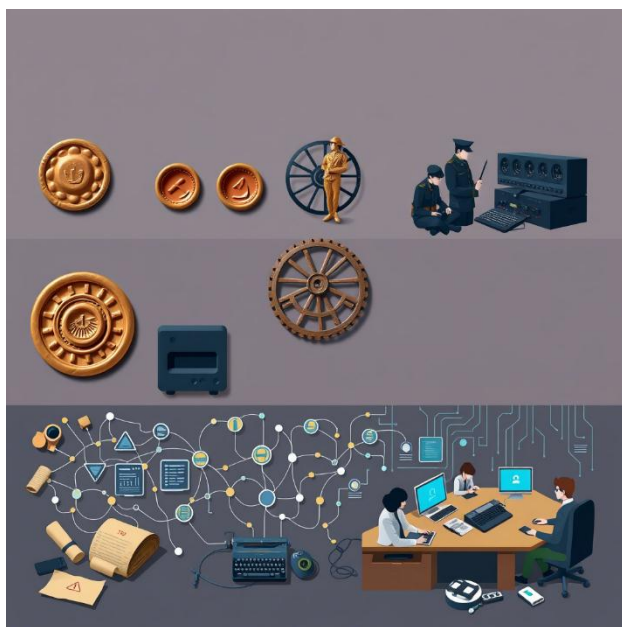
longterm exposure - долговременное воздействие

potential - потенциальный

Read the text: A brief history of Information Security

This article will not attempt to provide a comprehensive history of the field of information security, rather it will suffice to describe the earliest roots and key developments of what is now known as information security. Since the

early days of writing, heads of state and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of written correspondence and to have some means of detecting tampering. The use of wax seals and other sealing devices have been used since the early days of writing to signify the authenticity of documents, prevent tampering and to insure confidentiality of the correspondence. Julius Caesar is credited with the development and use of the Caesar cipher c50 B.C. to prevent his secret messages from being read should a message fall into the wrong hands.



World War II brought about many advancements in information security and may mark the beginning of information security as a professional field. WWII saw advancements in the physical protection of information with barricades and armed guards controlling access into information centers. It also saw the introduction of formalized classification of data

based upon the sensitivity of the information and who could have access to the information. During WWII background checks were also conducted before granting clearance to classified information. WWII also saw the development and use of automatic ciphering machines, the German Enigma machine for example, to encode and decode secret communications. The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user. These computers quickly became interconnected through a

network generically called the Internet or World Wide Web. The rapid growth and wide spread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting these computers and the information they store, process and transmit. The academic disciplines of computer security, information security and information assurance emerged along with numerous professional organizations — all sharing the common goals of insuring the security and reliability of information systems.

Ex.1. Answer the following questions:

1. Why did heads of state and military commanders need to protect written correspondence in ancient times?
2. What method was used in ancient times to prevent tampering and confirm authenticity of documents?
3. Who is credited with developing the Caesar cipher, and why was it used?
4. Which historical event is considered to mark the beginning of information security as a professional field?
5. What are some examples of information security practices developed during WWII?
6. What role did the Enigma machine play in WWII?
7. What major advancements occurred at the end of the 20th and beginning of the 21st century in the field of information security?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. This article gives a comprehensive history of information security.
2. In ancient times, leaders used methods to protect the confidentiality of written messages.
3. Wax seals were used only for decoration and had no role in security.

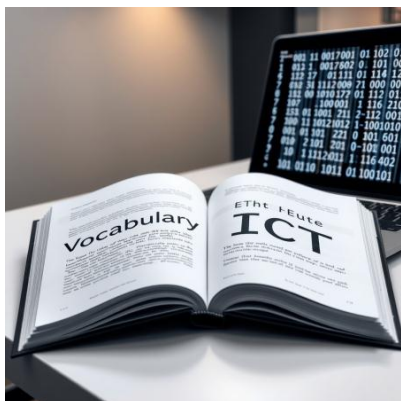
4. Julius Caesar invented the Caesar cipher around 50 B.C. to protect his secret messages.
5. World War II marked the beginning of information security as a professional field.
6. During WWII, physical protection of information included barricades and armed guards.
7. Data classification based on sensitivity began after World War II.
8. Background checks were conducted during WWII before granting access to classified information.
9. The Enigma machine was used by the Allies to decode German messages.
10. Small businesses and home users could not afford computers until the late 20th century.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.describe			
2. signify			
3. fall			
4.bring			
5.mark			
6. see			
7. encode			

Text 6



Study this vocabulary:

conduct - проводить

err on the side of caution - действовать с

наименьшим риском

gaming consoles - игровая приставка

hazardous - опасный

illustrate - иллюстрировать; показывать

long-term exposure - долговременное воздействие

potential - потенциальный

Read the text: Protect

information One of the primary reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. When you consider the millions of electronic messages that traverse the Internet each day, it is easy to see how a well-placed



network sniffer might capture a wealth of information that users would not like to have disclosed to unintended readers. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of cryptography, to prevent intruders from being able to use the information that they capture. Encryption is the process of translating information from its original form (called plaintext) into an encoded, incomprehensible form (called cryptography). Decryption refers to the process of taking ciphertext and translating it back into plaintext. Any type of data may be encrypted, including digitized images and sounds. Cryptography secures information by protecting its

confidentiality. Cryptography can also be used to protect information about the integrity and authenticity of data. For example, checksums are often used to verify the integrity of a block of information. A checksum, which is a number calculated from the contents of a file, can be used to determine if the contents are correct.

An intruder, however, may be able to forge the checksum after modifying the block of information. Unless the checksum is protected, such modification might not be detected. Cryptographic checksums (also called message digests) help prevent undetected modification of information by encrypting the checksum in a way that makes the checksum unique. The authenticity of data can be protected in a similar way. For example, to transmit information to a colleague by E-mail, the sender encrypts the information to protect its confidentiality and then attaches an encrypted digital signature to the message. When the colleague receives the message, he or she checks the origin of the message by using a key to verify the sender's digital signature and decrypts the information using the corresponding decryption key. To protect against the chance of intruders modifying or forging the information in transit, digital signatures are formed by encrypting a combination of a checksum of the information and the author's unique private key. A side effect of such authentication is the concept of nonrepudiation. A person who places their cryptographic digital signature on an electronic document cannot later claim that they did not sign it, since in theory they are the only one who could have created the correct signature. Current laws in several countries, including the United States, restrict cryptographic technology from export or import across national borders. In the era of the Internet, it is particularly important to be aware of all applicable local.

Ex.1. Answer the following questions:

1. Why are intruders often successful in stealing information?
2. What is a network sniffer able to do?
3. What can intruders do with stolen information? (Name at least two things)

4. What is encryption?
5. What is decryption?
6. Can only text be encrypted, or can other types of data also be encrypted?
7. What three aspects of data does cryptography protect?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Intruders are successful because they can easily read and understand the information they steal.
2. Network sniffers cannot capture large amounts of data from the Internet.
3. Encryption translates information into an incomprehensible form to protect it.
4. Only text data can be encrypted.
5. Cryptography only protects the confidentiality of information.
6. Checksums are used to verify the integrity of information.
7. An intruder cannot forge a checksum if it is not protected.
8. Cryptographic checksums help prevent undetected modification of data.
9. Digital signatures do not provide any way to verify the origin of a message.
10. Digital signatures are formed by combining a checksum and the recipient's public key.

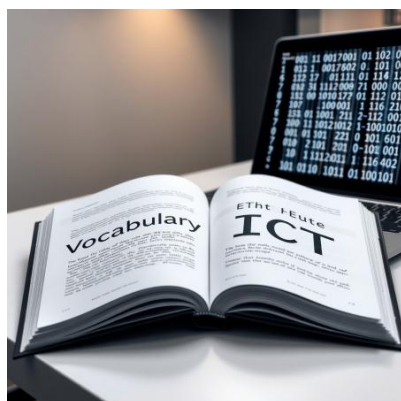
Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.acquire			

2. read			
3. comprehend			
4. traverse			
5. disclose			
6. modify			
7. refer			

Text 7



Study this vocabulary:

unauthorized access –

несанкционированный доступ

misuse – неправильное использование

confidentiality – конфиденциальность

transmission – передача

storage – хранилище

processing – обработка

hardware – аппаратное обеспечение

destruction – разрушение

triangle – треугольник

tangible object – материальный объект

essential – существенный

intentional – преднамеренный

vulnerabilities – уязвимости

gain – выгода, доход

inherent – свойственный

asset – объект, ценный вклад

subordinate – второстепенный

convict – осужденный

Read the text: Network Security: Working and Benefits

Network security is an organization's strategy that enables guaranteeing the security of its assets including all network traffic. It includes both software and hardware technologies. Access to the network is managed by effective network security, which targets a wide range of threats and then arrests them from spreading or entering in the network.

Network security is an integration of multiple layers of defenses in the network and at the network. Policies and controls are implemented by each network security layer. Access to networks is gained by authorized users, whereas, malicious actors are indeed blocked from executing threats and exploits.

Our world has presently been transformed by digitization, resulting in changes in almost all our daily activities. It is essential for all organizations to protect their networks if they aim at delivering the services demanded by employees and customers. This eventually protects the reputation of your organization. With hackers increasing and becoming smarter day by day, the need to utilize network security becomes more and more important.

Types of Network Security

Antivirus and Antimalware Software: This software is used for protecting against malware, which includes spyware, ransomware, Trojans, worms, and viruses.

Malware can also become very dangerous as it can infect a network and remain calm for days or even weeks. This software handles this threat by scanning for malware entry and regularly tracks files afterward in order to detect anomalies, remove malware, and fix damage.



then

Application Security: It is important to have an application security since no app is created perfectly. It is possible for any application to comprise of vulnerabilities, or holes, that are used by attackers to enter your network. Application security thus encompasses the software, hardware, and processes you select for closing those holes.

Behavioral Analytics: In order to detect abnormal network behavior, you will have to know what normal behavior looks like. Behavioral analytics tools are capable of automatically discerning activities that deviate from the norm. Your security team will thus be able to efficiently detect indicators of compromise that pose a potential problem and rapidly remediate threats.

Data Loss Prevention (DLP): Organizations should guarantee that their staff does not send sensitive information outside the network. They should thus use DLP technologies, network security measures, that prevent people from uploading, forwarding, or even printing vital information in an unsafe manner.

Email Security: Email gateways are considered to be the number one threat

vector for a security breach. Attackers use social engineering tactics and personal information in order to build refined phishing campaigns to deceive recipients and then send them to sites serving up malware. An email security application is capable of blocking incoming attacks and controlling outbound messages in order to prevent the loss of sensitive data.

Firewalls: Firewalls place a barrier between your trusted internal network and untrusted outside networks, like the Internet. A set of defined rules are employed to block or allow traffic. A firewall can be software, hardware, or both. The free firewall efficiently manages traffic on your PC, monitors in/out connections, and secures all connections when you are online.

Intrusion Prevention System (IPS): An IPS is a network security capable of scanning network traffic in order to actively block attacks. The IPS Setting interface permits the administrator to configure the rule set updates for Snort. It

is possible to schedule the rule set updates allowing them to automatically run at particular intervals and these updates can be run manually on demand.

Mobile Device Security: Mobile devices and apps are increasingly being targeted by cybercriminals. 90% of IT organizations could very soon support corporate applications on personal mobile devices. There is indeed the necessity for you to control which devices can access your network. It is also necessary to configure their connections in order to keep network traffic private.

Network Segmentation: Software-defined segmentation places network traffic into varied classifications and makes enforcing security policies a lot easier. The classifications are ideally based on endpoint identity, not just IP addresses. Rights can be accessed based on location, role, and more so that the right people get the correct level of access and suspicious devices are thus contained and remediated.

Security Information and Event Management (SIEM): SIEM products bring

together all the information needed by your security staff in order to identify and respond to threats. These products are available in different forms, including virtual and physical appliances and server software.

Virtual Private Network (VPN): A VPN is another type of network security capable of encrypting the connection from an endpoint to a network, mostly over the Internet. A remote-access VPN typically uses IPsec or Secure Sockets Layer in order to authenticate the communication between network and device.

Web Security: A perfect web security solution will help in controlling your staff's web use, denying access to malicious websites, and blocking

Wireless Security: The mobile office movement is presently gaining momentum along with wireless networks and access points. However, wireless networks are not as secure as wired ones and this makes way for hackers to enter. It is thus essential for the wireless security to be strong. It should be noted that without stringent security measures installing a wireless LAN could be like

placing Ethernet ports everywhere. Products specifically designed for protecting a wireless network will have to be used in order to prevent an exploit from taking place.

Endpoint Security: Endpoint Security, also known Endpoint Protection or Network Security, is a methodology used for protecting corporate networks when accessed through remote devices such as laptops or several other wireless devices and mobile devices. For instance, Comodo Advanced Endpoint Protection software presents seven layers of defense that include virus cope, file reputation, auto-sandbox, host intrusion prevention, web URL filtering, firewall, and antivirus software. All this is offered under a single offering in order to protect them from both unknown and known threats.

Network Access Control (NAC): This network security process helps you to control who can access your network. It is essential to recognize each device and user in order to keep out potential attackers. This indeed will help you to enforce your security policies. Noncompliant endpoint devices can be given only limited access or just blocked.

Ex.1. Answer the following questions:

1. What is the author's definition of network security?
2. What kind of technologies does network security involve?
3. How do you understand the meaning of the following statement from the text: *"Network security is an integration of multiple layers of defenses in the network and at the network"*?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Network security includes only software technologies.
2. Network security helps protect an organization's assets and network traffic.
3. Malware can remain undetected on a network for days or weeks.

4. Application security is not important because all apps are created without vulnerabilities.
5. Behavioral analytics tools help detect abnormal network activity.
6. Data Loss Prevention (DLP) allows employees to freely send sensitive data outside the company.
7. Email gateways are considered one of the safest parts of a network.
8. Firewalls can be either software or hardware.
9. An Intrusion Prevention System (IPS) does not actively block attacks.
10. Mobile devices do not require special network security measures.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.guarantee			
2. target			
3. arrest			
4.integrate			
5.block			
6. transform			
7. handle			

Text 8



Study this vocabulary:

unauthorized access – несанкционированный доступ

misuse – неправильное использование

confidentiality – конфиденциальность

transmission – передача
storage –хранилище
processing –обработка
hardware – аппаратное обеспечение
destruction –разрушение
triangle – треугольник
tangibleobject – материальный объект
essential – существенный
intentional– преднамеренный
vulnerabilities – уязвимости
gain – выгода, доход
inherent – свойственный
asset– объект, ценный вклад
subordinate– второстепенный
convict– осужденный

Read the text: What Is Endpoint Security? And Why Is It Crucial Today? Endpoint Security (or) Endpoint Protection refers to the approach of protecting a business network when accessed by remote devices like smartphones, laptops,

tablets or other wireless devices. It includes monitoring status, software, and activities. The endpoint protection software is installed on all network servers and on all endpoint devices.

With the proliferation of mobile devices like laptops, smartphones, tablets, notebooks etc., there has been a sharp increase in the number of devices being lost or stolen as well. These incidents potentially translate as huge loss of sensitive data for enterprises which allow their employees to bring in these mobile devices (enterprise-provided or otherwise) into their enterprise. To solve this problem, enterprises have to secure the enterprise data available on these mobile devices of their employees in such a way that even if the device falls into

the wrong hands, the data should stay protected. This process of securing enterprise endpoints is known as endpoint security.

Apart from this it also helps enterprises successfully prevent any misuse of their data which they've made available on the employee's mobile devices. (Example: a disgruntled employee trying to cause nuisance to the enterprise or someone who may be a friend of the employee trying to misuse the enterprise data available on the device).

Endpoint Security Definition

Endpoint Security is often confused with a number of other network security tools like antivirus, firewall, and even network security. In this page, we list some of the differences between **endpoint security** (or) **endpoint protection** and the network against various evolving security threats of today.

Why Is It Called 'Endpoint' Security?

As you can realize, every device which can connect to a network poses a considerable danger. And as these devices are placed outside of the corporate firewall on the edge of the network using which individuals have to connect to the central network, they are called as endpoints. Meaning endpoints of that network.

As already stated endpoint can be any mobile device ranging from laptops to the notebooks of today, which can be connected to a network. And the strategy you employ in security these endpoints is known as 'endpoint security'.

Endpoint Security Is Not The Same As Antivirus

Although the objective of endpoint security solutions is the same — secure devices — there is a considerable difference between endpoint security and antivirus. Antivirus is about protecting PC(s), — single or many depending upon the type of antivirus being deployed — whereas endpoint security covers the entire picture. It's about securing every aspect of the network.

Endpoint security usually includes 'provisions for application whitelisting, network access control, endpoint detection and response', things

which are usually not available in antivirus packages. It can also be said that antivirus packages are simpler forms of endpoint security.

Endpoint Security Is Different For Consumers and Enterprises

Endpoint security solutions can be broadly classified into 2 different types. One for the consumers and the other for enterprises. The major difference between the two is that there's no centralized management and administration for consumers, whereas, for enterprises, centralized management is necessary. This central administration (or server) streamlines the configuration or installation of endpoint security software on individual endpoint devices and performance logs and other alerts are sent to the central administration server for evaluation and analysis.

What Do These Endpoint Security Solutions Typically Contain? While there's certainly no limit to what endpoint security can contain — and this list is only going to expand in the future — there are some applications which are core to any endpoint security solution. (Because, well, securing a network is altogether a different ball game from securing a computer).

Some of these applications are firewalls, antivirus tools, internet security tools, mobile device management tools, encryption, intrusion detection tools, mobile security solutions etc, to name a few.

Traditional Vs Modern Endpoint Security

This is a no-brainer. Yet something which needs to be pointed out. Because enterprises are often reluctant to changes. Even if it is for their own good. But endpoint security is one area where enterprises have no choice but to adopt the modern endpoint security. Because they are much more than just an **antimalware tool** which can go a long way in securing your network against various evolving security threats of today.

Difference between Endpoint Security and Antivirus

Antivirus is one of the components of endpoint security. Whereas endpoint security is a much broader concept including not just antivirus but many security tools (like Firewall, HIPS system, White Listing tools, Patching and Logging/Monitoring tools etc.,) for safeguarding the various endpoints of the enterprise (and the enterprise itself against these endpoints) and from different types of security threats.

More precisely, endpoints security employs a server/client model for protecting the various endpoints of the enterprise. The server would have a master instance of the security program and the clients (endpoints) would have agents installed within them. These agents would communicate with the server the respective devices' activities like the devices' health, user authentication/authorization etc., and thus keep the endpoints secure.

Whereas antivirus is usually a single program responsible for scanning, detecting and removing viruses, malware, adware, spyware, ransomware and other such malware. Simply put, antivirus is a one-stop shop for securing your home networks, and endpoint security is suitable for securing enterprises, which are larger and much more complex to handle.

Difference between Endpoint Security and Network Security



against various security threats.

Endpoint security is about securing your enterprise endpoints (mobile devices like laptops, smartphones and more) — and, of course, the enterprise against the dangers posed by these endpoints as well — whereas network security is about taking security measures for protecting your entire network (the whole IT infrastructure)

The main difference between endpoint security and network security is that in the case of former, the focus is on securing endpoints, and in the case of latter, the focus is on securing the network. Both types of security are important. Ideally, it's best to start from securing the endpoints and building out. You

wouldn't leave the doors to your home open, just because there's a security guard out there, would you? In the same sense, both are important and should be given equal importance, starting from the endpoints and slowly building out.

In very simple terms, your network would be secure only if your endpoints are secured first. This you should make note of before starting to look for endpoint security and network security products.

Difference between Endpoint Security and Firewall

Firewalls are responsible for filtering the traffic flowing into and going out of your network based on 'a set of security rules'. Like, for example, restricting traffic

flowing into the network from a particular potentially dangerous website. Whereas endpoint security concerns itself not just with network filtering but performs many other tasks like patching, logging, and monitoring etc., for safeguarding the endpoints.

Ex.1. Answer the following questions:

What is an endpoint?

What does endpoint security consist in?

What is it necessary for?

What does the proliferation of mobile devices have to do with endpoint security?

Why do enterprises have to resort to endpoint security?

Is it necessary to identify the difference between endpoint security and endpoint protection? Explain why you think so.

How is endpoint security defined in the text?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Endpoint security protects a business network from threats that come through remote devices like laptops and smartphones.

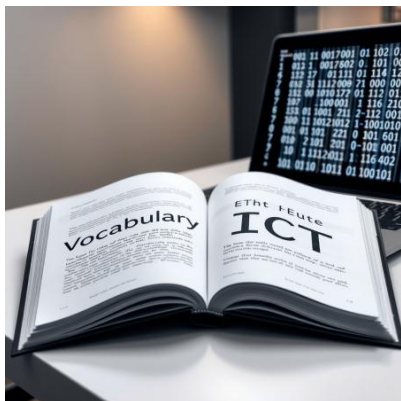
2. Endpoint protection software is only installed on endpoint devices, not on servers.
3. The increase in mobile devices has led to a rise in lost or stolen devices.
4. If a device with enterprise data is stolen, endpoint security ensures that the data remains protected.
5. Endpoint security helps prevent misuse of enterprise data by employees or unauthorized users.
6. Endpoint security is the same thing as antivirus software.
7. Antivirus is a part of endpoint security.
8. Endpoint security focuses only on filtering network traffic like firewalls.
9. Endpoint security is only important for individual consumers, not for enterprises.
10. Enterprise endpoint security requires centralized management.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.adopt			
2. scan			
3. secure			
4.filter			
5.perform			
6. leave			
7. start			

Text 9



Study this vocabulary:

authorized user – авторизованный пользователь

unauthorized access – несанкционированный доступ

accidental disclosure – случайное раскрытие

digital signatures – цифровые подписи

encrypted network communications –

зашифрованные сетевые коммуникации

wireless - беспроводной

CRYPTOGRAPHY

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. 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.

Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage.

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications. Older less secure applications such as telnet and ftp are slowly being replaced with more secure applications such as ssh that use encrypted network communications. Wireless communications can be encrypted using protocols such as WPA/WPA2 or the older (and less secure) WEP. Wired communications (such

as ITU-T G.hn) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as GnuPG or PGP can be used to encrypt data files and Email.

Cryptography can introduce security problems when it is not implemented correctly. Cryptographic solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. Public key infrastructure (PKI) solutions address many of the problems that surround key management.

Ex.1. Answer the questions:

- 1) What does information security use cryptography for?
- 2) How is this process called?
- 3) Who can transform the encrypted information into its original usable form?
- 4) How is this process called?
- 5) What does cryptography protect information from?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Cryptography transforms usable information into an unusable form for unauthorized users.
2. Decryption is the process of transforming encrypted data back into its original form using a cryptographic key.
3. Cryptography is only used to protect information during transmission, not during storage.

4. Cryptography is used for purposes other than encryption and decryption, such as authentication and digital signatures.
5. Telnet and FTP are considered more secure than SSH.
6. Wireless communications cannot be encrypted.
7. Wired communications like ITU T G.hn use AES for encryption.
8. Software applications like GnuPG or PGP can encrypt data files and email.
9. Cryptography never causes security problems if implemented without expert review.
10. The strength and length of an encryption key do not affect the level of security.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.render			
2. disclose			
3. sreplace			
4.encrypt			
5.secure			
6. introduce			
7. implement			

UNIT 7 Malicious computer programs and protection from their effects



Text 1



Study this vocabulary:

an amalgamation [æməˈlɡəˈmeɪʃn] –

объединение, слияние

malicious computer program

[məˈlɪʃəs kəmˈpjʊ:təˈprəʊɡræm] –

вредоносная компьютерная программа

cyberthreats [saɪbəˈθreɪts] – киберугрозы

to be vulnerable [tuː biː vʌln(ə)rəb(ə)l] – быть уязвимым

crippling [ˈkrɪplɪŋ] – нанесение вреда

erase [ɪˈreɪz] – удалить

encrypt [ɪnˈkrɪpt] – зашифровать

sophisticated [səˈfɪstɪkeɪtɪd] – сложный

to infiltrate [tu: 'ɪnfɪltreɪt] –просачиваться, проникать

to propagate [tu: 'prɒpəgeɪt] –распространять

to breach [tu: breɪʃ] –нарушать

to steal [tu:sti:l] –украсть, похитить

execution [eksɪ'kju:ʃn] –осуществление

nuisance [nju:sns] –досаднаяпомеха

harmless ['hɑ:mlɪs] –безвредный, безопасный

to glean [tu: gli:n] –подбирать, собирать

nefarious [nɪ'fe(ə)rɪəs]

consent [kənsent]

duplicious [dʒʊ'plɪsɪtəs]

bot [bɒt] –бот, робот

Read the text: Malware & Computer Virus Facts

Whether you're on a Windows, Apple or Linux computer, a desktop, laptop, smartphone or tablet, you're vulnerable to ever-evolving cyberthreats from computer viruses and other types of malware. The first step to protecting yourself and your data is understanding what you're up against. Here's an overview of the major types of malware, today's most common computer viruses and their potential impact.

The term "malware" — an amalgamation of malicious and software — is now used to describe any malicious computer program on a computer or mobile device. These programs are installed without the consent of users and can cause a number of unpleasant effects, including crippling computer performance, mining your system for personally identifiable information (PII) and sensitive data, erasing or encrypting data or even hijacking device operations or computer-controlled hardware. Hackers continuously develop increasingly sophisticated ways to infiltrate user systems. Let's look at some of the most common types of malware currently in use.

1. Computer Viruses

What is a computer virus? Computer viruses are a type of malware that earned their name because of how they spread by "infecting" other files on a disk or computer. Viruses then spread to other disk drives



and machines when the infected files are received in downloads from websites, email attachments, shared drives or when carried in files on physical media, such as USB drives or—in the early days—floppy disks.

2. Worms

Unlike viruses, worms don't require human help in order to infect, self-replicate or propagate. As soon as they breach a system, they infect their entry point and spread through the device and across any network to which the device connects. By exploiting network vulnerabilities—such as missed operating system (OS) updates or application patches, weak email security or poor internet safety practices—worms can execute, self-replicate and propagate at an almost exponential rate as each new infection repeats the process. Originally, most worms simply "ate" system resources and reduced performance. Now, most worms contain malicious "payloads" designed to steal or delete files upon execution.

3. Adware

One of the most common online nuisances is adware. Adware programs automatically deliver advertisements to host computers. Familiar examples of adware include pop-up ads on webpages and advertising messages that are part of the interface of "free" software. While some adware is relatively harmless, other variants use tracking tools to glean information about your location or browser history. Most of the time, adware collects information in order to serve

better targeted ads. But sometimes Adware is used for more nefarious purposes including redirecting search results, displaying pop-ups that can't be closed or link to malware, disabling antivirus software or even going all the way off the rails into the territory of spyware.

Technically, adware is installed with people's knowledge and consent. But when was the last time you read all the way through a several thousand word "Terms of Service" statement? By clicking the "I Agree" button, you grant consent. Because you have acknowledged and consented to the terms of service, these programs can't be termed malware. Today's antivirus software typically identifies these programs as "potentially unwanted programs" (PUPs).

4. Spyware

Spyware does just what it says. It spies on what you're doing at your computer. It collects data such as keystrokes, browsing habits, location data and even login information. While adware might include "repurposing" collected data for sale in the terms of service statement, spyware is more duplicitous. Spyware is considered malware because users are unaware of it. The only intent of spyware is malicious. Spyware collects and sells your data to third parties, typically cyber criminals, with no regard for how the data will be used. Spyware may also modify specific security settings on your computer or interfere with network connections.

5. Ransomware

Ransomware infects your computer, encrypts your PII and other sensitive data such as personal or work documents and then demands a ransom for their release. If you refuse to pay, the data is deleted. Some ransomware variants lock out all access to your computer. Sometimes, they might claim to be the work of legitimate law enforcement agencies and suggest that you've been caught doing something illegal.

6. Bots

Bots are programs designed to automatically carry out specific operations. Although they serve many legitimate purposes, they are also a popular type of

malware. Once on a computer, bots can cause the machine to execute specific commands without the user's approval or knowledge. Hackers may also try to infect multiple computers with the same bot to create a "botnet"—short for robot network. These zombie botnets give hackers the ability to remotely manage compromised computers, enabling them to steal sensitive data, to spy on user activities, to distribute spam automatically or to launch devastating Distributed-Denial-of-Service (DDoS) attacks on computer networks and websites.

7. Rootkits

Rootkits allow remote access or control of a computer by a third party. These programs are useful for IT professionals trying to troubleshoot network issues remotely, but they can easily become nefarious. Once installed on your computer, rootkits allow attackers to take complete control of your machine to steal data or install additional malware. Rootkits are designed to go unnoticed and actively hide their presence and that of other malware that they install.

8. Trojan Horses

Commonly called "Trojans," these programs hide in plain sight by masquerading as legitimate files or software. Once downloaded and installed, Trojans make changes to a computer and carry out malicious activities, without the knowledge or consent of the victim.

9. Bugs

Bugs—flaws in software code—are not a type of malware, they are errors in software code that popular vectors for attackers with malicious intent. Bugs can, on and of themselves, have detrimental effects on your computer, such as freezing, crashing or reducing performance. Security bugs create holes in a computer or network's defenses that are especially attractive to would-be attackers. While better security control on the developer end helps reduce the number of bugs, bugs are another reason why keeping current on software patches and system updates is crucial.

Ex.1. Answer the questions:

1. What does the term "malware" mean?
2. Why are all users vulnerable to malware regardless of their device?
3. How do computer viruses spread?
4. What is the main difference between a virus and a worm?
5. What are some negative effects that malware can have on your system?
6. What is adware?
7. Why is spyware considered malware, but not all adware is?
8. What happens when ransomware infects your computer?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Malware is short for "malicious software".
2. Malware can only affect Windows computers.
3. Encryption always protects your data from being stolen.
4. A computer virus spreads by itself without any user action.
5. Worms require human action to spread across networks.
6. Adware can sometimes be used for spying or redirecting users to dangerous websites.
7. Users are always aware that they have installed adware.
8. Spyware is considered malware because users are aware of its presence.
9. Ransomware locks your computer or encrypts your files until you pay a fee.
10. Bots are always malicious and never serve legitimate purposes.

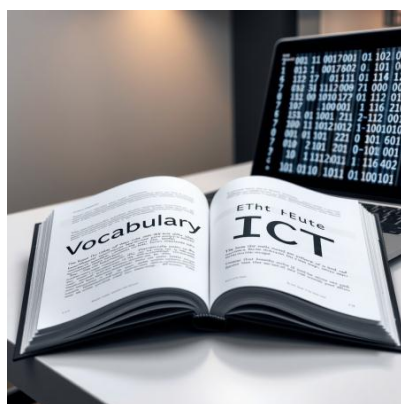
Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.deliver			
2. contain			
3. propagate			
4.breach			
5.infect			
6. spread			
7. cause			

Text 2.

Study this vocabulary:



Concept – концепция

terrorist radicalization – террористическая
радикализация

ethnicity – этническая принадлежность

unlawful acts – незаконные действия

suffrage – избирательное право

Malware protection methods and techniques

Today’s malware is definitely not the only security threat for individual and corporate users, but the tools of detecting and fighting malware remain fundamental in any security solution. There are several reasons for this, the main one being historical. As we already know it all started with viruses, and the first computer security solutions, respectively, were called “antiviruses.” Most people who are not sophisticated in data protection still say “antiviruses”

though, even when speaking about the most complex security solutions. They expect those solutions to fight “viruses,” although, as stated above, they are not the only threats.

There are three main rules which both home and corporate users must follow: Antivirus protection is strongly recommended. If you are not an expert in computer security, you should ensure that you employ proprietary antivirus protection and a firewall. The majority of the current antivirus programs provide protection against all types of computerized threats, including viruses, worms, Trojans and adware, etc. Integrated security solutions are also capable of filtering spam, preventing network attacks and restricting access to unwanted and dangerous Internet resources, etc.

Do not trust any information whose source cannot be guaranteed, whether in email, hyperlink, IM or other format. Do not open files and links from unknown sources. Even unexpected messages from friends or colleagues should be treated with caution as a sender’s address can easily be forged. The Internet can be a dangerous place and you need to remain constantly vigilant.

The risk of infection can also be reduced through what are termed ‘organizational measures’. This usually involves giving each user, whether on a home or corporate network, individual rights regarding what they can see and do whilst using the computer. For example: placing restrictions on the use of IM; restricting access to some websites; nominating only selected machines on the corporate network as being capable of accessing the internet, and so on.



Unfortunately, where a user’s intentions are honorable, such restrictions can sometimes negatively impact the company’s business processes. In this

situation both sides must seek a balance and in each case this balance may be different.

Do not neglect information from antivirus companies and IT security experts. They usually provide an early warning about any new type of Internet fraud, virus threat or epidemic that may be circulating.

The story of the clones of the LoveLetter worm serves to illustrate how fraudulent attacks can be successfully defeated. Immediately after the initial worm epidemic struck, almost every antivirus company issued guidelines for the user on how to protect themselves from this type of worm. In this case, that involved not opening any attachments with a VBS extension as this was how the worm was distributed. As a result of the industry's timely advice, none of the worm's numerous clones were able to wreak the same sort of havoc as that caused by the original LoveLetter worm.

However, sometimes information about the potential for a new virus to do damage is grossly over-exaggerated. Quite often, simple worms hidden inside emails purporting to be about the latest hot topic, for example, a football championship or natural disaster, are presented as the next big thing by some antivirus companies. Subsequently, if there is nothing else around to consume the media's interest, they may well seize upon the story and blow it out of all proportion too.

Ex.1. Answer the questions:

1. What is one of the main security threats mentioned in the text?
2. Why are tools for detecting and fighting malware still considered fundamental in any security solution?
3. What do most people still call modern security solutions?
4. What does a modern antivirus program usually protect against?
5. What is the second rule for protecting against malware?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Malware is the only serious threat to computer security today.
2. Tools for detecting and fighting malware are still considered fundamental in any security solution.
3. The term “antivirus” is used only for programs that protect against viruses.
4. Modern antivirus programs can protect against worms, Trojans and adware.
5. Integrated security solutions cannot filter spam or block dangerous websites.
6. You can safely open email attachments from unknown sources.
7. Even messages from known contacts can be dangerous.
8. Organizational measures involve giving all users full access to everything on the network.
9. Organizational security measures never interfere with business processes.
10. It is important to follow advice from IT security experts and antivirus companies.

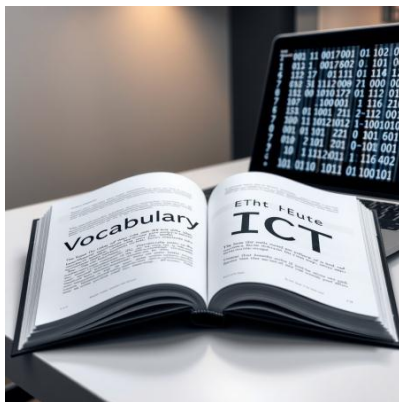
Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. remain			
2. expect			

3. filter			
4. trust			
5. open			
6. forge			
7. stay			

Text 3.



Study this vocabulary:

Non-governmental – неправительственная

hybrid combination – гибридная комбинация

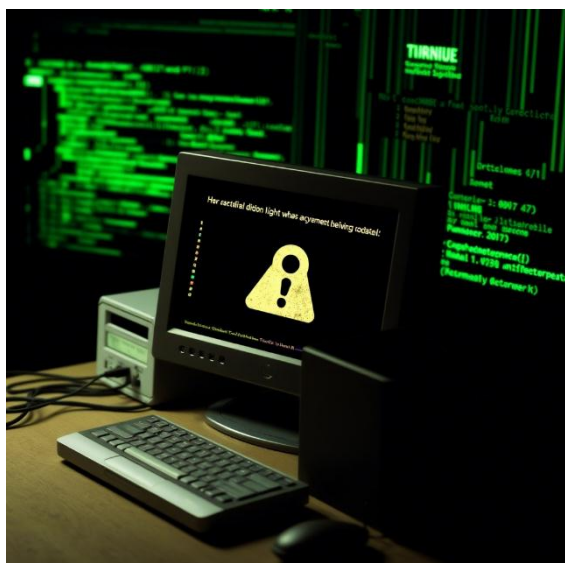
Crown Prosecution Service – королевская прокурорская служба

Directly – непосредственно

quasi-public – квазигосударственный

COMPUTER VIRUSES

Another critical security challenge is presented by computer viruses, hidden programs that can work their way into computer systems and erase or



corrupt data and programs. Viruses are programs that secretly attach themselves to other programs or files, known as the host, and change them or destroy data.

Viruses can be programmed to become active immediately or to remain dormant for a period of time, after which the infections suddenly activate themselves and cause problems.

A virus can reproduce by copying itself onto other programs stored in the same drive. It spreads as users install infected software on their systems or exchange files with others, usually by exchanging email, accessing electronic bulletin boards, trading disks, or downloading programs or data from unknown sources on the Internet. Because so many computers are interconnected, viruses can spread quickly, infecting all the computers linked on a local area network and then spreading over the Internet to other computers and networks. The Melissa virus infected 350,000 computers in the United States and Europe. The Mydoom virus infected a quarter-million computers in a single day in January 2004. The so-called “Love Bug” virus alone caused an estimated \$15 billion in damage. Viruses can do more damage today than ever before and cost organizations billions of dollars each year. Most viruses are created by black-hat hackers and involve outright vandalism or crime.

Each virus is given a name e.g. “Love Bug” or “Melissa” and can be classified as a particular type of virus. The main virus types include: logic bombs that destroy data when triggered boot sector viruses that store themselves in the boot sector of a disk file viruses that attach themselves to COM files (programs that have a COM extension e.g. command.com) macro viruses, often written in the scripting languages for Microsoft programs such as Word or Excel, are spread in Microsoft Office by infecting documents and spreadsheets email viruses which use email messages as a mode of transport and copy themselves by automatically mailing copies to hundreds of people in the victim’s address book companion viruses that instead of modifying an existing file, create a new program which is executed instead of the intended program cross-site scripting viruses that utilize cross-site scripting vulnerabilities to replicate polymorphic viruses that not only replicate themselves by creating multiple files of themselves, but also change their digital signature every time they replicate Two other types of malware – Trojan horses and worms – are often classified as viruses, but are actually forms of distributing malware.

Trojan horses are impostor files that claim to be something desirable but, in fact, are malicious. A Trojan horse appears to do one thing (install a screen saver, or show a picture inside an email for example) when in fact it does something entirely different, and potentially malicious, such as erase files. Trojans can also open backdoors so that computer hackers can gain access to passwords and other personal information stored on a computer. Trojans don't copy themselves or reproduce by infecting other files.

Worms are self-copying programs that have the capacity to move from one computer to another without human help, by exploiting security flaws in computer networks. Worms are self-contained and don't need to be attached to a document or program the way viruses do.

It is note-worthy that different types of malicious software (worms, Trojan horses, adware, spyware, etc.) are generally referred to as viruses though true computer viruses make up only a small subset of malware. For example, "ILOVEYOU" ("Love Bug") or "Melissa" are two examples of worms.

As viruses become more complex, the technology to fight them must increase in sophistication as well. The simplest way to protect against computer viruses is to install one of the many available antivirus software programs, such as Norton Anti-Virus and McAfee Virus Scan. There is no way to entirely stop the spread of computer viruses, because new ones are created all the time. However, a number of excellent "vaccine" programs exist that search for and destroy viruses and prevent new ones from infecting your computer system. These programs continuously monitor systems for viruses and automatically eliminate any they spot. Anti-virus and anti-malware programs can provide real-time protection against the installation of malware on a computer. The software scans disk files at download time, and blocks the activity of components known to represent malware. Users should regularly update antivirus software programs by going online to download the latest virus definitions.

But management must begin to emphasize security at a deeper level: in software design, corporate servers, Web gateways, and Internet service

providers. Because around 80 percent of the world's PCs run on Microsoft operating systems, a single virus can spread quickly among them. Computer users should carefully choose the files they load onto their systems, scan their systems regularly, make sure their antivirus software is up-to-date, and install software only from known sources. They should also be very careful when opening attachments to emails, since this is the way many viruses are spread.

Ex.1. Answer the questions:

1. What is a computer virus? How does a computer virus work?
2. What are the ways viruses spread? Why can viruses spread so quickly?
3. Name some of the famous viruses used to spread worldwide.
4. Enumerate the main types of true viruses. Which of the virus types given in the text do you think to be the most dangerous and why?
5. Describe a malicious program called "a Trojan horse".

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Computer viruses are hidden programs that can erase or corrupt data and programs.
2. A virus cannot attach itself to other programs or files.
3. All viruses activate immediately after infection.
4. Viruses spread only through physical media like disks and not over the Internet.
5. The Melissa virus infected 350,000 computers in the United States and Europe.
6. The Love Bug virus caused \$15 billion in damage.
7. Most viruses are created by ordinary users without malicious intent.
8. Worms need a host program to spread.
9. Trojan horses reproduce and spread automatically.

10. Macro viruses are often written in scripting languages like those used in Microsoft Word or Excel.

Ex. 4. Write down ten word-combinations with a verb.

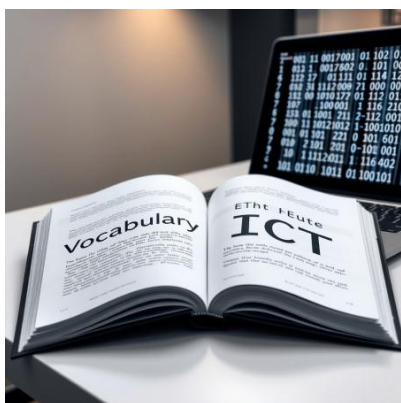
Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.work			
2. attach			
3. destroy			
4.spread			
5.download			
6. infect			
7. cost			

UNIT 8. Classification of crimes. Computer crimes.



Text 1



Study this vocabulary:

crowdsource - привлекать, получать,
использовать ресурсы/данные/советы,
полученные от внешней группы бескорыстных
исполнителей, обычно через интернет
disseminate - распространять; рассылать

exclude - исключить

penetrate - проникать

inappropriate - некорректный; несоответствующий

upstart - неожиданно получивший известность; новомодный

subversive - губительный

thriving - процветающий

unfettered - свободный; неограниченный

unambiguously - недвусмысленно; однозначно; чётко

phishing - "выуживание паролей" - новый вид банковского мошенничества путем отправления "спам" сообщений для получения секретных данных о личных счетах

Read the text “HACKING, DANGER, CRIME”

With the growth of newer, more open ways for people to post, crowdsource, and disseminate information has come a rise in the ability of people to cross digital boundaries, both for good and for harm. Nations, organizations, and all



kinds of entities have digital as well as physical borders—systems intended to provide technological access to those who belong to the group and to exclude those who do not. From the macro (large scale) to the micro (small scale) to the meso (in between) levels of society, it is increasingly a challenge to maintain these boundaries, keep outsiders from intruding, and otherwise prevent the often quite serious problems that can arise in a more open system.

Outsiders can attempt to penetrate a computerized system by hacking into it. *Hacking* is the manipulation of the programming codes that tell computers exactly what to do and is also often the term used to describe the manipulation or inappropriate release of the information that is obtained in this way. Hacking can be done both legally and illegally, and for positive and negative purposes. The term also sometimes refers to creative, upstart, usually independent and somewhat subversive forms of computer programming, content creation, and information dissemination. Hacking in this sense is a thriving culture that actively encourages creative approaches to programming and other digital innovation and the unfettered sharing of that which is produced and accessed.

Some of these approaches are outside the boundaries of current laws, some are within them and clearly noncriminal, and some exist at the borderline and require a society to consider how open it wants its information to be.

Certainly, when digital spaces are hacked into and information is rerouted or repurposed (or destroyed or made unintelligible, as by a computer virus), breaches of security, even terrorism, can occur. These are unambiguously crimes and can occur on the smallest and largest of scales. In the increasingly common crime of *phishing*, usernames and passwords are stolen when individuals are tricked into providing them to thieves impersonating legitimate entities. This information can then be used for a number of destructive purposes, including theft of funds and identities. Large information systems can also be destroyed or disabled by intrusions and viruses introduced by hackers. Monetary systems, power grids, websites, personal information, and basically anything that is gathered, organized, and stored via computer can be affected when digital security is compromised. This is called *computer crime* or *cybercrime*.

Ex.1. Answer the following questions:

1. What is hacking?
2. Give the definition of “phishing”.
3. What two purposes does hacking have?
4. Give the examples of illegal hacking.
5. What is cybercrime?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Hacking always involves illegal activity and is never used for good purposes.
2. Digital systems are designed to allow unrestricted access to everyone.
3. Hacking can include creative and innovative computer programming.
4. Maintaining digital boundaries is becoming easier due to more open systems.

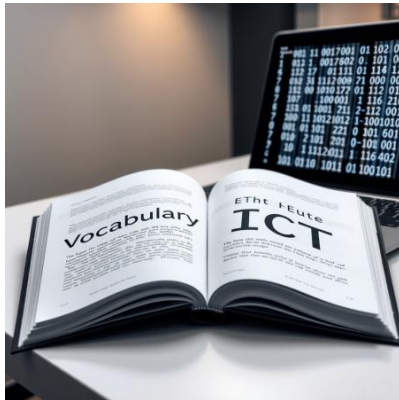
5. Hackers can steal usernames and passwords through phishing attacks.
6. Phishing is a harmless form of hacking that does not lead to serious consequences.
7. Computer viruses cannot cause security breaches or damage large information systems.
8. Cybercrime only affects personal computers and not larger systems like power grids or monetary systems.
9. The word 'hacking' is only used to describe criminal actions.
10. Some forms of hacking exist at the borderline of legality and require society to consider how open information should be.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. keep			
2. maintain			
3. disseminate			
4. crowdsource			
5. attempt			
6. penetrate			
7. encourage			

Text 2



Study this vocabulary:

Viruses – вирус

Antivirus protection – антивирусная защита

Worms – черви

Adware – рекламное ПО

network attacks – сетевая атака

source – источник

The first challenge to tackling VERLT successfully lies in the elusiveness of the concept. The possible motivations, ideas and other factors that might drive an individual towards VERLT are various and complex, and no single factor is necessary or sufficient to account for terrorist radicalization. There is no single profile of individuals who have become involved with terrorism, and presumptions based on past or current individual cases are, therefore, extremely limited in their applicability. Broad profiles built on stereotypical assumptions based on religion, “race”, ethnicity, sex, or socio-economic status are not only discriminatory, but also ineffective.

Radicalization is not a threat to society if it is not connected to violence or other unlawful acts, such as incitement to hatred, as legally defined in compliance with international human rights law. Radicalization can actually be a force for beneficial change. For instance, the political and human rights advocates who were instrumental in the abolition of slavery, and those who championed universal suffrage were at one time considered to be radical, as they stood in opposition to the prevailing views in their societies.

Terrorist radicalization is a process whereby an individual comes to accept terrorist violence as a possible, perhaps even legitimate, course of action. This may eventually, but not necessarily, lead this person to advocate, act in support of, or engage in terrorism. There is, however, no clear-cut pathway towards terrorism. Terrorist radicalization may occur in a great variety of circumstances in different ways and at different speeds. Each case of terrorist

radicalization and recruitment for terrorism results from the unique intersection of an enabling environment with the personal circumstances and psychology of a given man or woman.

Terrorist radicalization and recruitment does not occur in a vacuum. It should be viewed as an interactive process between the individual and external influences, including terrorist propagandists and recruiters, broader developments in society, and the actions of public authorities. The terms “self-directed” or “self-initiated” radicalization are often used when there is a minimal degree of interaction with people actively seeking to radicalize and recruit an individual. Terrorist radicalization facilitated by the Internet has become of particular and growing concern to countries throughout the OSCE area and beyond. It is associated with the phenomenon of so-called lone terrorists or self-starters, who seemingly act on their own without any clear outside direction or support.

Terrorist radicalization is a dynamic process: it may be accelerated, possibly slowed down and in some cases reversed. Therefore, in order to be able to prevent and counter VERLT, it is important to understand the nature and impact of different factors and the degree to which they might vary and interact in different cases. In this regard, it is useful to distinguish between push and pull factors.²² Certain factors, such as a charismatic recruiter, might have traction, pulling the individual down a path of violent radicalization. Other factors, such as experiencing violence, including at the hands of agents of the state, might make an individual more vulnerable to the appeal of terrorism, pushing him or her towards violent radicalization.

Conditions Conducive to Terrorism

While there is no consistent set of factors driving terrorist radicalization, some have been identified as being particularly pertinent. Conditions conducive to terrorism recognized at the level of the UN and the OSCE include “prolonged unresolved conflicts, dehumanization of victims of terrorism in all its forms and manifestations, lack of rule of law, violations of human rights, ethnic, national

and religious discrimination, political exclusion, socio-economic marginalization and lack of good governance”.

While there are numerous structural conditions of a socio-economic and political nature that can possibly push individuals towards terrorism, such as discrimination and other forms of human rights violations (including those resulting from counterterrorism measures), relative deprivation, or a lack of access to education, these are in and of themselves not sufficient to account for terrorist radicalization.²⁴ It is important to take into account other factors of a psychological, interpersonal and ideological nature to explain mobilization. Such factors can help explain why one particular individual might follow a path of terrorist radicalization, while another from a comparable situation and background does not.

Psychological and cognitive factors, such as one’s self-image, a sense of identity and belonging, expectations, beliefs and attitudes, are dynamic and shape how a person experiences and reacts to his or her environment and events. They can have an impact on the development of negative feelings of displacement, of “being odd”, for instance, feelings of exclusion, rejection, relative deprivation, humiliation, victimization, injustice, frustration, revolt or superiority. This can push someone to be more susceptible to the appeal of terrorism. Youth have often proven more vulnerable to VERLT: as they grapple with questions of identity and their place in the world and their future, they are more inclined to take risks and to challenge the status quo. Psychological susceptibility can also be suddenly and dramatically increased as a result of trauma caused by a triggering event that acutely affects a person.

The spread of, and exposure to, ideas and narratives that legitimize terrorism and foster its appeal are critical pull factors. Many terrorists and violent extremists skilfully tailor, package and disseminate their narratives in a way that will reach and resonate with the particular individual or group targeted for radicalization and recruitment. There are a number of different approaches that

can be used to provide legitimacy and enhance the appeal of terrorism, including:

Using the logic that the ends justify the means, arguing that violence is a necessity in the pursuit of an imperative social, ideological, political or other goal, and that there is no alternative;

Dehumanizing intended victims on the basis of intolerance, hate and denial of universal human dignity;

Presenting terrorism as something exciting, counter-cultural or anti-establishment; and



Building on the charisma and/or perceived legitimacy of terrorists and, in particular, their leaders.

Social interactions, group dynamics and interpersonal relationships play a primary role as pull factors, except in instances of self-directed or self-initiated radicalization. People are drawn into VERLT through personal acquaintances – peers, relatives – or they are sought out by terrorist recruiters. Terrorist recruiters identify, prey on and groom vulnerable men and women, gain a hold on them by providing material and/or psychological support, and abuse their trust to manipulate them or indoctrinate them into becoming involved with terrorism.

For the fight against terrorism to be effective and sustainable, it should be conducted at all times in accordance with the rule of law and international human rights standards. The state's response to the threat of VERLT should be evidence-based and proportionate to avoid losing the trust and support of the public, as well as to avoid victimization and other forms of unintended validation of terrorist narratives. Moreover, it cannot be limited to repressive actions focused on pursuing terrorists, denying them material capabilities and

thwarting their plans. The traditional counterterrorism work of law enforcement and intelligence agencies needs to be supplemented with prevention efforts to address conditions that are conducive to the spread of terrorism, disrupt terrorist radicalization and stem recruitment.

OSCE participating States have recognized the need to address “the various social, economic, political and other factors, including violent separatism and extremism, that engender conditions in which terrorist organizations are able to recruit and win support”. Many of them have developed specific policies and put significant efforts into this.

Countering VERLT requires both effective criminal-justice action against those who incite others to terrorism and seek to recruit others for terrorism, and comprehensive, multi-disciplinary efforts to address conditions that are conducive to terrorism.

Preventing terrorism should be based on a legislative framework that provides for the appropriate criminalization of preparatory offences. Definitions of such offences in national legislation, similar to defining acts of terrorism, should be clear, precise, non-discriminatory, non-retroactive and accessible to the public. The Council of Europe Convention on the Prevention of Terrorism has been identified as an international good practice. It defines the criminal offences of “public provocation to commit a terrorist offence”, “recruitment for terrorism” and “training for terrorism”.

UN Security Council resolution 1373 obliges states to suppress terrorist recruitment, and resolution 1624 (2005) calls on states to prohibit, by law, incitement to commit terrorist acts. To comply with international standards, the criminalization of incitement to terrorism must be accompanied by adequate safeguards in line with the principle of legality, and should uphold fundamental rights, including the freedom of expression. In particular, the offence of incitement to commit a terrorist act will be human rights-compliant if it focuses on *direct* incitement, with an intention to promote terrorism, and if it establishes

an evidence-based causal link between the incitement and the likely realization of a terrorist act.

Simply holding views or beliefs that are considered radical or extreme, as well as their peaceful expression, should not be considered crimes. “Radicalization” and “extremism” should not be an object for law enforcement counterterrorism measures if they are not associated with violence, or with another unlawful act (e.g., incitement to hatred), as legally defined in compliance with international human rights law. Extremist individuals or groups who do not resort to, incite or condone criminal activity and/or violence should not be targeted by the criminal-justice system.

The investigation and prosecution of terrorism-related criminal cases, including of incitement to, and recruitment for, terrorism, should be based on specific evidence, guarantee due process and fair trials, as well as comply with the absolute prohibition of torture or other cruel, inhuman or degrading treatment or punishment, the right to life and the right to liberty and security.

However, the nature of terrorism as a serious crime is such that the police or other competent state agencies may need to resort to special investigation techniques (SITs), such as the use of undercover agents, surveillance and interception of communications. SITs can involve severe interference with human rights, in particular fair-trial and privacy rights. Therefore, the use of such techniques should be:

Limited to serious cases and proportionate to the gravity of the matter under investigation; and Based on laws that establish and clearly define mechanisms for prior authorization, supervision, ex post facto review and accountability to effectively uphold human rights, in particular the right to a fair trial, and the rule of law.

Ex.1. Answer the following questions:

1. What is the main challenge in tackling VERLT?

2. Why can't we rely on profiles to identify people who might become involved in terrorism?
3. When is radicalization considered a threat to society?
4. Give an example of how radicalization can be positive.
5. What is terrorist radicalization?
6. Is terrorist radicalization predictable?
7. What is "self-initiated" radicalization?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

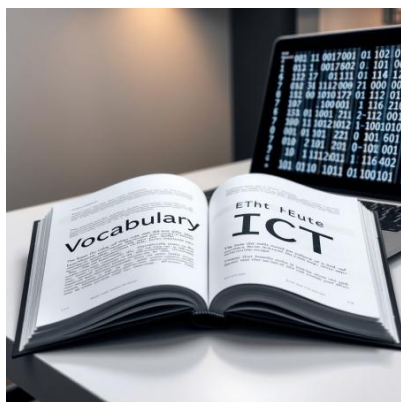
1. There is a single, clear profile that can be used to identify people who might become involved in terrorism.
2. Radicalization is always dangerous and harmful to society.
3. Some forms of radicalization have led to positive changes in history.
4. Terrorist radicalization always follows a clear and predictable path.
5. Terrorist radicalization can occur without direct interaction with recruiters.
6. Push factors are things that attract someone to terrorism, like charisma of a leader.
7. Pull factors include things like discrimination or personal trauma.
8. Socio-economic conditions alone are enough to explain why people turn to terrorism.
9. Psychological factors can help explain why one person becomes radicalized and another does not.
10. Young people are often more susceptible to radicalization because they are searching for identity and purpose.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.lie			
2. tackle			
3. drive			
4.apply			
5.stand			
6.oppose			
7. pull			

Text 3



reliance on information technology - уверенность в информационных технологиях;

penetrate defence - пробить защиту

non-combatant targets - мирное население (цели)

create worldwide havoc - производить ужасные разрушения

coerce a government - оказать давление на

государство

Non-governmental, non-police organizations

Non-governmental, non-police organizations are a hybrid combination of public and private arrangements that contribute directly to the order-maintenance assemblage by acting as gatekeepers to the other levels of governance, but also contributing towards (cyber) crime prevention. The

Internet Watch Foundation, for example, provides governance under the auspices of a mandate from the UK ISPs, Police, Crown Prosecution Service and Government. One of its principle functions is to bring to the attention of ISPs any illegal materials reported to its hotline, particularly child pornography, the eradication of which is one of the objectives of the Foundation. If deemed actionable following a judgment made against set criteria by a trained operative, the IWF takes appropriate action either by informing the offender's Internet services provider, alerting comparable hotlines in the offender's jurisdictions, else, serious enough and within the UK it may pass on details of a WWW site directly to the police. The IWF also contributes more generally towards cybercrime prevention and public awareness. It was formed in December 1996 with the endorsement of the Metropolitan Police, Department of Trade and Industry (DTI), Home Office and the associations of the ISPs, such as the Internet Service Providers Association and the London Internet Exchange. The standing of the Internet Watch Foundation has increased and it has become the quasi-public face of Internet regulation in the UK, more notably since it re-launch in 2000.

Another example of a non-governmental, non-police organization is the (US) Computer Emergency Response Team (CERT) based at Carnegie Mellon University in Pittsburgh since its establishment in 1988. It was created in the aftermath of a devastating attack by the Morris Worm which illustrated the Internet's vulnerability by bringing much of it down. Located at the Software Engineering Institute, a federally funded research and development centre of Carnegie Mellon University, the purpose of CERT was to combat unauthorized access to the Internet. Its programmers would log reported hacks and carry out the initial investigations. Where security breaches were found to be too complicated to deal with in-house, they were farmed out to an unofficial brain trust' (Adams 1996) and to the relevant public police organizations when an offence was serious and could lead to prosecution. In 2003 CERT joined the Arlington based US-CERT team created by the Department of Homeland

Security as part of the national infrastructure protection programme. Prior to the partnership, CERT (Carnegie Mellon) had become the model for many similar computer security organizations throughout the world. CERT was based within a non-governmental public institution, yet, initially funded by a combination of private and governmental resources.

Although the non-governmental, non-police organizations are mainly private bodies, they often perform public functions and a growing concern is that they, as such, lack the formal structures of accountability normally associated with public organizations. Governmental non-police organizations provide governance under the auspices of regulations, rules and law through charges (levies), fines and the threat of prosecution. Not normally perceived as police, they are nevertheless actively involved in investigating, resolving and even prosecuting cybercrime. They include agencies such as Customs, the Postal Service, and Trading Standards organizations etc. These agencies may employ a range of hi-tech software solutions to protect themselves and also assist them when in conducting investigations.

They also include a higher tier of agencies that set cyber security policy and also oversee the implementation and enforcement of national Internet infrastructure protection policies. Some governments, such as Singapore, China, Korea, Vietnam and Pakistan (in 2010), have at one time or another, and with varying degrees of success, explicitly sought to control their citizen's use of the Internet through such agencies. They have either required users to register with governmental monitoring organisations, or they have sought to directly control Internet traffic in their jurisdictions through government-controlled ISPs (Center for Democracy and Technology, 1996; Caden and Lucas, 1996; BBC 2010). The majority of nations tend to take a more liberal (or pragmatic) approach towards cyber security. Consequently, at the national level in many of the more liberal jurisdictions there exist various higher tier governmental multi-sector cross-sector organizations, agencies or forums with a remit to protect the electronic

infrastructure either through active interventions or through the co-ordination of the activities of bodies at an international level. Such arrangements can be complex as the UK example illustrates.



Multi-sector co-ordination is at the heart of the UK Cyber Security Strategy (Cabinet Office, 2009a), which is part of the UK National Security Strategy set by the Cabinet Office (Cabinet Office, 2009b). To help implement and administer the Cyber Security Strategy are two new agencies. The Office of Cyber Security (OCS) in the Cabinet Office provides overall strategic leadership and coherence across government. Because cyber security also impacts upon the Critical National Infrastructure the Office of Cyber Security works with the Centre for the Protection of National Infrastructure (formed in 2007 out of NISCC, the National Infrastructure Security Co-ordination Centre and NSAC the National Security Advice Centre - a part of the UK security service). CPNI is an interdepartmental organization which draws upon participants from industry, academia and various government departments and agencies to protect national security by reducing the vulnerability of the national infrastructure to terrorism and other threats, including electronic attack.

In support of the Office of Cyber Security is the Cyber Security Operations Centre (CSOC), based at GCHQ in Cheltenham, which has a more tactical remit. CSOC will try to understand the nature of attacks, provide advice, monitor the health of cyberspace and co-ordinate responses to such incidents. A major part of CSOC's remit is to identify national cybercrime threats. Within the Cyber Security Strategy lies the Home Office Cyber Crime Strategy, published in March 2010 to outline the government's approach towards cybercrime (Home Office, 2010a). It is the latest part of a complex jigsaw of national security policy that has gradually been introduced since 2008 to increase the

cohesiveness of the UK's National Security Strategy (see further Wall, 2010). Most EU member countries have similar infrastructure protection and cyber security strategies and agencies with similar functions to OCS and CPNI. There are also emerging a number of EU wide agencies, such as ENISA (European Network and Information Security Agency) whose role it is to support the internal market by facilitating and promoting increased co-operation and information exchange on issues of network and information security.'

The UK experience in multi-sector coordination is similar in principle to that of the US. The US Department of Homeland Security (DHS) was created in the aftermath of September 11, 2001. The DHS brought together 22 previously disparate domestic agencies into one department to protect the nation against threats to the US homeland. Amongst the agencies the DHS incorporated under Information Analysis and Infrastructure Protection (IAIP), was the National Infrastructure Protection Center (NIPC) which since 1998, articulated the National Infrastructure Protection Plan of which the Internet was part. The NIPC brought —together representatives from U.S. government agencies, state and local governments, and the private sector in a partnership to protect our nation's critical infrastructures (NIPC 1998). In 2009 it became the National Infrastructure Coordinating Center (NICC) to serve as the Office of Infrastructure Protection's focal point for coordination and information sharing with the 18 national critical infrastructure and key resources sectors during normal operations and during incident management activities'. Under NICC coordination umbrella are many US state-funded non-police organizations that are also involved in policing the Internet to resolve specific problems. For example, the United States Postal Service has a responsibility for the cross-border trading of pornography and the US Securities and Exchange Commission a responsibility for dealing with fraud.

There is a final level of very important and influential governmental non-police organizations which set regulatory policy (often secondary legislation). They are the departments of government that are responsible for trade, and

therefore tend to carry the e-commerce portfolios: in the UK this is BIS (Department of Business, Innovation and Skills, formerly BERR and DTI); in the US it is the FTC, (Federal Trade Commission).

Ex.1. Answer the questions:

Are non-governmental, non-police organizations a hybrid combination of public and private arrangements?

Do they contribute directly to the order-maintenance and towards (cyber) crime prevention?

Was the (US) Computer Emergency Response Team (CERT) created in the aftermath of a devastating attack by the Morris Worm?

Are non-governmental organizations actively involved in investigating, resolving and even prosecuting cybercrime?

What national cybercrime threats can be identified nowadays?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Non-governmental, non-police organizations contribute to order-maintenance and cybercrime prevention.
2. The Internet Watch Foundation (IWF) works only with UK internet users.
3. One of the main functions of IWF is identifying and reporting child pornography online.
4. The Internet Watch Foundation was formed in 1998.
5. CERT was created after the attack of the Morris Worm in 1988.
6. CERT is part of the US police force.
7. CERT only works independently and does not collaborate with other agencies.
8. In some countries, such as China and Singapore, governments do not control citizens' use of the Internet.

9. Non-governmental, non-police organizations are always fully accountable like public institutions.

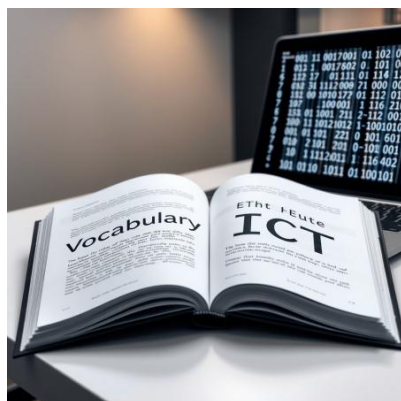
10. CERT joined US-CERT in 2003 under the Department of Homeland Security.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. contribute			
2. bring			
3. report			
4. identify			
5. deem			
6. increase			
7. launch			

Text 4



fastest-growing - быстро растущий

computer hacking - хакерство

stalking - шпионаж

bogus companies - фиктивная компания, фирма-однодневка

rumour - слухи, сплетни

COMPUTER CRIME

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.

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. 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?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Information systems are becoming more important as business assets.
2. Computer crime is the only threat to information systems.
3. Computers allow people to share information easily, but also increase the risk of unauthorized access.
4. Crackers are the same as white hat hackers.
5. Unauthorized users can access computer systems only if they have passwords.
6. The number of reported Internet security violations has decreased in recent years.
7. In 1990, over 82,000 incidents were reported to CERT.
8. Phishing involves pretending to be a real organization in order to steal banking details.
9. Piracy refers to the legal copying of digital content.
10. All companies are completely safe from computer crime if they don't connect to the Internet.

Ex. 4. Write down ten word-combinations with a verb.

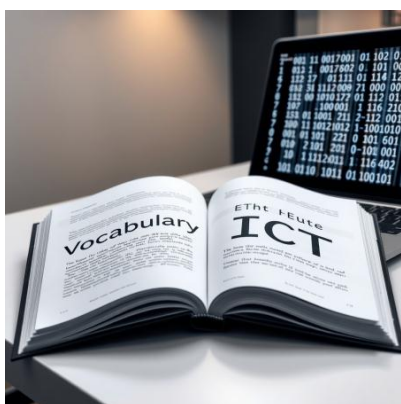
Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.share			
2. affect			
3. connect			
4.become			
5.steal			
6.invent			
7. modify			

UNIT 9.Cybercrime.Cyberterrorism and extremism: definition, types



Text 1



bogus companies - фиктивная компания, фирма-однодневка

computer hacking - хакерство

fastest-growing - быстро растущий

rumour - слухи, сплетни

stalking - шпионаж

Russian Cybercrime: A Profile and Comparison

As an increasing number of human activities take place in the digital sphere, criminal activity utilizing technological means is also beginning to flourish. After the end of the Cold War, tensions remained between the Russian Federation and the former Soviet republics on the one hand, and Western Europe and the United States on the other. Although many of the sentiments and conflicts from that period remain, now the arenas for these conflicts have shifted

from missile silos and propaganda programs to cybercrime and cyber-terrorism. Cybercrime rapidly became the most popular way for individuals and governments to target their enemies for economic and political reasons. The rise of cybercrime is not a secret to anyone; and governments around the world now recognize the magnitude of cyber threats, pouring resources into defending themselves from organizations such as WikiLeaks and the hacker group Anonymous.

This paper aims to prove that the United States is falling behind the Russian Federation and other Russian speaking countries in the struggle for cyber-dominance, and that one of the primary reasons for this lapse is the United States' smothering of entrepreneurship and innovation in young programmers through law enforcement and legislation. The paper will reveal the particular gaps and weaknesses of the United States, which have been exploited by hackers and criminals from across the globe. These hackers live in countries where they are not only allowed to experiment and perfect their hacking skills but, in fact are often encouraged by their respective governments to do so. For example, the government of the Russian Federation actively recruits educated programmers from universities as well as self-educated successful hackers to deal with domestic issues, such as the organization of protests and anti-government meetings, as well as international matters of intelligence and even espionage. Through an analysis of Russian and American views on the issue of cybercrime, the longstanding traditions that influence these views, as well as each government's public and private response to the domestic presence of skilled cybercriminals, I will show that the unbounded success of Russian-speaking hackers on the global scale and their innovative ability to consistently defeat their opposition is a product of the hackers' national culture and the freedoms that they are granted. Before discussing the impact of modern cybercrime and the differences between its Russian and American variants, it is important to understand the nature of cybercrime itself. Cybercrime can be defined as "criminal activities conducted in cyberspace by means of Internet technology"

and can be divided into two categories: “1) those involving unauthorized access to data and systems for criminal purposes, and 2) those involving fraud, falsification, diversion of funds, obtaining illicit content, or defamation via online services. Furthermore, it should be noted that, although cybercrime can be labeled as one of the newest waves in organized crime and does possess some entirely novel intricacies, “cybercrime is not an altogether new breed of crime... the crimes carried out by this new breed of criminal often reflect emotions as old as humankind.” Cybercrime is a relatively new and rapidly changing phenomenon, and for this reason it is defined somewhat differently in different countries. In spite of specialized definitions, however, the general idea of cybercrime remains relatively consistent. A. Shchetilov identifies three types of cybercrime in Russia: “illegal access to information stored in global computer networks; crimes using information in forms other than those that are computer-based; and crimes involving the distribution of harmful computer programs.” In China, Sun Tianzhy and Cao Peizhong define cybercrime as “those crimes that use computers as the main tool, as well as those that have computer assets as their primary target.”

In sum, cybercrime consists of either stealing information over the Internet or disrupting the use of a certain website or online service. While the public is quite familiar with certain types of infringements, such as “spam,” in the context of email, general public knowledge of cybercrime is relatively low.

In turn, knowledge and

familiarity with how cybercrime is committed is even more rare. The five most common tools and methods utilized in cybercrime are keylogging, distributed



denial of service (DDoS), pharming, phishing, and botnets. Keylogging is defined as “using software or devices to secretly monitor and record keystrokes, enabling espionage activities or the harvesting of personal data,” and it was among the first methods to be widely used by cybercriminals.”

Keylogging records each key pressed on a keyboard in sequence, allowing the owner of the keylogger to record every character typed, regardless of whether or not the character is displayed on the screen. Keylogging is also one of the most varied forms of cybercriminal activity. It includes programs that simply record all keystrokes in a text document, as well as more innovative devices, such as acoustic keyloggers, which record the sound of fingers typing on a keyboard and then, through analysis of these sounds, determine which key was pressed and in what order. Without any explicit application, the potential for keylogging is essentially endless, enabling anything from identity or password theft to government agency remote access. However, most applications of keylogging occur on a personal level, and Vanessa Vitaline “identifies keylogging as a general threat.”

Keyloggers, much like Torrent clients, remain prominent because they are circulated by legitimate and malicious sources alike. According to the security website BullGuard.com, one of the reasons keyloggers continue to grow in sophistication is because some companies actually promote keyloggers “for benign purposes like allowing parents to monitor their children's whereabouts on the Internet.” Like peer-to-peer downloading services, which are not innately illegal, keyloggers illustrate how a perfectly legal technology may be utilized for illegal purposes. The second type of cybercrime is a distributed denial of service (DDoS) attack, or “inundating computer system resources with tasks sufficient to render them unavailable to authorized users.”

DDoS attacks basically simulate or create enough traffic to a particular computer or network resource that it then becomes unavailable to legitimate users. In most cases, a DDoS attack simply aims to make a website or service inaccessible. DDoS attacks are one of the most potent and popular modern

methods of cybercrime. They are used heavily by the hacker group Anonymous, for example, which was involved in a DDoS of the website of the International Federation of the Phonographic Industry (IFPI) in 2009.

Ex.1. Answer the questions:

1. Did cybercrime rapidly become the most popular way for individuals and governments to target their enemies for economic and political reasons?
2. Why are cybercrimes defined somewhat differently in different countries?
3. How do you understand the nature of cybercrime?
4. What are the five most common tools and methods utilized in cybercrime?
5. What types of programs does keylogging include?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Cybercrime is becoming more common as more human activities move into the digital sphere.
2. After the Cold War, cybercrime replaced traditional geopolitical conflicts between Russia and the West.
3. The United States leads in cyber-dominance compared to the Russian Federation.
4. One reason the U.S. lags in cybersecurity is because it promotes innovation too much.
5. Russian-speaking hackers are often encouraged by their governments to develop hacking skills.
6. The Russian government recruits only uneducated hackers from the streets.
7. Cybercrime is a completely new type of crime with no roots in traditional criminal behavior.
8. Cybercrime can be defined as criminal activity conducted in cyberspace using Internet technology.

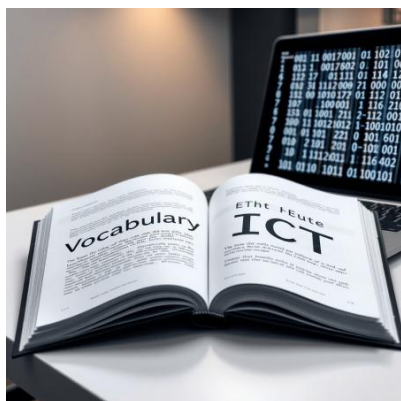
9. There are three categories of cybercrime according to A. Shchetilov.
10. In China, cybercrime includes both using computers as tools and targeting them as assets.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. remain			
2. shift			
3. pour			
4. smother			
5. exploit			
6. recruit			
7. show			

Text 2



Study this vocabulary:

to prescribe punishment – назначить наказание

to pass a new law – принять новый закон

to identify a suspect – установить личность подозреваемого

an unauthorized access – несанкционированный доступ

a breach of rules – нарушение правил

The Rise of Cybercrime



Due to the enormous potential of rendering a website or online service completely inaccessible, Vitaliy Vekhov confirms “the rapid growth, over the past 10 years, of DDoS crimes.” DDoS crimes have become increasingly powerful as more and more financial institutions and civil services rely on the Internet and computer systems, which can then be targeted by criminal means such as a DDoS attack and rendered useless. Additional cybercrime methods include pharming—“directing traffic from a legitimate Web site to a site controlled by a criminal hacker” and thus allowing the potential theft of personal information or the promotion of a certain ideal or information—and phishing—“illegally accessing an individual’s financial data to capture online banking and financial information” most often by way of email or instant messaging. Phishing and pharming as well as keylogging techniques represent a more passive movement in cybercrime as they seek to either steal information or control what an Internet user views. DDoS attacks, on the other hand, have the potential to lead to physical harm and property damage when the scope is widened to the control of power grids or Air Traffic Control Towers. The newest and perhaps most powerful tools at cybercriminals’ disposal are botnets —“networks of infected machines, usually managed by a single command center, that are capable of

causing serious damage to networked systems and enabling large-scale identity theft.” Botnet consists of a collection of computers that have been compromised, most often by a piece of malware, and then used as “bots” to carry out other tasks. Botnets have many different applications, but they are most often used to conduct very large DDoS attacks, using each “bot” as simulated traffic. They allow the originator of the attack to not only utilize the power of their machine, but of every machine they are able to convert into a “bot.”

Botnets and other cybercrime methods illustrate that “cybercrimes, uniquely different from traditional crimes, are often harder to detect and prosecute” and, thus, present a unique challenge to modern nations and individuals attempting to maintain tight security. Chen Junjing “concludes that these [cyber] crimes are more widespread than traditional crimes and are increasing at a faster rate... Furthermore, cybercrime does greater damage to society than traditional crime and is more difficult to investigate.” Cybercrime mirrors a broader societal trend in which governments, corporations, and individuals rely more and more on technology. With the increase in cybercrime, governments and law enforcement agencies around the world must adapt to meet its evolving demands. This process, however, is slow and onerous because cybercrime presents a series of unique challenges that are not present in traditional crime. First, cybercrime can be perpetrated both locally and remotely, the latter constituting “the majority of computer crimes” according to A. I. Zhurba, a Ukrainian researcher of cybercrime. N. N. Akhtyrskaya further states that “the process of investigating these [cyber] crimes is typically fragmentary, complex, and fraught with false leads.” In addition to being difficult to investigate, the scope of damage a particular act of cybercrime can range from hindering “the judiciary, . . . radio, and television broadcasters; and medical care providers” to “the sabotage of critical infrastructure, such as the supply of electricity or water,” according to a 2008 report by the Swedish Emergency Management Agency. Governments, therefore, need to pay particular attention to the trends of cybercrime, such as the “rapid growth of phishing since 2000”

discussed by Rodion Nasakin, and address the fact that “perpetrators of cybercrime are often more sophisticated in their methods than are the law enforcement agencies that investigate them.”

Vanessa Vitaline, writing about cybercrime in France, “concludes that, despite countermeasures taken by governments and police authorities, cybercrime continues to grow exponentially.” Vladimir Golubev and Timofey Saymarly at the Center for Research on Problems of Computer Crime in Ukraine provide an additional warning that “western countries currently have inadequate personnel trained to combat this type of [remote cybercrime] attack, a lack that they must remedy.” Remote attacks constitute the majority of all cybercrime and “are more dangerous than direct attacks, because [they] may have catastrophic global consequences.”

Cybercrime is a relevant and pertinent issue for law enforcement around the world. Understanding the main methods and tools behind these crimes is important, but in order to accurately describe the nuance of international cybercrime, it is also necessary to discuss the differences between approaches to cybercrime in the United States and in Russia, as well as the effect of these approaches on national security and competitiveness.

In order to understand how cybercrime originating in Russia and other former Soviet countries relates to the United States, one must first determine the character of such cybercrime. In 2010 the entirety of global cybercrime garnered revenues of seven billion U.S. dollars, according to a presentation done by Group-IB. Out of that 7 billion, 1.3 billion dollars (approximately 19%) originated in Russia and 2.5 billion dollars (approximately 36%) came from Russian-speaking countries. In their report, members of Group-IB present the costs of various services including the



“guaranteed hack of a mailbox (Yandex, Mail, Rambler, Gmail)” starting at 1500 rubles (approximately \$50 USD) as well as a “mobile phone bug” starting at around \$5000. What makes such a wide array of services, illegal services, so readily available and affordable from Russian sources? Danny Lieberman, in an article published on the website Infosec Island, describes how “Russia has outstanding universities with world class specialists in mathematics, physics, and computer science... Russia, very simply, has very, very good raw material for hacking” and goes on to cite the entry on Wikipedia.com dedicated to Russian mathematicians. Lieberman adds, “having great talent is a great start for getting world-class results in any field.” Yevgeny Kaspersky, co-founder of the Kaspersky Lab, which specializes in computer and Internet security, describes “Russia as a nation of ‘super hackers.’”

Kaspersky attributes Russian hacking prowess to “Russia’s technical education,” provided by certain universities around the country that specialize in teaching hacking—including the Institute of Cryptography, Telecommunications and Computer Science, which was co-sponsored by the Russian Ministry of Defense and the KGB, and a college in the Siberian city of Tomsk, where one in every five residents is a student. However, such a large talent pool does not necessarily encourage its members to participate in cybercrime. Accordingly to a publication by the Center for Strategic and International Studies, after the Federal Agency for Government Communications and Information (FAPSI) disbanded in 2003, “many of the employees were recruited by hacker groups, while others joined the Russian security service successor of the KGB, the FSB.”

To offer some insight into why young, educated, programmers would seek criminal work instead of legitimate occupations, Mark Galeotti, director of the Organized Russian and Eurasian Crime Research Unit at Keele University, states that “for a lot of the Russian techies [crime] became very lucrative,” and criminal organizations “began to recruit top graduates from universities who

could earn ten times what they would get in Russia and twice what they would get in the West.”

With an ever-increasing number of young professionals graduating from professional schools with aspirations to work in the field of technology, one writer for TheAge.com.au draws a parallel between the creators of organizations such as the Russian Business Network (RBN) and the “young entrepreneurs from similar backgrounds [who] launched Google and eBay.” In the struggle to find employment, large numbers of educated and skilled programmers in Russia end up working independently as hackers or cybercriminals, or for companies and organizations such as the Russian Business Network (RBN). The RBN is a Russian cybercrime syndicate that Wikipedia describes as “a multi-faceted cybercrime organization, specializing in and in some cases monopolizing personal identity theft for resale.”

Utilizing tactics similar to those of the traditional mafia, the Russian Business Network does not always maintain a concrete identity. The Economist wrote in 2007: “in one sense, RBN (Russian Business Network) does not exist. It has no legal identity; it is not registered as a company.” Furthermore, much like the secretive crime syndicates of the past, “its senior figures are anonymous, known only by their nicknames... [I]ts web sites are registered at anonymous addresses with dummy e-mails.” So what, then, is the RBN? VeriSign, a prominent Internet security firm, identifies the network as “a for-hire service” that “caters to large-scale criminal operations,” offering a range of services such as spamming, phishing, and bot-herding.

The RBN occasionally works on a very large scale. For example, in 2006 it conducted one operation known as “Rock Phish,” which earned an estimated \$150 million. VeriSign sets the organization apart from other, less reputable websites and Internet organizations by emphasizing that the “RBN is solely criminal,” even naming it “the baddest of the bad.” After hacking an RBN computer, VeriSign operatives discovered that “every major Trojan in the last year links to RBN,” accounting for 30,000 entries of stolen data. The

organization's secrecy is as extensive as the scope of its operations—the number of employees can only be estimated, and only the most extremely powerful or vocal members of the group can be individually identified. “Flyman,” for example, is the alias of the head of the RBN, whose uncle is believed to be a senior politician in Saint Petersburg. As with studies of other, more traditional criminal enterprises, the funding and support of cybercriminal organizations warrants scholarly attention. How and why do organizations such as the RBN flourish in Russia? In an interview with BBC reporter Sarah Rainsford, a former Russian hacker known only as “Andrei,” who started hacking at the age of 14, describes hacking as an intellectual exercise: “it’s like when you have a maths problem... you don’t know what tools to use, you know nothing. But you want to master it, understand it, and then use that knowledge in the future.”

Ex.1. Answer the questions:

What do cybercrime methods pharming and phishing include?

What does Botnet consist of?

How does Botnet work?

Do you agree that cybercrime does greater damage to society than traditional crime and is more difficult to investigate?

What a series of unique challenges not presented in traditional crime does cybercrime have?

What kind of organizations is the Russian Business Network (RBN)?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. DDoS attacks can make websites completely inaccessible.
2. DDoS attacks are only used against small businesses and not financial institutions.

3. Pharming redirects users from real websites to fake ones controlled by hackers.
4. Phishing usually happens through email or instant messaging.
5. Phishing and pharming are considered active forms of cybercrime.
6. DDoS attacks cannot cause physical damage.
7. Botnets are networks of infected computers that can be used for cybercriminal activities.
8. Botnets are easy to detect and shut down.
9. According to Chen Junjing, cybercrime is less widespread than traditional crime.
10. Cybercrime causes less damage to society than traditional crime.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.rely			
2. target			
3. steal			
4.seek			
5.earn			
6. address			
7. join			

Text 3

Botnet consists of a collection of computers that have been compromised, most often by a piece of malware, and then used as “bots” to carry out other tasks. Botnets have many different applications, but they are most often used to conduct very large DDoS attacks, using each “bot” as simulated traffic. They allow the originator of the attack to not only utilize the power of their machine, but of every machine they are able to reach. Although Andrei voices the opinion of many young computer programmers around the world, for some reason such hackers have become powerful and active in Russia and other Russian-speaking countries, but not in the United States. One student in Tomsk, Alexei, refers to hacking as “an art” and another, Zheniya, explains how requests for him to use his hacking knowledge quickly escalated from friends and relatives wanting to spy on neighbors, to “people who wanted me to infect a large number of users who were clients of a certain bank, so they could use their computers to transfer money.”

These reports from Russian hackers indicate that Russia provides an environment that encourages aspiring programmers to “join the ranks of Russia’s hackers for hire,” as Rainsford puts it. Young Russian hackers such as Zheniya and Alexei represent the cream of the crop of the hacking world, “consistently finish[ing] among the top three teams in international information protection contests.” Members of organizations such as the Russian Business Network reside at the top of the cyber food chain. The Economist notes that, “despite the attention it is receiving from Western law enforcement agencies, RBN is not on the run. Its users are becoming more sophisticated.”

The majority of legal pressure on these hackers comes from the law enforcement agencies of Western countries, and even these efforts fail to halt or mitigate the illegal activities of the RBN. Not only are organizations like RBN not intimidated by Western law enforcement, they even retaliate against such efforts. In October 2006, when the National Bank of Australia moved against

RBN's "Rock Phish," "RBN-based cybercriminals replied by crashing the bank's home-page for three days."

Although the RBN may appear to be behind the majority of cybercrime, Dancho Danchev stresses: "the RBN is the tip of the iceberg... What about the hundreds of thousands other not so well known malware serving netblocks?" As a large number of powerful and educated Russian hackers continue to find employment in hacking and committing cybercrimes, one question inevitably arises: what effect, if any, has this phenomenon had on the United States? Is the United States prepared to deal with these syndicates? Perhaps American programmers are already working clandestinely for the US government, have less potential, or simply do not exist, but in any case, it is important to note that the majority of well-known hackers and cybercriminals are not American. The founders of the website The Pirate Bay, who have been involved in numerous lawsuits around the world, are Swedish and Finnish. The Pirate Bay is one of the most used torrent resources on the Internet and is actually planning "to launch airborne drones that act as proxy servers" in order to make it more difficult for law enforcement to shut down their website.

The founder of the website Megaupload, Kim Dotcom, who was brought under charges for copyright infringement in January of 2012, is of German-Finnish origin. Perhaps the most well-known hacking group in the United States, Anonymous, maintains its members' anonymity, and Julian Assange, the founder of WikiLeaks, is Australian. The media typically portrays the United States as vulnerable to European and Australian cybercriminals, but the United States actually lags behind much of the world in cyber-capabilities. Delvin Barrett, writing for the Wall Street Journal, explains that "federal law-enforcement officials say they are concerned about cyber-retaliation" from Anonymous. What more encouraging message could a cybercriminal receive? What, then, accounts for the disparity between the capabilities of Russian and American hackers? Perhaps the single most important factor affecting an American hacker's ability to work, experiment, and grow is the controversial

and suffocating anti-piracy legislation in the United States. Both legitimate and criminal organizations expressed outrage at the Stop Online Piracy Act (SOPA) from the United States House of Representatives and the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP) from the Senate. In protest, groups such as Anonymous launched cyber-attacks and organizations Google and Wikipedia encouraged a “deluge of phone calls and emails that hammered offices.” The presence of this legislation actively hindered the freedom of hackers to develop their skills. Shawn Henry, the FBI’s top cyber investigator, describes the American model of smothering hacking potential as “unsustainable” and, when referring to America’s ability to protect its own assets from computer hackers, adds: “We’re not winning.”

One of the primary causes of this ineptitude is a failure to recognize and therefore completely understand the character and mentality of cybercriminals. For example, in order to find a definition of the term “fire sale,” one must now search the comments on private websites for its unofficial definition. Wikipedia indicates that the article “Fire sale (attack)” was marked for deletion, because, according to a Wikipedia editor, there is not enough evidence on fire sales to be



“worth a separate article.” In response to the deletion, a user answered, “Do a search, and you will find the term used.” The editor responded, “I did that. Pretty much everything I found was either a blog (not a reliable source) or a reference to the movie.”

While looking for accredited opinions on medical treatments or statistical information, a privately owned and run blog may not be the best source. However, when discussing a culture that lives on blogs, chat clients, and forums, labeling a blog as “not a reliable source” is counterproductive. At a time when Wikipedia, the younger generation’s go-to source for information, is deleting

content because it is primarily discussed in blogs, readers whose interest is national security must be cautious and understand the importance of blogs in cybercriminal circles. In contrast, Russian hackers do not face such restrictive legislation and are not compelled to act in secret. On the contrary, “some activist groups are not supervised by the secret services, but rather by the presidential administration.”

According to a report published by Group-IB, “the dollar-value of online criminal activity conducted by the Russian mafia and other criminal organizations doubled in 2011.” Not only are Russian-speaking criminals already ahead of law enforcement and their counterparts in the West, but they are continuing to flourish, partially as a result of the lack of adequate Russian legislation: “The Group-IB report blamed lax Russian laws for the expansion of cybercrime.”

Group-IB officials go on to say that, “while the Russian government has tried to tighten legislation aimed at preventing and punishing such activity, the company said more was needed.” They also suggest that “the Kremlin either controls the hackers or, more plausibly, turns a blind eye so long as they stop in to help when the government calls.”

Cybercrime is a powerful and malicious reality of the modern world, and it is manifested in such procedures as DoS attacks, phishing, and botnet herding. Russia stands out as a safe haven for a large, capable, and active hacking community. It is home to many talented and well-educated young professionals who may lack opportunities for legitimate employment, but are allowed to practice cybercrime freely. Russia lacks legislation that prohibits or discourages hacking and, in some cases, the government even supports and finances hackers’ education and employment. Furthermore, the United States’ competitiveness in hacking is hindered by their devotion of resources to the enforcement of legislation aimed at limiting Internet and hacking entrepreneurship, which discourages talented individuals from developing their valuable skills. By focusing its resources on hackers’ education rather than on strict control of the

Internet, Russia has progressed much further and faster than the United States in the increasingly important arenas of hacking and computer programming. According to a report by the Federal Research Division of the Library of Congress, the United States faces “a dilemma in balancing the need to gain access to personal data—both to prevent and to prosecute cybercrimes—with the need to protect the individual privacy and civil liberties.”

Because Russian Federation has yet to show that they are ready to legislatively protect civil liberties or prosecute cybercrimes, the United States and other Western powers face increasing numbers of capable Russian hackers. However, it would not be completely accurate to paint such a bleak picture of the United States’ cyber security or exaggerate the ineptitudes of the U.S. government. It should be noted that “police officers from the UK, Germany, Netherlands, Australia, and other countries work alongside the FBI at the NCFTA [National Cyber-Forensics & Training Alliance].”

In addition to international collaborations, companies based in the United States, either independently or through third parties, have begun to combat cybercriminals. “Once a company detects a network breach, rather than expel the intruder immediately, it can waste the hacker’s time and resources... Companies can also allow intruders to make off with bogus files or ‘beacons’ that reveal information about the thieves’ own machines.”

While both law enforcement in the United States and private entities are dedicating time and resources to combating cybercrime, these defensive maneuvers, which companies are forced to use in order to stay in business, are “sometimes outside the law.” Western authorities also deserve credit for the extradition of Julian Assange and the arrest of Kim Dotcom—two large steps in combatting criminal enterprises on the Internet. The presence of “officials from the Department of Defense, the Department of Homeland Security and the National Security Agency” at the hacking conference DefCon in late 2011 and the “Meet the Feds” event they hosted are also steps in the right direction.

Western authorities must remain vigilant in their efforts to protect their citizens and infrastructure, but they must also recognize the shortcomings in their stifling approach to cybercrime. They must adapt to meet the nature of modern cyber criminals and hackers and dedicate resources to catch up to and surpass China and Russia in global cyber-dominance. In order to remain competitive in the rapidly developing world of cybercrime, the United States will need to find a workable balance between protecting civil liberties, privacy, and intellectual property rights on the one hand, and allowing talented hacking students to flourish as they do in Russia.

Ex.1. Answer the questions:

Where does the majority of legal pressure on RBN's hackers come from?

The majority of well-known hackers and cybercriminals are not American, aren't they?

Do organizations like RBN even retaliate against efforts of Western law enforcement to halt or mitigate their illegal activities? What did they do?

Did the Group-IB report blame lax Russian laws for the expansion of cybercrime?" What about American law?

Will any country need to find a workable balance between protecting civil liberties, privacy, and intellectual property rights In order to remain competitive in the rapidly developing world of cybercrime?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Botnets are networks of computers compromised by malware and used as "bots" to carry out cyber attacks.
2. Botnets are most often used for small-scale cyber activities like sending spam.
3. Russian hackers are less skilled than their American counterparts.
4. The Russian Business Network (RBN) is not a major player in cybercrime.

5. Western law enforcement has successfully stopped RBN's criminal activities.
6. In 2006, RBN-based hackers crashed the National Bank of Australia's homepage for three days.
7. Dancho Danchev says that the RBN represents the entire scope of global cybercrime.
8. Most famous hackers and cybercriminals are from the United States.
9. Kim Dotcom, founder of Megaupload, was brought under U.S. charges in 2012.
10. Anonymous is a Russian hacker group.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.blame			
2. publish			
3. finish			
4.compel			
5.act			
6. face			
7. store			



Text 4

random – выбранный наугад

insecurity – отсутствие безопасности

in the vicinity of – поблизости

foremost – на первом месте

constitute – составлять

by virtue of – в силу

assailant – субъект нападения

abduction – похищение

POLICING CYBERCRIMES



The Internet and the criminal behaviour it transforms (cybercrime) pose considerable challenges for order maintenance and law enforcement because Internet-related offending takes place within a global context while crime tends to be nationally defined. Policing cyber-crime is made all the more complex by the very nature of policing and

security being networked and nodal and also because within this framework the public police play only a small part in the policing of the Internet. In this paper it is argued that the future of the public police role in policing the Internet is more than simply acquiring new knowledge and capacity, but it is about forging new relationships with the other nodes within the networks of Internet security. These relationships require a range of transformations to take place in order to enhance the effectiveness and legitimacy of the nodal architecture. It will then be argued that some of the contradictions faced by ‘the police’ are being reconciled by the gradual reconstitution of a neo-Peelian paradigm across a global span, which brings with it a range of instrumental and normative challenges. The relationship between the public police and technology dates back to their origins in the early nineteenth century. Traditionally a responsive organization designed to counter the dangers produced by urban migration caused by eighteenth-century industrial technology, the police had, by the

second half of the nineteenth century, situated themselves as an all-purpose emergency service. It is a heritage that gave them consensual public support and a high degree of local police force independence. As a consequence, it has left ingrained within the organisational and occupational cultures of the police the instinct to protect the public and claim ownership over policing. Although the police and their constitutional position has changed considerably since their formation, many of the original Peelian police principles survive, though adapted to modernity: a bureaucratically organised responsive local police that maintains order and enforces law; officers who are identifiable from the rest of the public, professional in conduct, accountable to law and the community for their actions. However, the increasing pervasiveness of the Internet, along with its global, transformative impacts create a range of entirely new demands upon the public police which question their traditional local dominance over the security domain and could in fact marginalize them completely. Not only does the concept of cybercrime produce problems for the police because Internet-related offending takes place within a global context whereas crime tends to be nationally defined, but policing the Internet is also a complex affair by the very nature of policing and security being networked and nodal (Johnson & Shearing, 2003). While the application of concepts of networked and nodal security may be disputed in the terrestrial world' (Crawford & Lister, 2004, p. 426), nowhere is it more networked and nodal than in cyberspace. This paper explores how the public police are situated in the networks of security that contribute to the policing of harmful behaviour in cyberspace. The first part will question our understanding of cybercrime to identify the tensions arising between the globalisation of harmful behaviour and specific jurisdictional definitions of crime. The second part will probe the networked and nodal architecture of Internet policing to locate, and then situate, the role of the police. It will be argued that the future of the public police role in policing the Internet is more than simply acquiring new knowledge and capacity. For the police to have a role in the policing of cyberspace, they will need to forge new relationships with the

other nodes that constitute the networks of Internet security. These relationships will require a range of transformations to take place in order to enhance the effectiveness and legitimacy of the nodal architecture. The third part of this paper will identify the challenges that face the police if they are to maintain their role in networked policing. Finally, the fourth part will look at those responses to argue that some of the contradictions faced by the police‘ have been reconciled by the reconstitution of a neo-Peelian paradigm across a global span. Whilst this may (re)situate the police it nevertheless requires a range of fresh instrumental and normative responses.

Ex.1. Answer the questions:

1. Do the Internet and the criminal behavior it transforms (cybercrime) pose considerable challenges for order maintenance and law enforcement?
2. Which of the original Peelian police principles survive?
3. Do the increasing pervasiveness of the Internet, along with its global, transformative impacts create a range of entirely new demands upon the public police?
4. Is policing the Internet also a complex affair by the very nature?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

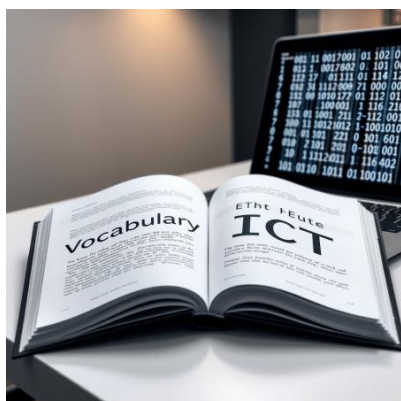
1. The Internet and cybercrime present considerable challenges for law enforcement due to their global nature.
2. Public police play the main role in policing the Internet.
3. Policing cybercrime is simple because traditional national laws can easily apply online.
4. The future of public police in cyberspace involves building new relationships with other security actors.

5. The neo-Peelian paradigm has no relevance in modern global policing of the Internet.
6. Police forces were originally created to deal with cyber threats.
7. Traditional policing principles still influence modern police culture today.
8. The Internet has not changed the way police must approach security.
9. Cybercrime can be policed using the same methods as traditional crime.
10. The paper argues that the public police need to change how they operate in order to remain effective in cyberspace.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. forge			
2. police			
3. change			
4. give			
5. survive			
6. question			
7. probe			



Text 5

to destabilize societies – дестабилизировать общество

to assassinate - покушаться

to access – получить доступ

explosives – взрывчатые вещества

cyber space – кибер пространство

adversaries – противник, враг

adherents – приверженец, последователь

Cybercrime as the Focus of Policing Cyberspace

Although a topical and newsworthy subject, little is known about cybercrime ‘other than from press and television reportage. Upon reflection, the term cyberspace crime ‘would have been more meaningful because it more clearly the space in which the harmful behaviour takes place. However, because the term is principally a media construct it has subsequently obtained its own linguistic agency and it has entered the public parlance and we are stuck with it. Cyber-terrorism, information warfare, phishing (an email purporting to be from a legitimate bank, requesting confirmation of personal details), spams, denial of service attacks, hacktivism, hate crime, identity thefts, online gambling, plus the criminal exploitation of a new generation of pornographic peccadilloes, it is alleged, conspire to threaten public safety and temper governmental and commercial ambitions for the growth of an information society. Although there is a fairly widespread consensus that cybercrimes exist. There is much confusion as to what they actually are and what risks they pose.

To add to the confusion over what constitutes a cybercrime is the frequent practice of media, practitioner and some academic commentators to refer to just about any offence involving a computer as a cybercrime’. This practice tends to be accompanied by the tendency to mix, sometimes deliberately so, the debates relating to personal internet security with those relating to corporate or national security. Making matters even worse is the discussion of online offending and deviant behaviours in global terms when in fact their definitions and solutions might be found locally. All this has shaped public understanding about cybercrimes and has, arguably, led to a difference between the level of

cybercrimes experienced by individuals (which is quite low) and the level of cybercrimes they feel exist (which is quite high). This disparity given rise to a reassurance gap between public demands for policing cybercrime and the level of service that the police can realistically provide. It is therefore important to look first at what is being understood as cybercrime because it contributes to setting the policing agenda. Furthermore, without reliable sources of knowledge, misinformation cannot be countered, misunderstandings are perpetuated and there is no firm platform to establish a responsive criminal justice policy.

Since cybercrimes are the product of networked computers, they must be defined in terms of the informational, networked, and globalised transformation of deviant or criminal behaviour by networked technologies. These transformations give Internet users a global reach, new capacities for distributed peer to peer networking and a panoptic gaze that creates an asymmetric ability to enable one person to simultaneously reach many. These characteristics also contribute to the reorganisation of the division of criminal labour, on the one hand automating and deskilling it, while on the other hand reskilling‘ and empowering the single agent‘ who can single-handedly control a complete and complex criminal activity. The implications of this are profound because the overall set-up and running costs are low and because so few individuals are involved in each incidence of offending, intelligence about the perpetrator is unlikely to leak out.

If Internet transformations are the key to understanding cybercrime, then in order to understand their impact it is necessary to consider what happens if the Internet is removed from the equation. By applying a simple transformation test ‘ three different groups of cyber-criminal opportunity can be identified as points on a spectrum. At the near end lie behaviours which are commonly referred to as cybercrimes, but are in fact first generation traditional‘ crimes in which computers have been used for information gathering or communication to assist with the organisation of a crime. Remove the computer and the criminal behaviour persists because the offenders will revert to using other information

sources or types of communication. Towards the middle of the spectrum lie the second generation hybrid‘ cybercrimes. These are traditional‘ crimes for which entirely new global opportunities have emerged (e.g., globalised frauds and deceptions, also the global trade in pornographic materials including child pornography). Take away the Internet and the behaviour will continue by other means, but not by the same volume or across such a wide span. At the far end of the spectrum, however, are the third generation true‘ cybercrimes which are solely the product of opportunities created by the Internet and which can only be perpetrated within cyberspace (online intellectual property thefts, spams). These are the spawn of the Internet and therefore embody all of its transformative characteristics. Spamming is a good example of a true cybercrime. It is an illegal behaviour in its own right in the laws of the USA, EU, and many other jurisdictions, but it also facilitates secondary offending by enabling engagement with potential victims. Many of the offences that result are small-impact bulk victimization de minimis offences. Take away the Internet and spamming and true cybercrimes vanish. These distinctions are important because the first two types tend to be subject to existing laws and existing professional experience can be applied to law enforcement regarding these offences. Any legal problems arising tend to relate more to legal procedures than substantive law. The final group, however, are solely the product of the Internet and pose the greater regulatory challenges. It is also important, of course, to look for any common features in the substantive behaviours. In this way they can be linked to existing bodies of substantive law and associated experience within the criminal justice processes. Crimes against the machine or Computer integrity‘ crimes are offending behaviours that assault the integrity of network access mechanisms. They include hacking and cracking, vandalism, spying, denial of service, and the planting and use of viruses and Trojans. Many jurisdictions now have legislation such as the Computer Misuse Act 1990 (UK), the Computer Fraud and Abuse Act 1986 (USA) (18 U.S.C. 1030), internationally harmonized by conventions such as the Council of Europe’s Convention on Cybercrime (ETS No. 185; ETS

No. 189), to protect against unauthorized access to computer material; unauthorized access with intent to commit further offences; and unauthorized modification of computer material. Computer integrity cybercrimes also pave the way for further offending. For example, unauthorized access can also be the to more serious crimes. Identity theft from computers becomes serious when the information is subsequently used against the owner. Similarly, crackers may use Trojans to install back doors‘ which are later used to facilitate other crimes, possibly by spammers who have bought lists of IP addresses of infected computers (BBC, 2003).

Crimes using machines or Computer-related‘crimes are committed using networked computers to engage with victims in order to dishonestly acquire cash, goods, or services. In addition are socially engineered variants such as phishing‘, advanced fee frauds and the manipulation of new online sales environments, particularly auction sites. Most jurisdictions have legislation



concerning thefts and provide legal measures for the recovery of lost assets, as well as intellectual property laws to protect against the unauthorised exploitation of intellectual property. Crimes in the machine or Computer content‘ crimes relate to the content of computers—materials held on networked computer systems. They include the trade and

distribution of pornographic materials, the dissemination of hate crime materials, and more recently, the publication of video nasties of the murders of kidnapped foreign nationals. Most jurisdictions have variants of the obscenity laws and laws that prohibit incitement, although their legislative strength can

vary where Internet content is also protected by laws of free speech. In common with the other two crime groups, legislation does nevertheless vary across jurisdictions in terms of judicial seriousness (see below).

This mental map or matrix' (see further Wall, 2002a, p. 192), illustrates that true cybercrimes are criminal behaviours transformed or mediated by the Internet and distinguishes them from more traditional forms of criminal behaviour. They are, to all intents and purposes, new wines in no bottles! (Wall, 1999) Of the wide range of deviant and criminal behaviours that fall under the rubric of cybercrime, many—both traditional and hybrid—are already covered by existing areas of law. However, while they can be found in the police crime diet, they are not a particularly large part of it and tend to fall within the scope of specialist rather than everyday police work while other behaviours, those referred to as true cybercrimes, are entirely alien to the police. This raises questions not only about whether it is the police who should deal with these offences, but also, in the light of the contrast between the high levels of incidence reported by some statistical sources and very low levels of computer misuse prosecutions, who should be policing cyberspace if the police are not? In the UK, for example, during the first decade following the introduction of the Computer Misuse Act 1990 there were only about 100 or so prosecutions against hackers and even fewer convictions (Hansard, 26/3/02, Col. WA35), and this trend is also found outside the UK (see Smith, Grabosky & Urbas, 2004).

Ex.1. Answer the questions:

1. Why cybercrimes are believed to threaten public safety and temper governmental and commercial ambitions for the growth of an information society?
2. How many groups of cyber-criminal opportunity can be identified as points on a spectrum?
3. Develop the statement: "Since cybercrimes are the product of networked computers..."

4. Is the Internet content protected by laws of free speech?
5. Is the contrast between the high levels of cybercrime incidence (reported by some statistical sources) and very low levels of computer misuse prosecutions obvious?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. The term "cybercrime" is precise and clearly defines the space in which harmful online behaviour takes place.
2. Cybercrime is mainly discussed in the media and not fully understood by the public.
3. All crimes involving computers are true cybercrimes.
4. Cybercrime includes phishing, denial of service attacks, and identity theft.
5. There is a clear distinction between traditional crime and cybercrime.
6. True cybercrimes can exist outside of the Internet.
7. Spamming is an example of a true cybercrime.
8. First-generation cybercrimes disappear when the Internet is removed.
9. Second-generation cybercrimes depend entirely on the Internet and cannot occur otherwise.
10. Third-generation cybercrimes are often covered by traditional laws.

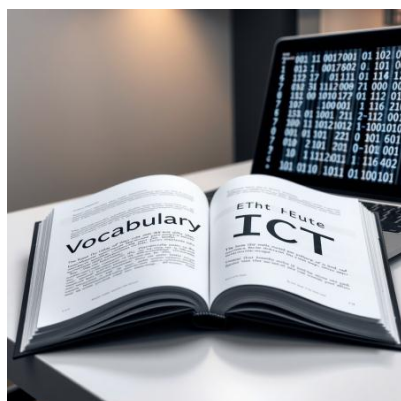
Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing

1.cover			
2. assist			
3. automate			
4.reskill			
5.call			
6. conspire			
7. grow			

Text 6



to wound - ранить

to take/hold smb. hostage – брать кого-то в заложники

to release – освобождать

to injure - травмировать

to hijack - захватить

to explode - взрываться

to execute – казнить

to bomb smth. – бомбить что-то

to blow up - взорвать

hostage - заложник

Read the text: A BRIEF HISTORY OF TERRORISM

In terms of targeting, many of the tactical means and methods of modern terrorism have, until relatively recently, followed those utilized between States in their armed conflicts *interse*. It has been argued specifically that, a century ago, terrorist codes on targeting victims closely resembled professional military codes, in that they respected the distinction between soldiers and officials on the one hand, and innocent civilians on the other (e.g., the targeted assassination of Archduke Franz Ferdinand of Austria on 28 June 1914). This was the case from

approximately the mid-nineteenth century onwards, when increasingly industrialized weaponry facilitated a lack of targeting, in the sense that killing the enemy became more indiscriminate and deadly. The industrialized and indiscriminate means and methods of warfare utilized during the two “total wars” of the twentieth century (e.g., in widespread disregard of the principle of distinction) effectively taught those who would become post-war revolutionary terrorists, and who also would adopt more irregular weapons and forms of fighting, such as urban guerrilla warfare. In the contemporary world, indiscriminate weaponry (e.g., high-level bombing capacities, weapons of mass destruction (WMDs), and so on) is a recurring feature.

In terms of terrorist strategy, a useful way to conceptualize the evolution of modern terrorism as a resort to revolutionary violence is provided by David Rapoport’s influential concept of the “waves” of terrorism (The Four Waves of Terrorism). For



example, one wave is the late nineteenth century/early twentieth century “anarchist wave”. Another is the “anti-colonial wave” (starting with the post-World War I political principle of self-determination, e.g., the Aaland Islands arbitration in 1921, and its violent evolution into a legal right after World War II, examples being the Algerian Civil War and the Vietnam War).

In turn, the tactics employed in each of these waves often mirrored those utilized between States during armed conflict, not least because demobilized soldiers throughout the ages have returned to their homes at the end of a war fully trained tactically to utilize force, while the name of each terrorist wave reflects its dominant strategic goals. The wave theory further reflects that terrorist groups rise and fall, that they can dissolve when no longer capable of

inspiring others to continue with violent resistance to authority, to violently redress one or other grievance, or to protest violently against a lack of political concessions. This point also suggests that terrorism and its motivations are clearly impacted by the conditions of and changes in social and political cultures.

In contrast, Parker and Sitter (2016) posit that violent terrorist situations occur around the world not so much in waves, but because terrorist actors are motivated differentially through four goal-oriented strains: socialism, nationalism, religious extremism or exclusionism. These underlying motivators are not chronologically sequential, i.e., one strain dies and a new one arises. Instead, they can work in parallel, and can occasionally overlap, to motivate different terrorist movements according to their needs.

Such academic discourse offers a flavour of some of the discussions and debates that occur when seeking to better comprehend or categorize “terrorist” groups. This University Module Series, however, does not take a view regarding what the motivational factors of various non-State actors may or may not be. These are issues that those teaching this or any other parts of this University Module Series may wish to explore further within different contexts.

Ex.1. Answer the questions:

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

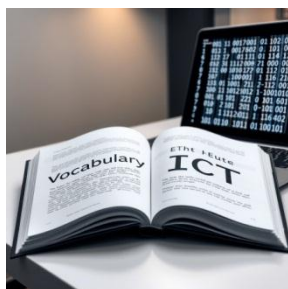
1. Modern terrorism has always used completely different methods than those used in state military conflicts.
2. In the past, terrorists avoided targeting innocent civilians.
3. The assassination of Archduke Franz Ferdinand was a targeted attack aimed only at military personnel.

4. Industrialized weaponry made warfare more precise and less deadly over time.
5. Revolutionary terrorists after World War II adopted irregular weapons and tactics like urban guerrilla warfare.
6. Indiscriminate weapons like WMDs are no longer used today.
7. David Rapoport developed the concept of four waves of terrorism.
8. One of the waves of terrorism identified by Rapoport is the anarchist wave.
9. The anti-colonial wave started before World War I.
10. According to Rapoport, terrorist groups continue to be strong even when they can no longer inspire others.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.start			
2. evolve			
3. overlap			
4.follow			
5.resemble			
6. teach			
7. rise			



Text 7

to threaten - угрожать

to sniff out - вынюхивать

to force - заставлять

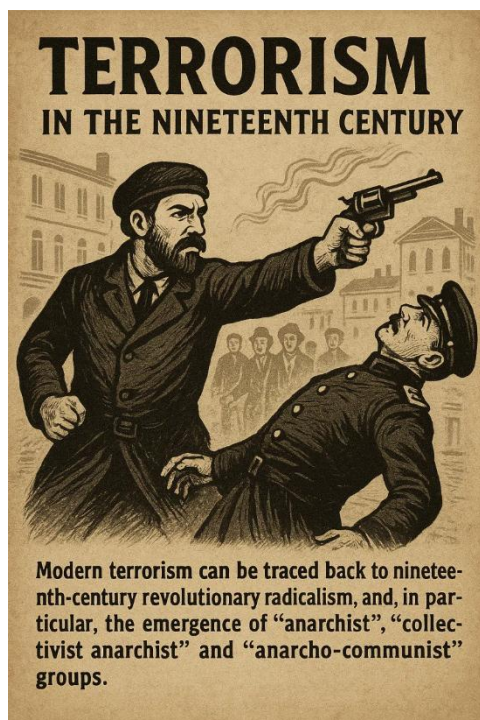
equipment – оборудование

target - цель

to accuse - обвинять

Read the text: TERRORISM IN THE NINETEENTH CENTURY

Modern terrorism can be traced back to nineteenth century revolutionary



radicalism, and, in particular, the emergence of “anarchist”, “collectivist anarchist” and “anarcho-communist” groups. For example, from the mid-nineteenth century onwards, groups led or influenced by the Frenchman Pierre-Joseph Proudhon, author of *What is Property?* (1840), the German Karl Marx, and the Russian Mikhail Bakunin, were promoting one or another anti-establishment model. Within a decade, similar groups had appeared throughout Western Europe, the Balkans and Asia. The German revolutionary Karl Heinzen

was the first to articulate the use of violence, even mass murder, by individuals to effect political change in his influential 1853 pamphlet, *Mord und Freiheit*, coining the term *Freiheitskämpfer* or “freedom fighter” in the process. However, as these early radicals became disillusioned by their failure to provoke widespread social revolution among the peasantry through traditional means such as distributing political pamphlets and leaflets urging uprisings and riots to put government under pressure, they turned instead to violence in the hope of forcing political reform and of undermining the State. In this way, “propaganda by the deed”, as a strategy for political action, became central to the politics of European anarchism (see, for example, Fleming, 1980).

The principal violent method of spreading terror utilized by virtually all such groups at the time was targeted assassination, which not only carried with it serious personal risk but also the potential for political martyrdom. The assassination of Czar Alexander II in 1881 by the Russian revolutionary group *Narodnaya Volya* is emblematic of this period of terrorism.

Targeted assassination could be differentiated from ordinary criminal acts, because targeting persons acting in an official State capacity signified a deep, personal commitment to a “cause that could inspire others, and epitomised the revolutionary ‘code of honour’ by sparing innocent citizens”. This arguably made terrorist assassination a more humane form of violence than civil war, since the terrorist’s targeted attack would strike only against State “oppressors”, and would help maintain the low casualty rate of terrorism that was also an advantage of the “propaganda by the deed” strategy (Morozov, 1880, p. 106).

Technological developments in the mid and late nineteenth century also played a pivotal role in the rise of terrorism. The ready availability of dynamite allowed terrorists to perpetrate and disseminate their deadly acts more widely as propaganda by the deed. The development of mass communication technologies allowed news, learning, ideas and events to be rapidly communicated across long distances, opening up an era of mass communication and of migration that was crucial to inspiring groups elsewhere. The invention of the telegraph and the steam-powered rotary press meant that newspapers could receive messages almost instantly after transmission from around the world and gave millions of people access to information about events virtually as soon as they occurred. New technologies, together with greater access to educational opportunities, facilitated the migration of agricultural labourers and artisans to urban centres. The development of commercial railways and trans-Atlantic passage steamers aided groups to travel long distances, and to carry their political sympathies further afield. Although the successful assassination of Czar Alexander II would initially inspire a wave of anarchist violence that shook Europe and the Americas over the following decades (Zimmer, 2009), Russian rebels

encouraged and trained a variety of rebel groups who were emerging elsewhere, even when their political aims were vastly different. While anarchists carried out bombings in France, Germany, Italy, Spain and elsewhere, which at times turned into cycles of retribution between anarchists and the authorities (Zimmer, 2009), Western States.

The twentieth century link between modern terrorism and the ideal of self-determination arose within the competing ideologies of communist/socialist theory (Lenin, 1914/1972), and those reflected in a League of Nations Covenant in which there is no express reference to the principle of self-determination. In contrast to the rejection of all prior Czarist debts and obligations by the post-war revolutionary Government of the Soviet Union, the United States, under the presidency of Woodrow Wilson, was a strong proponent of the “peoplehood” principle of self-determination (Morgan, 1980, pp. 355-359). However, Wilson did not hold sway on this concept of self-determination at the Versailles conference at which the final version of the Covenant was agreed. In addressing the issue of self-determination, article VI of the Wilson-Miller draft of the proposed League Covenant provided that: The League of Nations shall require all new states to bind themselves, as a condition precedent to their recognition as independent or autonomous states, to accord to all racial or national minorities within their jurisdiction exactly the same treatment and security, both in law and in fact, that is accorded to the racial or national majority of their people.

Even so, such issues in the era of the League of Nations represented only a number of the factors to be considered during the formation of new States, whether within the operational context of mechanisms to attain statehood, or as a matter of self-help. When issues relating to self-determination arose early on in the League’s existence during the Aaland Islands dispute in 1920 between Sweden and Finland, the League Council appointed the International Commission of Jurists to determine the matter. The Commission concluded that the mere recognition of the principle of self-determination, as made out in a number of treaties, did not create a positive rule of the law of nations. In part,

this was due to the Committee's apprehension about creating a precedent for secession, thereby encouraging anarchy. However, a subsequent Committee of Inquiry refined this result by concluding that if Finland failed to provide the islanders with certain specified guarantees, they would indeed have a right under international law to a plebiscite, which could have resulted in separation from Finland. Nowadays, the Aaland Islands solution is regarded as a precedent for successful international dispute settlement.

In the meantime, the spate of terrorist assassinations continued. By the 1930s, several bilateral agreements referred to the suppression of terrorism, and many extradition treaties contained clauses excluding assassination attempts against Heads of State from the exempted list of political offences (e.g., Convention on Extradition 1933, article 3(e)). The assassinations of King Alexander I of Yugoslavia and the French Minister for Foreign Affairs together in Marseilles on 9 October 1934 brought matters to a head, when the requested extradition of the persons accused was refused by Italy on the grounds that the offences were political. In response, a Committee of Experts was established by the League Council to draft a Convention on Terrorism for the establishment of an International Criminal Court, which would have jurisdiction over certain acts specified as acts of terrorism in the Convention, and which States Parties were obliged to criminalize within their national laws. Article 1(2) of the Terrorism Convention defines "acts of terrorism" as "criminal acts directed against a state". Such acts must be "intended or calculated to create a state of terror in the minds of particular persons, or a group of persons or the general public". The Convention is silent on the purpose of the fear generated.

Nonetheless, State and regional traditions of asylum, coupled with strong national sympathies, made any differentiation between "terrorist" and "political" offences problematic, and the granting of asylum remained possible then, as now. Moreover, the 1937 Terrorism Convention, as a creature of its time, had no "international" criminal law to be grounded in which provides that: The present Convention does not affect the principle that, provided the offender

is not allowed to escape punishment owing to an omission in the criminal law, the characterisation of the various offences dealt with in the present Convention, the imposition of sentences, the methods of prosecution and trial, and the rules as to mitigating circumstances, pardon and amnesty are determined in each country by the provisions of domestic law. Therefore, the law applicable to any criminal prosecution for acts established as offences under the Convention was to be that of the referring, and thus, prosecuting, State. Unfortunately, World War II erupted soon after, and neither convention entered into force.

Ex.1. Answer the questions:

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Modern terrorism can be traced back to nineteenth-century revolutionary radicalism.
2. Anarchist groups in the 19th century included “collectivist anarchists” and “anarcho-communists”.
3. Terrorist groups in the 19th century targeted innocent civilians almost exclusively.
4. The assassination of Czar Alexander II in 1881 was a typical example of terrorist violence during that period.
5. Terrorist assassinations were not considered politically motivated acts.
6. Early radicals used only peaceful methods like distributing pamphlets throughout the 19th century.
7. Karl Heinzen coined the term “freedom fighter” (Freiheitskämpfer) in his 1853 pamphlet *Mord und Freiheit* .
8. The strategy called “propaganda by the deed” became central to European anarchism.

9. Technological developments had no impact on the spread of terrorism in the 19th century.

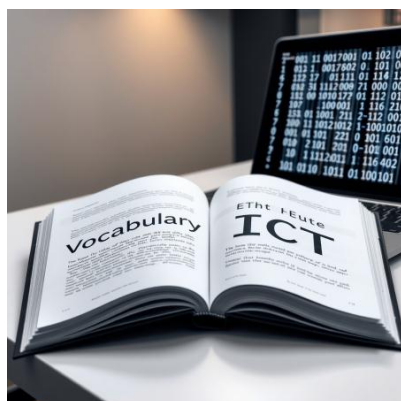
10. Dynamite made it harder for terrorists to carry out attacks.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.draft			
2. oblige			
3.link			
4.refuse			
5.create			
6. criminalize			
7. hold			

Text 8



Study this vocabulary:

to witness - свидетельствовать

violate/ to break/ to breach - нарушать

to magnify/ to exaggerate - преувеличивать

to expose to violence – подвергать насилию

to explode - взрываться

to avert a threat – предотвращать угрозу

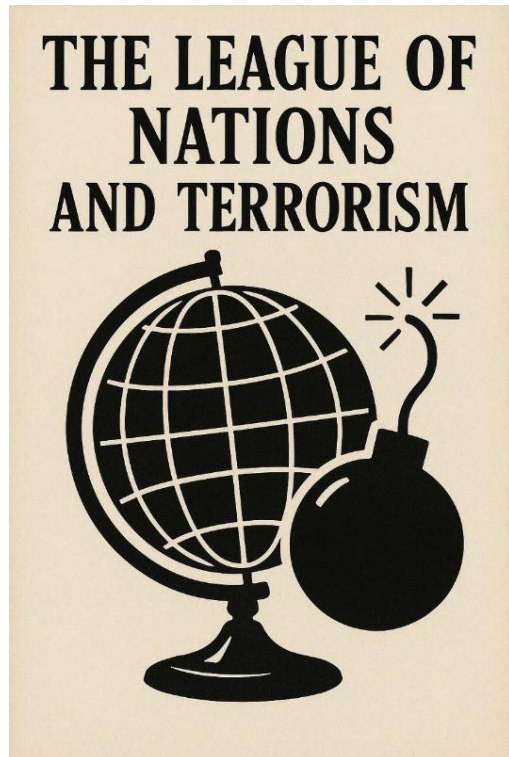
to assassinate - покушаться

to adhere to / to stick to ...- придерживаться

Read the text: THE LEAGUE OF NATIONS AND TERRORISM

The 1919 Versailles Peace Treaty between Germany and the Allied Powers that concluded World War I precipitated the next phase in the development of modern terrorism. The Covenant of the League of Nations (the League Covenant) redistributed former German and Turkish colonies and other dependencies through the League mandate system, which was designed to ensure a “mild form of international accountability for [their] administration”. Otherwise, standards to help integrate minority peoples in the new States created after 1919, such as Yugoslavia, were also provided for, and were intended to serve a peace-making function, while deterring trans boundary alliances. Nonetheless, protected common rights, such as the right to a nationality, the free exercise of belief, employment and identity, and rights enshrined in the ideals of the mandate system and policies on minorities did not apply to the peoples and minorities in the victorious States, which later were instead the guarantors of peace and security as a whole, while the victors also presumably rejected the notion of new colonial acquisitions when declining to annex former colonies and non-governing territories. Overall, the Covenant system of mutual defense appeared to be designed to favour international security concerns rather than those of the rule of law and international law, in the event of a conflict.

In any event, many terrorist activities that have occurred during the post-1945 era have not been associated with self-determination debates at all. Identified causes of terrorism have instead ranged through the entire spectrum of



human discontent, including the economic, political, social, psychological, ideological, etc., with short or long-term goals, both objective and subjective, becoming the object of violence . In response, some in the international community, especially academics, have sought to label terrorist groups according to their motivational goals or ideologies rather than in terms of criminal acts, as is the approach within the United Nations system. Consequently, students may come across the categorization of such groups within scholarship as “revolutionary”, “separatist”, “ethnocentric”, “nationalist” or “religious”.

In terms of the use of violence and force by terrorists, this also ranges across a wide spectrum, from individuals with military training and experience, to what Whittaker has termed “throw away” operatives, who are effectively sent untrained on suicide missions. Their use of violence also illustrates the slow evolution of terrorist tactics and strategies, including traditional assassination, bombings, arson, hostage-taking, hijacking, kidnapping, sabotage, the perpetration of hoaxes and suicide bombings.

More recent tactics can include unconventional forms of terrorism, including nuclear terrorism (for example, fabricating a dirty bomb, attacking a nuclear reactor,etc.), high-tech terrorism involving cyberattacks, ecological terrorism (for instance, the threat of destruction to the environment) and terrorist attacks aiming at destroying cultural heritage,as perpetrated by ISIL (see, for example, the Executive Committee of the Commonwealth of Independent States, 1999, article 1).

Of particular interest is the fact that such issues and debates have shaped the approach of the international community to its universal anti-terrorism conventions so that are framed around terrorist acts as serious international crimes regardless of any underlying motivation.

Broadly speaking, anti-terrorism instruments were adopted roughly in three phases. Beginning with legislation covering the safety of aviation and shipping, the early instruments were developed from the 1960s through to the

early 1990s, and addressed specific types of terrorist offences. Notably, acts perpetrated during “liberation conflicts” were expressly made exceptions to terrorist crimes, for example, the 1979 Hostages Convention as such acts were to be dealt with under other areas of international law, such as international humanitarian law. The most recent phase reflects the broadening, post-categorization of terrorist groups and “causes”, to include groups such as the Taliban, Al-Qaida and ISIL, and thus reflect the contemporary terrorist threat to the international community. Within this latter phase, anti-terrorism instruments have been developed that deal with new crimes associated with terrorist bombings, the financing of terrorism and nuclear terrorism.

Ex.1. Answer the questions:

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. The 1919 Versailles Peace Treaty marked the end of World War I and had no impact on the development of modern terrorism.
2. The League of Nations' mandate system was intended to ensure international accountability for the administration of former colonies.
3. Minority rights were protected equally in all countries, including victorious states like France and Britain.
4. Many post-1945 terrorist activities are connected to debates about self-determination.
5. Causes of terrorism are limited only to political motives.
6. Terrorist groups are always defined by their criminal acts in international law.
7. Terrorist violence is limited to highly trained military individuals.
8. Traditional terrorist tactics include assassination, bombings, arson, and hostage-taking.

9. Nuclear terrorism involves cyberattacks on nuclear systems, but does not include physical attacks on reactors.

10. Ecological terrorism refers to using environmental destruction as a tool of terror.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.conclude			
2. design			
3. deter			
4.apply			
5.range			
6. label			
7. attack			

Text 9

Suspicious - подозрительный

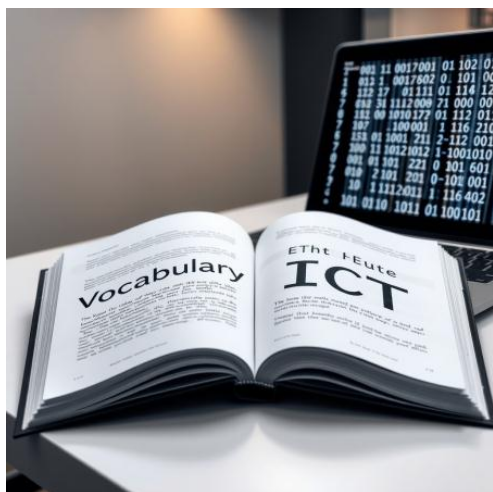
Leverage - воздействовать, усиливать, использовать

Disseminate - распространять

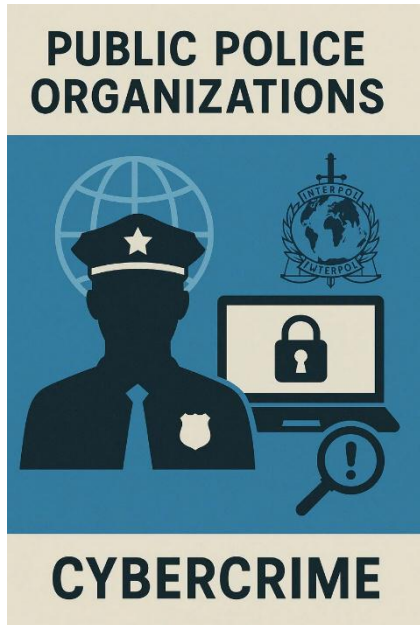
Collaboration - сотрудничество

Assist - помогать, оказывать содействие

Robust - мощный, сильный, крепкий



Public police organizations



Public police organizations draw upon the democratic mandate of government to impose governance by maintaining order and enforcing national law. Surprising to many, the public police play a comparatively small role in enforcing criminal sanctions upon wrongdoers online, however, whilst small it is an important role because of the public's reliance upon the police in times of emergency. The role played by the police in policing cybercrimes can vary from force-to-force and investigative tactics usually combine traditional policing methods with the use of computers to investigate wrongdoers and collect evidence, they may also use software based techniques to proactively police some priority concerns (Sommer, 2004).

Although the public police are located within nation states and work under national laws, they are nevertheless networked by transnational policing organizations, such as Europol and Interpol, whose membership requires formal status as a police force (see Sheptycki, 2002). In most Western countries, the public police are organized regionally, and within most local police services there usually exist specialist individuals or groups of police officers who can respond to Internet related complaints from the public. Some police forces set up their own cybercrime units, whilst others enter into strategic alliances with neighboring police forces to provide such services. In addition, there also usually exist national police organizations which deal with the collection of intelligence and the investigation of organized crime. The US and UK experiences sum up the complexities of mapping cybercrime onto traditional policing structures and illustrate the need for specific arrangements for policing cybercrime.

In the USA, the policing of its population of 250 million is carried out by upwards of 17,000 independent local police forces (the actual number varies according to definition of police used). The smaller forces tend to outsource the investigation of cybercrimes to larger forces that possess the expertise. At a national and cross-state level, jurisdiction for cybercrime lies with the Federal Bureau of Investigation. Although the US Secret Service, once a bureau of the Treasury, but since March 2003 part of the Department of Homeland Security, carries a responsibility for investigating crimes —involving U.S. securities, coinage, other government issues, credit and debit card fraud, and electronic funds transfer fraud (US Secret Service, Duties and Functions).

Policing the UK's population of 60+million is delivered by about 55 main local police forces (the number varies slightly depending upon how they are defined). Most forces have a cybercrime investigation capability themselves or with a neighboring force. The types of cybercrime dealt with are traditional crimes that use computers or hybrids, those traditional cybercrimes for which the internet has created globalised opportunities for victimisation. The main problem area for the public police in the UK as in the US are the true cybercrimes, those which are the spawn of the internet, such as spamming, spam driven frauds and scare ware.

Policing cybercrime in the UK is now shaped by a series of strategies. The Cyber Crime Strategy (Home Office, 2010a) mentioned earlier, specifically deals with online criminal activity, and sits alongside the National Fraud Strategy (NFA, 2009) and the Association of Chief Police Officers E-crime Strategy (ACPO, 2009). In theory, this combination provides a co-ordinated policing response to the different types of potential harm found online.

Ex.1. Answer the questions:

1. Do the public police play a comparatively small role in enforcing criminal sanctions upon wrongdoers online?

2. Do the public police usually combine traditional policing methods with the use of computers to investigate wrongdoers and collect evidence?
3. Do the public police work under national laws?
4. The public police are networked by transnational policing organizations, such as Europol and Interpol, aren't they?
5. Do national police organizations deal with the collection of intelligence and the investigation of organized crime?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

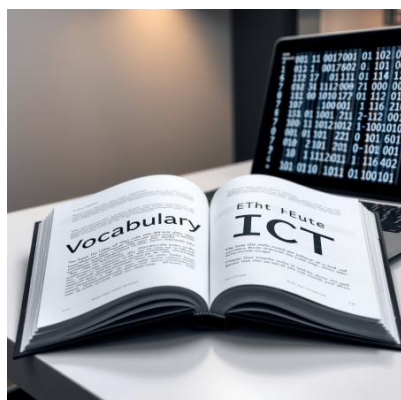
1. Public police organizations are based on democratic mandates to maintain order and enforce national law.
2. The public police play a large and dominant role in enforcing criminal sanctions online.
3. Public reliance on police during emergencies makes their role in cybercrime policing unimportant.
4. Investigative tactics used in cybercrime can combine traditional methods with computer-based investigations.
5. All local police forces have the same level of expertise in cybercrime investigation.
6. In the UK, there are no specialist individuals or groups dealing with cybercrime.
7. Some police forces set up their own cybercrime units.
8. The US Secret Service investigates only traffic violations.
9. National police organizations deal with intelligence collection and organized crime.
10. The Federal Bureau of Investigation (FBI) has jurisdiction over cybercrime at cross-state level in the USA.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.require			
2. network			
3. organize			
4.vary			
5.play			
6. impose			
7. collect			

Text 10



Study this vocabulary:

bring in guilty - признавать виновным

term for serving punishment - срок отбывания наказания

find innocence - признать невиновным

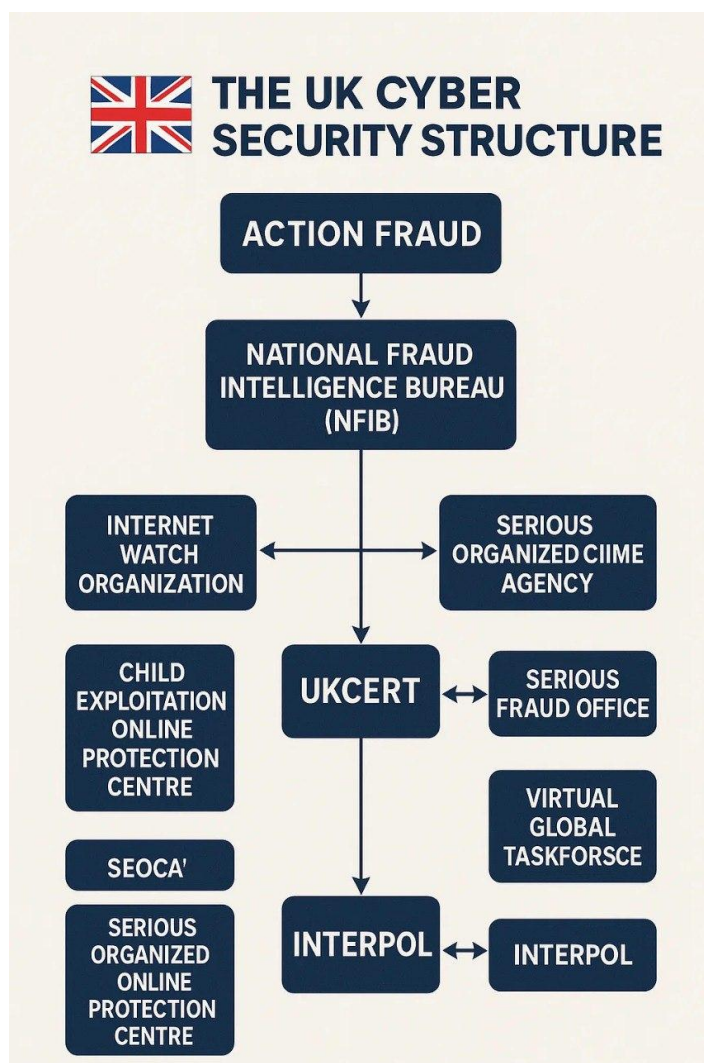
delinquent - малолетний преступник

identity-related crime - преступление, связанное с

использованием личных данных

The UK Cyber security structure

Central to the UK's cybercrime policing response is a combination of a new national policing capability and new internet crime reporting facilities. The new Action Fraud reporting centre was established in late 2009 as a central point



of contact for the public. Supported by the National Fraud Authority it receives reports of frauds and related forms of cybercrime such as phishing (id theft) which are currently the main type of cybercrime affecting individuals and businesses. Action Fraud also offers news and information on fraudsters activities to alert the public of the dangers facing them.

Reports of websites containing obscene imagery are still received, evaluated and acted upon by the Internet Watch Organization (IWF).

The IWF is an independent organization created in 1996 by internet service providers to combat obscene imagery, and broadened in 2000 to include to racist material in its remit. It operates with special ACPO/ Crown Prosecution Service (CPS) immunity under Section 46 of the Sexual Offences Act 2003 which allows staff to view obscene images including child pornography without risk of prosecution. The IWF refers actionable cases to the Child Exploitation Online Protection Centre (CEOP), part of the Serious Organized Crime Agency (SOCA). Originally destined to become an independent agency in April 2011, it is now (following a July 2010 announcement) due to join SOCA, the NPIA (National Police Improvement Agency) and other policing agencies with a national remit become part of the new integrated UK National Crime Agency (Home Office 2010b, 23-30). Reports of hacking (crimes against the machine)

are currently received from systems security officers by UKCERT (UK Computer Emergency Response Team). Paragraph 86 of the Cyber Crime Strategy states that the Action Fraud reporting model may be extended to the other types of cybercrime in the future.

The reports of cybercrime received by Action Fraud are passed on to the National Fraud Intelligence Bureau (NFIB) which analyses them and decides how they are to be acted upon through its national tasking system. Located within the City of London Police, the NFIB also builds up a national picture of particular types of fraud that would otherwise be regarded as local problems of which the true scale would never be known. The NFIB works alongside the National Police Central e-Crime Unit (PCeU) which is based within the Metropolitan Police and investigates cybercrimes that have national impact. Alongside these arrangements are a range of other anti-e-crime initiatives, such as an Office of Fair Trading (OFT) facility that enables the public to report bogus websites.

Whenever reported cybercrimes are found to be serious, then other agencies such as SOCA (Serious Organized Crime Agency), the Serious Fraud Office (SFO), CEOP or even the security services may become involved. When the crimes transcend borders – as many do – then Interpol may become involved. If the reports of crimes specifically refer to child abuse on a global scale then the Virtual Global Taskforce (VGTF) becomes involved. Set up in 2003, the VGTF is an international working partnership between different police forces and other law enforcement agencies such as Interpol. The following table summarises the seven networks of security. The answer to the earlier questions posed about the effectiveness of the role of the public police in cyberspace become clearer when understood in terms of the various networks of security which operate to police the internet. Yes, there are low levels of police performance indicators against high levels of policing technology but what the security networks to show is that the police actually only play a very small part in governing the Internet and even then it tends to be jurisdictionally based. This

is not however, to say that cyberspace goes un-policed, rather, as Reiner once observed with regard to terrestrial policing more generally: not all policing lies in the police.

The broader governance of the Internet is, then, characterized by a sense of order resulting from a complex assemblage of networked nodes of security that continually shape virtual behavior, transcend the state/non-state binary, and also state sovereignty (Shearing, 2004, p. 6). The term assemblage is particularly useful in this context when considering the relationships between nodes and also within them. Without attributing causality, assemblage describes the relationship between heterogeneous contributors to governance that work together as a networked and functional entity, but do not necessarily have any other unity.

In some of these networked relationships there may be a consensus of interest in approach, while in others the consensus may be in the outcomes or goals achieved. Consequently, a replication is found in the bifurcation of broader functions in terrestrial policing between the maintenance of order through the assemblage and the enforcement of law to deal with more serious offending behavior. By separating the two, some sense can be made of the rather conflicting messages that are emerging in debates over policing the Internet. Networked security, for example, exploits the natural surveillance (see earlier) that networked technologies enable and allows both primary and secondary social control functions to operate. Furthermore, it also tends to mediate, to some extent, global disparities arising from national or jurisdictional legal differences in definition.

The observation made earlier that many cybercrimes fall outside the traditional police agenda would seem to render them unproblematic from a police resourcing point of view—they simply do not get resourced. On the other hand, the public police not only tend to lay claim culturally (organizational and occupational) to a greater ownership of policing the Internet than they actually own, but more importantly, they are also expected to do so by the public because

of their traditional consensual relationship with the state and their symbolic duty to protect the public from danger.

We see in the debates over the policing of the Internet a replication of the reassurance policing debate (Crawford & Lister, 2004), though with a slight twist. The reassurance policing debate is borne out of the increasing recognition that the police alone cannot win the fight against crime and disorder nor meet the public's seemingly insatiable demand for a visible policing presence (Crawford & Lister, 2004, p. 413). The debate, when shifted to cyberspace, takes for granted that the police alone cannot win the fight against crime, but nevertheless demands a more visible policing presence. This begs two questions: what challenges do cybercrimes pose for the public police? And how do the police deal with them?

Ex.1. Answer the questions:

1. When and why was the new Action Fraud reporting centre established in UK?
2. Does the National Fraud Intelligence Bureau (NFIB) analyze the reports of cybercrime and decide how they are to be acted upon through its national tasking system?
3. Does the Metropolitan Police and investigate cybercrimes that have national impact?
4. Do cybercrimes fall outside the traditional police agenda?
5. Can the police alone win the fight against crime meet the public's seemingly insatiable demand for a visible policing presence?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. The UK's cybercrime policing response includes a new national policing capability and improved reporting facilities.

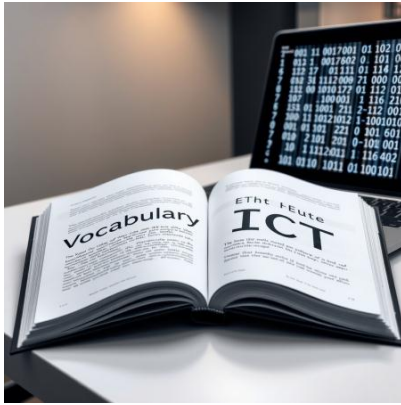
2. Action Fraud was created in 2003 as a central point for reporting cybercrime.
3. Action Fraud only receives reports about hacking, not fraud or phishing.
4. The Internet Watch Foundation (IWF) was founded by internet service providers in 1996.
5. The IWF has immunity under Section 46 of the Sexual Offences Act 2003.
6. The Child Exploitation Online Protection Centre (CEOP) is part of Interpol.
7. Reports of hacking are handled by UKCERT.
8. The National Fraud Intelligence Bureau (NFIB) works within the Metropolitan Police.
9. The National Police Central e-Crime Unit (PCeU) investigates cybercrimes with national impact.
10. The Office of Fair Trading does not participate in cybercrime prevention.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.mediate			
2. shape			
3. state			
4.join			
5.establish			
6. alert			
7. allow			

Text 11



Study this vocabulary:

to keep up with criminals – быть в курсе преступной деятельности

inevitably – неизбежно, обязательно

allegations – необоснованное обвинение;

утверждение

backfire – иметь негативные последствия

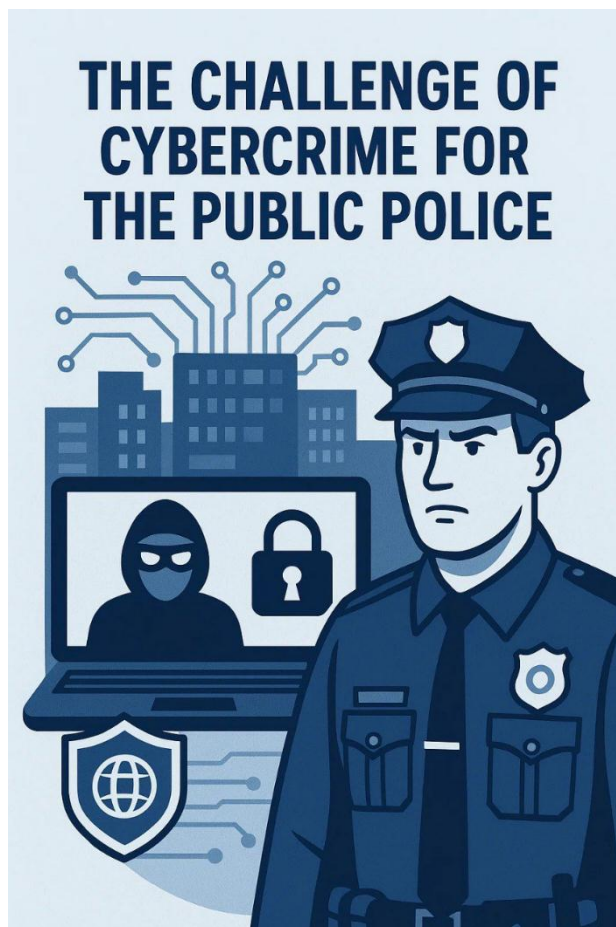
accumulation – накопление

allocation – распределение, назначение

bulk – объем; основная масса

The Challenge of Cybercrime for the Public Police

The relationship between the police and technology is long-standing and



complex, and a brief reflection explains much about the situation of the public police today. On the one hand, the police were created to deal with the social disorder caused by the technologies of the industrial revolution. On the other hand their responsive and localized nature always meant that they fell behind in their access to, and use of, technology. A long-standing complaint made by members of police and law enforcement agencies is that they do not have the facilities to keep up with criminals,

especially with regard to offences that require, what Brodeur has termed, a high policing response. Indeed, for over a century readers of the Police Review and

other contemporary police journals were regularly told by police correspondents that they lacked the resources to obtain the latest technologies that would help them to respond to criminals. More recently, the complaints have focused upon obtaining modern IT equipment and high specification broadband links. Of course, such complaints inevitably backfire as they result in (often unfounded) allegations about police ineffectiveness, which ultimately reinforce the police-originated myth that criminals are ahead of the game. However, while historical themes can be drawn out, what distinguishes the modern debates from their predecessors is not just access to latest technology and skill sets, but access to technology to facilitate networking and networked policing, including access to relevant networks of security. But, it is one thing to possess the technological capabilities and another to be able to utilize them, and there are a number of institutional obstacles to this task. The public police, like the other criminal justice agencies are deeply conservative institutions that have been moulded by time-honoured traditions, and therefore do not respond readily to rapid change. Furthermore, much of this innate conservatism originates in the police also being symbolic expressions of state sovereignty. Therefore, one way that the police forces generally respond to new issues, whilst preserving their symbolic and organizational conservatism is through the origination of specialist units into which officers with appropriate specialisms are absorbed. While this tactic constitutes an actual and visible response, it nevertheless tends to marginalise the problem it sets out to solve, and runs the risk of preventing the broader accumulation of organizational and professional experience across the force in dealing with the issue at hand. Ultimately, it is the presence of a relevant body of specialist knowledge and expertise within a police force (and whether the other officers know about it) that can determine whether or not the organizational and occupational response of the police to a new public concern is effective or not. Nevertheless, the global reach of new forms of technological crime organization, such as cybercrimes, are markedly different to the daily public police crime portfolio. The public police were originally introduced to

keep the dangerous classes off the streets by maintaining local order and enforcing law (mostly the former), and modern police agencies remain largely responsive to public complaints. The reutilized responses to these complaints determine police funding and leave the police subject to tight budgetary constraints which restrict the immediate allocation of major resources to emerging matters and therefore their responsive capability. The limitations of the Peelian policing paradigm to have long been understood and there have been employed a number of strategies to resolve the contradictions. At a procedural level, there has been the establishment of international harmonization and police coordination treaties, such as the Council of Europe's Convention on Cybercrime. A range of national/federal and even international police organizations (for example, Interpol, Europol), have been introduced to complement locally organized police in their investigation of crimes occurring across police jurisdictions. However, despite these procedural and organizational responses, cybercrimes still pose a range of challenges to the police, which are outlined below.

Characteristic of many cybercrimes is that they are small-impact bulk victimizations with a large aggregated loss, but spread out globally across a range of jurisdictions. Since local policing strategies are often reduced to decisions that are made at a very local level over the most efficient expenditure of finite resources (Goodman, 1997, p. 686), the public interest, a key criterion in releasing police resources for an investigation, is often hard to justify in individual cases of cybercrime victimization.

Peelian Paradigm' refers to the structure, values and principles of the British Police which were subsequently adopted by many countries around the world and which formed a basis for modern policing standards. Set up by Sir Robert Peel in the late 1820s, the British Police were essentially a bureaucratically organized agency formed locally but partly funded by government to keep the dangerous classes off the streets, maintain order and enforce law.

Ex.1. Answer the questions:

1. Do the police complain that they lack the resources to obtain the latest technologies that would help them to respond to criminals?
2. Are the public police, like the other criminal justice agencies deeply conservative institutions that have been moulded by time-honoured traditions, and therefore do not respond readily to rapid change?
3. Do the reutilized responses to citizens' complaints determine police funding and leave the police subject to tight budgetary constraints which restrict the immediate allocation of major resources?
4. What international police organizations have been recently introduced to complement locally organized police in their investigation of crimes occurring across police jurisdictions?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. The relationship between police and technology is new and simple.
2. Police were originally created to deal with social disorder caused by industrial technologies.
3. Police have always been ahead of criminals in terms of access to modern technology.
4. Law enforcement agencies say they can easily keep up with cybercriminals using current IT tools.
5. Cybercriminals are often said to be "ahead of the game" compared to the police.
6. Modern debates about policing cybercrime are exactly the same as older debates.
7. Possessing technological capabilities is enough to successfully fight cybercrime.

8. Public police forces are very flexible and open to rapid change.
9. Police departments often create specialist units to handle cybercrime.
10. Creating specialist units helps spread cybercrime knowledge across the entire police force.

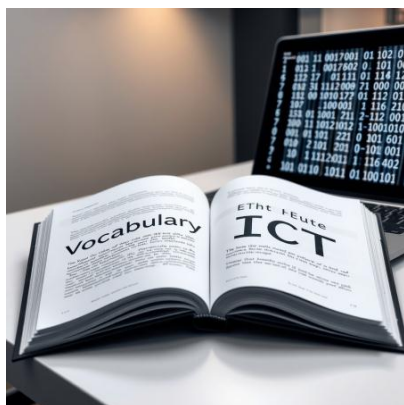
Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.respond			
2. reinforce			
3. utilize			
4.accumulate			
5.know			
6. keep			
7. justify			

Text 12

Study this vocabulary:



validity –законность; действительность

entrapment –провокация

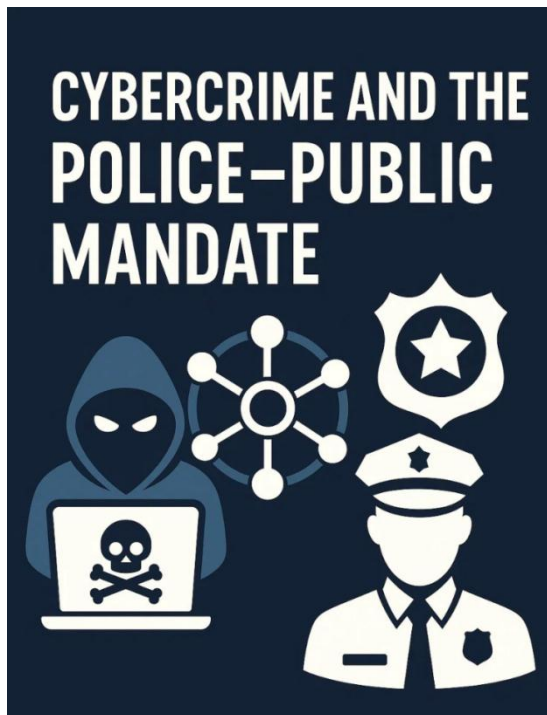
to capture –поймать; захватывать

innocuous –безопасный; безвредный

to take heed –принять во внимание

Cybercrime and the Police–Public Mandate

The future of the public police role in policing the Internet is about more



than simply acquiring new expert knowledge and capacity. As is increasingly the case with bulk policing it is about forging new types of working relationships with other nodes within the networks of Internet security. Relationships that require a range of new transformations to take place in order to enhance the effectiveness and legitimacy of the nodal architecture—a flattening of policing structures, parity of legal definitions across boundaries, broadly accepted frameworks of accountability to

the public, shared values, multi-agency and cross-sectoral dialogues, and more. Without these transformations there will always be the danger of a drift away from the disciplinary society towards a technology driven control society of ubiquitous law enforcement and also ubiquitous crime prevention. However, this adverse potential is for the time being tempered by the intervention of law, the human condition (through inaccurate data entry), and some theory failure in crime prevention caused by an inadequate conceptualization and understanding of cybercrime and its associated risks. This will not last indefinitely however.

Some of the contradictions faced by the police have been reconciled by the reconstitution of the Peelian principles of policing and the emergence of a neo-Peelian agenda across a global span. Whilst this resituates the police as an authority within the networks of security it nevertheless demands a range of instrumental and normative responses from them. Whilst one of those responses is to temper the drift towards ubiquity, there is also optimism in the potential for those same technologies also to provide important opportunities for police

reform. The surveillant characteristics that make technology a powerful policing tool, for example, also make it a natural tool for overseeing police practice, and for creating broader organisational and public accountability (The prognosis is fairly good in one respect: we are gradually learning more about the impact of networked technologies upon criminal behavior, and therefore learning more effective and acceptable ways of dealing with them. More research about Internet victimisation is being commissioned by funding bodies and the recent inclusion of relevant questions in the Bureau of Justice Statistics National Crime Victimization Survey (NCVS) and the British Crime Survey (2003-2004 and again from 2010) will yield useful empirical data about victimisation that will counter some of the misinformation about cybercrime that has accrued during the past decade. Within the UK public policing family, we have in recent years seen the publication of the UK Cyber Crime Strategy, subsequent creation of the Office of Cyber Security, the introduction of the (National) Action Fraud reporting centre and the National Fraud Intelligence Bureau, plus the Police Central E-Crime Unit. When combined with the various regional police units, a corpus of professional policing experience in the field is being established—as is also the case in other jurisdictions. And the laws are still being revised. In the UK, the Computer Misuse Act 1990 has been expanded by s. 35–38 of the Police and Justice Act 2006 to make DDOS attacks and the distribution of hacking tools illegal. In the common law jurisdictions, the laws are, of course, also being clarified by case law.

Another plus is that the actions of police officers are currently framed by legislation and codes of practice, however, it is of concern that many of the other partners in policing the Internet are not, other than within the broader confines of law. Particularly worrying is the lack of checks and balances on the noticeable shift towards the technological determinism of automated policing initiatives, driven largely by the influence of the cyber-security industry in the application of software solutions to cybercrime. There are, for example, a broad range of moral, ethical, and legal concerns about the implications of the high

degree of entrapment when employing honeypots and honeynets, not least in the validity and strength of evidence presented to the court that is if this form of policing is in fact designed to capture offenders or simply deter offending through the technological imposition of panoptic discipline and its chilling effect. Take for example, something as seemingly innocuous as spamming, which is a true cybercrime in more ways than one (Wall, 2005b). Many ISPs have introduced anti-spam software into the delivery process and in so doing contravene the long-standing end-to-end principle of the Internet which is freedom of movement across the network to its nodes while leaving choice and mode of receipt to the end users. No one in their right mind wants to receive spam, except perhaps the spammers, yet there has been little critical discussion about the application of spam filters into the delivery mechanisms. The point here is that true cybercrime is increasingly being regarded as a technical problem and as a consequence, important decisions are being made largely on scientific grounds simply because a filter can be made possible. In the case of spam there is understandably little objection, but since the technological solutions appear to work, then, why not also apply similar filtering to hash-set analyses of images or to certain words or combinations of words, and filter out everything that is deemed undesirable? The main concern here is that whilst the offending behaviors may be the provenance of comparatively few individuals (compared with all Internet users), all users are affected by what effectively become the application of an anti-social criminology of everyday life (Hughes, McLaughlin, & Muncie, 2001). In this matter we may do well here to take heed of the concerns expressed by the Frankfurt School—Horkheimer and Adorno in the *Dialectic of enlightenment* about using technology to solve problems, because without balances and checks, the technology becomes aware of everything but itself and its own blind spots and biases' (Agger, 2004, p. 147).

This paper has explored the challenges that cybercrimes pose for the police and their mandate from the public. It has mapped out the nature of the cybercrime issue, highlighted some of the public misunderstandings about it,

before examining the role played by the public police in policing the Internet within the broader architecture of Internet governance. It has illustrated how the Internet and the criminal behavior it transforms challenge the processes of order maintenance and law enforcement. Not only does Internet-related offending take place within a global context while crime tends to be nationally defined, but the police's public mandate prioritizes some offending over others, particularly where there is a perceived dangerous other, as in the production of child pornographic images. Furthermore, policing the Internet is a very complex affair by the very nature of policing and security being networked and nodal. It is also complex because within this framework the public police play only a small part in the overall policing process. Yet the Peelian heritage of the police that has long defined their relationship with the state and the public has caused the police to instinctively assert ownership over the policing function. Cyberspace generates many questions about whether their cultural heritage and traditional constitutional position actually fits them organizationally for a role in policing cyberspace.

In formulating responsive strategies to cybercrime we need realistic expectations of what the police can and cannot do and what are the capacities of the other nodes in the security networks. Accordingly, Internet governance should be configured to assist and strengthen the Internet's natural inclinations to police itself, keeping levels of intervention apposite while installing appropriate structures of accountability. Remember that the same networked technologies that empower criminals also provide a range of highly effective policing tools that are made all the more powerful by the capture of data trails following each Internet transaction and which enable policing to transcend time, place, and space. Indeed, much of the debate in past years about equipping a beleaguered and under-equipped police to cope with technology is rapidly being replaced by increased concerns about over-surveillance through the gradual hard-wiring of society. A delicate balance has to be drawn between the need to maintain order and the enforcement of laws in order to provide a balance

between the desires of law and the desires of law enforcement. Without such a balance, every infringement of law could easily become automatically identified by using technology and we will begin to descend into a world of strict liability characterized by reverse burden of proof. In such a scenario, we are likely to experience an uncontrollable drift from a disciplinary society to a control society where post-event Peelian policing models will be replaced by a pre-crime mentality based upon simulations of crime and behavioral prediction. In such a situation, entire populations could become vulnerable to being evaluated in terms of their individual potential criminality and to technological sorting according to their particular risks to society.

Ex.1. Answer the questions:

1. What is the future of the public police role in policing the Internet?
2. Does the emergence of a neo-Peelian agenda demand a range of innovative instrumental and normative responses?
3. Do many ISPs have introduced anti-spam software into the delivery process?
4. Has there been little critical discussion about the application of spam filters into the delivery mechanisms?
5. What is the main goal of balances and checks system?
6. Comment on the statement: “Furthermore, policing the Internet is a very complex affair by the very nature of policing and security being networked and nodal”.

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. The future of public police in cyberspace is only about acquiring new technical skills.

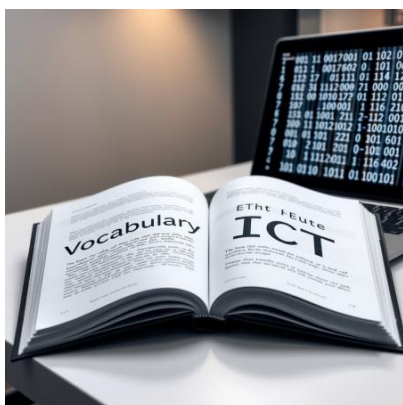
2. Public police must change their structures and legal definitions to improve cybercrime policing.
3. Cybercrime policing can be done effectively using traditional hierarchical and national approaches.
4. The Peelian principles are no longer relevant in modern cybercrime policing.
5. Technological solutions like spam filters raise no ethical concerns.
6. Spamming is considered a true cybercrime.
7. Anti-spam software always respects the end-to-end principle of the Internet.
8. Cybercrime policing requires collaboration between multiple agencies and sectors.
9. There is currently an unlimited amount of empirical data available on cybercrime victimization.
10. The UK has developed specific strategies and units to deal with cybercrime.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.clarify			
2. flame			
3. concern			
4.filter			
5.affect			
6. maintain			
7. highlight			

Text 13



Study this vocabulary:

undeniable –бесспорный

to pose serious threats –представлять серьезную угрозу

the release of –освобождение

adequate protection –необходим ая защита

The Effects of Cybercrime on the Global Economy



Within the past few weeks, news of the cyber-hack into Sony Pictures' confidential files has demonstrated once again the undeniable influence that individuals can hold over a major corporation due to the empowerment of the globalization of modern technology. Unlike any other time in human history, the rise of the "Information Age," which has led largely to positive global effects like easing barriers to trade, efficiency in communication or sharing ideas, and enhancing the

private citizen's ability to raise awareness for social progress, has also enabled criminal activity to pose serious threats to not only fellow individuals, but massive corporations and governments as well. For this reason, the White House has called the attacks on Sony a "serious national security matter" due to

the effects that cybercrime can inflict not only on a nation's informational security, but also on the global economy.

While Sony's decision to cancel the release of "The Interview," the film that sparked the hacks into Sony's information, has reportedly cost the corporation \$200 million USD, the Center for Strategic and International Studies (CSIS) found that cybercrime costs the global economy about \$445 billion USD every year. Furthermore, losses from theft of intellectual property of individuals exceeds \$160 billion USD each year. Studies show that most victims of cyber-hacking come from the world's most developed countries, including the United States, China, Japan, and Germany. Although some major cyber-attacks are government sponsored, such as the Sony attack which was allegedly supported by North Korea, the majority of attacks occur against private citizens and are connected to the theft of personal information.

Regarding the international system as a whole, cyber-attacks cause a major stumbling block for global economic growth due to its detrimental effects on innovation and the theft of ideas. Many small businesses without adequate protection are hacked without any knowledge of the act until their sales greatly suffer years later due to competitors gaining knowledge of the company's logistics, target markets, or personal information. As shown by the Sony attack, even some of the largest companies involved in software development can still fall victim to these attacks, but fortunately international collaboration has begun to show signs of reducing the rate of cyber crime. Therefore, as technological advances continue to spur on the efficiency in global commerce, firms must focus on protecting their personal and corporate information from information traders involved in the illicit markets of cybercrime.

Ex.1. Answer the questions:

1. What a positive global effect has the rise of the "Information Age," led largely to?

2. Why did the White House call the attacks on Sony a "serious national security matter"?
3. Can cyber-criminal activity pose serious threats to not only fellow individuals, but massive corporations and governments as well?
4. Why do cyber-attacks cause a major stumbling block for global economic growth?
5. Why do firms must focus on protecting their personal and corporate information from information traders involved in the illicit markets of cybercrime?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

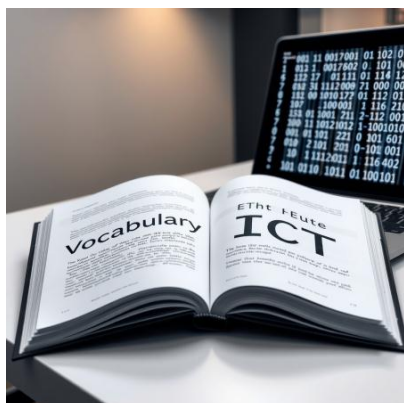
1. The cyber-hack into Sony Pictures' systems shows that individuals can have a strong influence over major corporations through modern technology.
2. The Information Age has only had positive effects on global society and economy.
3. The White House called the attacks on Sony a minor issue with no impact on national security.
4. The film "The Interview" was released without any problems after the cyberattack.
5. Cybercrime costs the global economy about \$445 billion USD every year.
6. Losses from theft of intellectual property amount to more than \$160 billion USD annually.
7. Most victims of cyber-hacking are located in developing countries.
8. All cyber-attacks are sponsored by governments.
9. Cyber-attacks have no effect on innovation or economic growth.
10. Small businesses are immune to cyber-attacks if they do not use advanced software.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1. provide			
2. connect			
3. occur			
4. creat			
5. spur			
6. trade			
7. focus			

Text 14



Study this vocabulary:

economical disruption –экономические
 потрясения
 to compete with their peers –соревноваться со
 сверстниками
 gain acceptance – получить признание
 conspire – сговор

unsavory – неприятный

insert – вставлять

CYBER-CRIMES AND THEIR IMPACTS

In the current era of online processing, maximum of the information is online and prone to cyber threats. There are a huge number of cyber threats and their behavior is difficult to early understanding hence difficult to restrict in the early phases of the cyber attacks, Cyber attacks may have some motivation behind it or may be processed unknowingly. The attacks those are processed knowingly can be considered as the cyber crime and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense etc.

In the current era of online processing, maximum of the information is online and prone to cyber threats. There are a huge number of cyber threats and their behavior is difficult to early understanding hence difficult to restrict in the early phases of the cyber attacks. Cyber attacks may have some motivation behind it or may be processed unknowingly.

The attacks those are processed knowingly can be considered as the cyber crime and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense etc. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society.

Some of the kinds of Cyber-criminals are mentioned as below.

Some of the kinds of Cyber-criminals are mentioned as below.

-  **Crackers** These individuals are intent on causing loss to satisfy some antisocial motives or just for fun.
-  **Hackers** These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers.
-  **Pranksters** These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.
-  **Career criminals** These individuals earn part or all of their income from crime.
-  **Cyber terrorists** There are many forms of cyber terrorism

□ Crackers: These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.

□ Hackers: These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.

□ Pranksters: These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.

□ Career criminals: These individuals earn part or all of their income from crime, although they Malcontents, addicts, and irrational and incompetent people: "These individuals extend from the mentally ill do not necessarily engage in crime as a full-time occupation. Some have a job, earn a little and steal a little, then move on to another job to repeat the process. In some cases they conspire with others or work within organized gangs such as the Mafia. The greatest organized crime threat comes from groups in Russia, Italy, and Asia. "The FBI reported in 1995 that there were more than 30 Russian gangs operating in the United States. According to the FBI, many of these unsavory alliances use advanced information technology and encrypted communications to elude capture".

□ Cyber terrorists: There are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of like-minded Internet users who crash a website by flooding it with traffic. No matter how harmless it may seem, it is still illegal to those addicted to drugs, alcohol, competition, or attention from others, to the criminally negligent.

□ Cyber bulls: Cyber bullying is any harassment that occurs via the Internet. Vicious forum posts, name calling in chat rooms, posting fake profiles on web sites, and mean or cruel email messages are all ways of cyber bullying.

□ Salami attackers: Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into bank's servers, which deducts a small amount from the account of every customer. In general cyber crimes can be categorized as follows- Data Crime

a. Data Interception

An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack

usually involves sniffing network traffic, but may include observing other types of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. However, in all variants of this attack, and distinguishing this attack from other data collection methods, the attacker is not the intended recipient of the data stream. Unlike some other data leakage attacks, the attacker is observing explicit data channels (e.g. network traffic) and reading the content. This differs from attacks that collect more qualitative information, such as communication volume, not explicitly communicated via a data stream.

b. Data Modification

Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites.

In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. An example of this is changing the dollar amount of a banking transaction from \$100 to \$10,000.

In a replay attack, an entire set of valid data is repeatedly interjected onto the network. An example would be to repeat, one thousand times, a valid \$100 bank account transfer transaction.

c. Data Theft

Term used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information

is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law.

Network Crime

a. Network Interferences

Network Interfering with the functioning of a computer Network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing Network data.

b. Network Sabotage

'Network Sabotage' or incompetent managers trying to do the jobs of the people they normally are in charge of? It could be the above alone, or a combination of things. But if Verizon is using the help the children, hindering first responders line then they might be using network problems as an excuse to get the federal government to intervene in the interest of public safety. Of course if the federal government forces these people back to work what is the purpose of unions and strikes anyway [6].

Access Crime

a. Unauthorized Access

"Unauthorized Access" is an insider's view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality.

b. Virus Dissemination

Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are examples of malicious software that destroys the system of the victim.

Related Crimes

a. Aiding and Abetting Cyber Crimes

There are three elements to most aiding and abetting charges against an individual. The first is that another person committed the crime. Second, the individual being charged had knowledge of the crime or the principals' intent.

Third, the individual provided some form of assistance to the principal. An accessory in legal terms is typically Hemraj Saini, Yerra Shankar Rao, T.C.Panda / International Journal of Engineering Research defined as a person who assists in the commission of a crime committed by another or others. In most cases, a person charged with aiding and abetting or accessory has knowledge of the crime either before or after its occurrence. A person who is aware of a crime before it occurs, and who gives some form of aid to those committing the crime, is known in legal terms as an "accessory before the fact." He or she may assist through advice, actions, or monetary support. A person who is unaware of the crime before it takes place, but who helps in the aftermath of the crime, is referred to as an "accessory after the fact".

b. Computer-Related Forgery and Fraud: Computer forgery and computer-related fraud constitute computer-related offenses.

c. Content-Related Crimes: Cyber sex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses.

The total cost to pay by victims against these attacks is in millions of millions Dollar per year which is a significant amount to change the state of undeveloped or under-developed countries to developed countries. Some of the facts related to cyber crimes can be significantly marked by the information provided by a US base news agency.

Ex.1. Answer the questions:

- 1.What different types of Cyber-criminals are mentioned in the work?
2. What types of cyber crimes can be categorized as data crimes? Give examples.

3. What term is used to describe when information is illegally copied or taken from a business or other individual?
4. What is it a data modification attack?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. In the current era, most information is stored online and therefore vulnerable to cyber threats.
2. Cyber threats are easy to understand and restrict in their early stages.
3. All cyber attacks are considered cyber crimes.
4. Crackers usually act with antisocial motives or just for fun.
5. Hackers always break into systems with criminal intent.
6. Pranksters cause long-term damage through cybercrime.
7. Career criminals earn all their income from cybercrime.
8. Russian organized crime groups use advanced IT and encrypted communication to avoid detection.
9. Cyber terrorists always work alone and never operate in groups.
10. Cyber bullying includes sending cruel emails and creating fake profiles online.

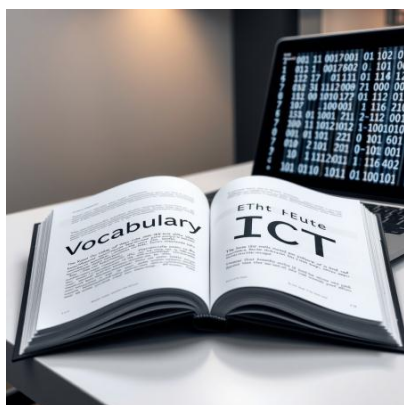
Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.alter			

2. tamper			
3. repeat			
4.engage			
5.gain			
6. modify			
7. assist			

Text 15



Study this vocabulary:

sensor — датчик

share data – совместно использовать ресурс;
делиться данными

scam – надувательство, обман

illegal transactions – незаконные сделки

identify risk – распознать риск

hack into – взламывать; проникать

Impacts of Cyber-Crime

Lunda Wright, a legal researcher specializing in digital forensic law at Rhodes University, has an interesting research finding on a blog posted in October 2005. It states that there has been an increased rate of prosecutions of cyber-criminals. There has been an increased clamping down on cyber-piracy related to the film and music works. There are novel lawsuits and strategies for litigation. There is a greater dependence on the skills of computer forensic experts in corporations and government. Finally, there is an increase in inter-government cooperative efforts.

Organized crime groups are using the Internet for major fraud and theft activities. There are trends indicating organized crime involvement in white-collar crime. As criminals move away from traditional methods, internet-based crime is becoming more prevalent. Internet-based stock fraud has earned

criminals millions per year leading to loss to investors, making it a lucrative area for such crime. Police departments across the nation validate that they have received an increasing number of such crimes reported in recent years. This is in sync with the national trend resulting from increased computer use, online business, and geeky sophisticated criminals. In the year 2004, cyber-crime generated a higher payback than drug trafficking, and it is set to grow further as the use of technology expands in developing countries. Scott Borg, director of the U.S. Cyber Consequences Unit, an agency supported by the U.S. Department of Homeland Security, recently indicated that denial-of-service attacks won't be the new wave of future. The worms, viruses are considered not quite mature' as compared to the potential of attacks in future.

Impacts of Cyber-Crime

- Increased rate of prosecutions of film and music
- Novel lawsuits and strategies for litigation
- Greater dependence on computer forensic
- Increase in inter-government cooperative efforts
- Organized crime involvement in white-collar crime
- Internet-based stock fraud earning millions per year
- Increasing number of crimes reported to police
- Cyber-crime generated higher payback than drug trafficking in 2004



Potential Economic Impact

- Over 74 million U.S. victims in 2010
- \$32 billion in financial losses
- 69% of online adults have been victims

Cyber-crime generated higher payback

Potential Economic Impact

The 2011 Norton Cyber crime disclosed that over 74 million people in the United States were victims of cyber crime in 2010. These criminal acts resulted in \$32 billion in direct financial losses. Further analysis of this growing problem found that 69 percent of adults that are online have been victims of cyber crime resulting in 1 million cyber crime victims a day. Many people have the attitude that cyber crime is a fact of doing business online.

As today's consumer has become increasingly dependent on computers, networks, and the information these are used to store and preserve, the risk of being subjected to cyber-crime is high. Some of the surveys conducted in the past have indicated as many as 80% of the companies' surveyed acknowledged financial losses due to computer breaches. The approximate number impacted was \$450 million. Almost 10% reported financial fraud

Each week we hear of new attacks on the confidentiality, integrity, and availability of computer systems. This could range from the theft of personally identifiable information to denial of service attacks.

As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy.

The disruption of international financial markets could be one of the big impacts and remains a serious concern. The modern economy spans multiple countries and time zones. Such interdependence of the world's economic system means that a disruption in one region of the world will have ripple effects in other regions. Hence any disruption of these systems would send shock waves outside of the market which is the source of the problem.

Productivity is also at risk. Attacks from worms, viruses, etc take productive time away from the user. Machines could perform more slowly; servers might be inaccessible, networks might be jammed, and so on. Such instances of attacks affect the overall productivity of the user and the organization. It has customer service impacts as well, where the external customer sees it as a negative aspect of the organization.

In addition, user concern over potential fraud prevents a substantial cross-section of online shoppers from transacting business. It is clear that a considerable portion of e-commerce revenue is lost due to shopper hesitation, doubt, and worry. These types of consumer trust issues could have serious repercussions and bear going into more detail.

Ex.1. Answer the questions:

1. What do organized crime groups use the Internet for?
2. Has there been an increased clamping down on cyber-piracy related to the film and music works?
3. Why is the high risk of being subjected to cyber-crime?
4. The economy is exposed to all the threats posed by cyber-criminals. Give some reasons why?
5. Why does the disruption of international markets remain a serious concern?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Lunda Wright is a legal researcher at Rhodes University who studies digital forensic law.
2. Internet-based crime is becoming less common as criminals continue to use traditional methods.
3. There has been an increased rate of prosecutions of cyber-criminals.
4. The text says that cyber-piracy related to film and music works is being ignored by authorities.

5. Litigation strategies for dealing with cybercrime are no longer evolving.
6. Computer forensic experts are becoming less important to corporations and government agencies.
7. International cooperation against cybercrime is decreasing.
8. Organized crime groups are not involved in cybercrime.
9. In 2004, cybercrime generated less income than drug trafficking.
10. Scott Borg believes denial-of-service attacks will be the most advanced form of cybercrime in the future.

Ex. 4. Write down ten word-combinations with a verb.

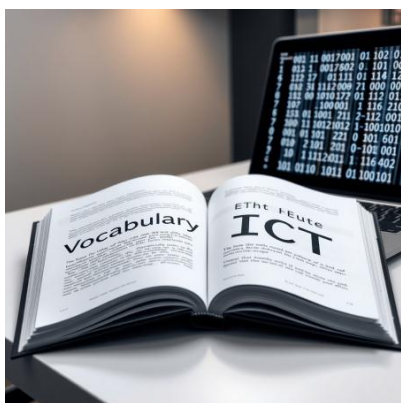
Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.send			
2. jam			
3. bear			
4.disrupt			
5.lose			
6. impact			
7. acknowledge			

UNIT 10. Information and telecommunication computer technologies in investigating crimes



Text 1



Study this vocabulary:

cutting-edge software - передовое программное обеспечение

iris recognition - распознавание радужной оболочки глаза

facial recognition - распознавание лиц

positioning systems - система навигации и определения положения

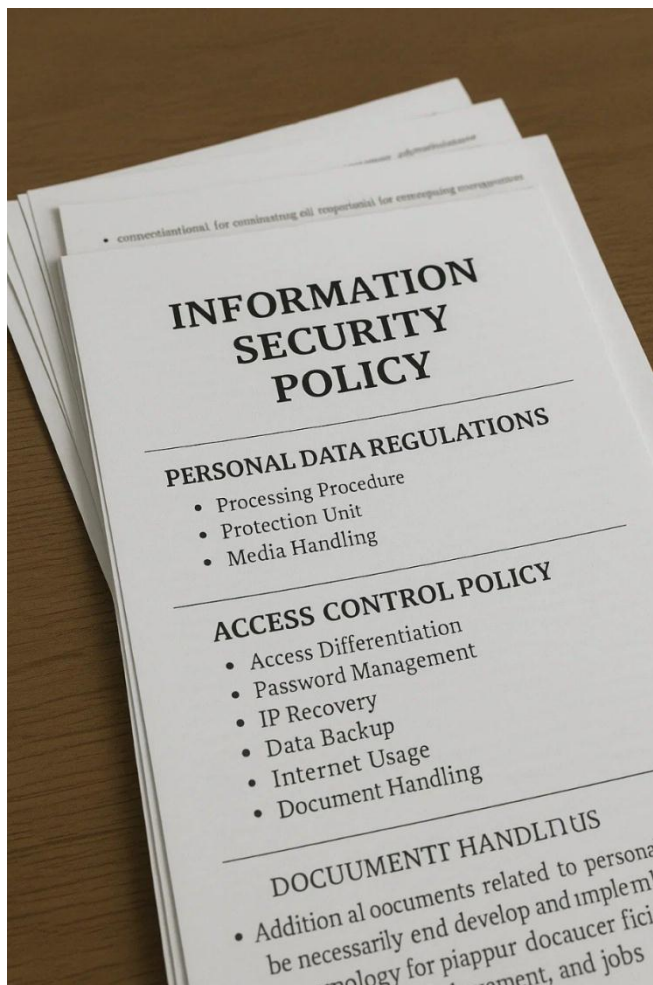
surveillance cameras - камера видеонаблюдения, слежения

For any company, the implementation of an infrastructure technical security system begins with the adoption of a package of applied organizational measures. The main document will be the Information Security Policy, many internal regulations can be developed as appendices to it. It is not recommended

to issue documents as appendices, the development of which is regulated by the need to protect personal data and comply with the requirements of the regulator.

Inspection organizations request separate documents:

1. Regulation on the procedure for processing personal data.
2. Regulations on the unit entrusted with the protection of personal data.
3. Other documents, in particular, the journal of the movement of removable media.



Their absence can lead to fines. In addition to the documents related to personal data, it is necessary to develop and implement:

- a policy of control and prevention of an unauthorized access to information and infrastructure facilities;
- methodology for determining the degree of access differentiation;
- password management regulations, providing for ensuring their complexity, timely replacement, responsibility for

the transfer;

- IP recovery policy after accidents, indicating the time periods necessary for it;
- data backup policy with indication of their volume, frequency of copying, storage location;
- methods of working with the Internet and software installation policy;
- policy on working with paper documents (printing, copying, scanning);

- regulations on divisions and job descriptions of employees.

The staff must be familiar with the documents. They should be stored in a place accessible for review, for example, on the company's server.

Ex.1. Answer to the following questions:

1. What does public safety require?
2. What is the security of information technologies in the field of law enforcement becoming?
3. What is the interest of the criminal world in obtaining information about the actions of law enforcement officers expressed in?
4. What tasks of information security is it necessary to solve?
5. What is used to solve the problems of ensuring the security of information technologies in the law enforcement sphere?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Implementation of a technical security system begins with organizational measures.
2. The main document in information security is the Employee Handbook.
3. Internal regulations can be developed as appendices to the Information Security Policy.
4. It is recommended to issue all internal documents as appendices, including those related to personal data protection.
5. Inspection organizations may request separate documents like the Regulation on processing personal data.
6. Companies do not need a special regulation on the unit responsible for data protection.
7. Absence of required documents can lead to fines.
8. There is no need for a password management policy.

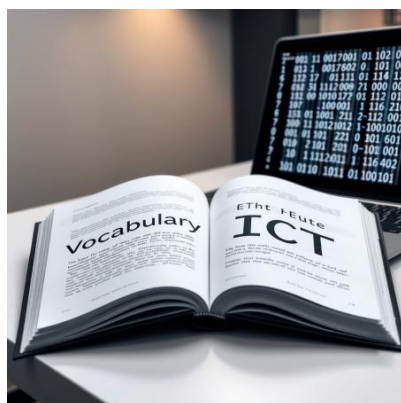
9. A data backup policy should specify volume, frequency of copying, and storage location.
10. Employees do not need to know about security documents.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.issue			
2. regulate			
3. comply			
4.work			
5.determine			
6. ensure			
7. store			

Text 2



Study this vocabulary:

have access to the genetic data - иметь доступ к генетической базе данных

in a targeted way - целенаправленно

a false sense of security – ложное чувство безопасности

from number-plate recognition cameras - с камер, считывающих (распознающих) номерные знаки

infrared night vision capability - оборудование инфракрасного ночного видения

Engineering and Technical Measures of Security systems

Engineering measures are a set of special bodies, technical means and activities that work together to perform a specific task of protecting information. Engineering means include shielding the premises, organizing an alarm system, and guarding the premises from a PC.

Technical means of protection include hardware, software, cryptographic means of protection, which make it difficult to attack, help to detect the fact of its occurrence, to get rid of the consequences of the attack.

Technical means of security subsystems of modern distributed information systems perform the following main functions:

- authentication of partners in the interaction, allowing to verify the authenticity of the partner when establishing a connection;

- authentication of the source of information, which allows to verify the authenticity of the source of the message;

- access control providing protection against unauthorized use of resources;

- data confidentiality, which provides protection against unauthorized receipt of information;

- data integrity, which allows detecting and, in some cases, preventing information from changing during its storage and transmission;



- affiliation that provides proof of ownership of information to a particular person.

To implement these functions, the following mechanisms are used:

- encryption, which transforms information into a form that cannot be understood by unauthorized users;

-electronic digital signature transferring the properties of a real signature to electronic documents;

-access control mechanisms that control the process of access to user resources based on information such as access control databases, passwords, security labels, access time, access route, access duration;

-integrity control mechanisms that control the integrity of both the individual message and the message flow and use for this purpose checksums, special labels, message sequence numbers, cryptographic methods;

-authentication mechanisms that, based on user-supplied passwords, authenticating devices or his biometric parameters, decide whether the user is who he is;

-traffic enhancement mechanisms that add additional information to the message flow that “masks” useful information from the attacker;

-notarization mechanisms that serve to authenticate the source of information.

Ex.1. Answer to the following questions:

1. What are engineering measures?
2. What do engineering means include?
3. What do technical means of protection include?
4. What functions do technical means of security subsystems of modern distributed information systems perform?
5. Which mechanisms are used to implement these functions?

Ex. 2. Make four alternative questions based on the text.

Ex. 3. True or false?

1. Engineering measures include special bodies, technical means and activities aimed at protecting information.
2. Engineering means of protection do not include shielding premises or alarm systems.

3. Technical means of protection consist only of software tools.
4. One of the functions of technical security means is authentication of partners during interaction.
5. Data confidentiality refers to protection against unauthorized modification of data.
6. Data integrity means detecting and preventing changes to information during storage and transmission.
7. Authentication of the source of information helps to verify who sent the message.
8. Access control prevents unauthorized users from using system resources.
9. Encryption makes information easy for anyone to read.
10. Electronic digital signature serves only to encrypt messages.

Ex. 4. Write down ten word-combinations with a verb.

Ex. 5. Make a table of the four forms of the verb and fill it with examples from the text.

Infinitive (Base Form)	Past Simple	Past Participle	Present Participle / -ing
1.shield			
2. organize			
3. detect			
4.transform			
5.base			
6. check			
7. implement			

REFERENCES

1. Алешугина Е. А., Профессионально ориентированный английский язык для специалистов в области информационных технологий [Текст]: учеб. пособие. / Е. А. Алешугина, Д. А. Лошкарева; Нижегород. гос. архитектур.- строит. ун - т – Н. Новгород: ННГАСУ, 2020. – 104 с.
2. Зарубежная практика правоохранительной деятельности в борьбе с киберпреступлениями как инструментом современного терроризма : учеб.пособие / сост.: В. А. Гончарова, С. В. Борисова. - Краснодар : Краснодарский университет МВД России, 2020. - 144 с. - ISBN 978-5-9266-1642-9 : 86.17 р. - Текст : непосредственный + Текст : электронный. - <http://ebs.libkrumvd.ru/elib/5938/>, требуется авторизация
3. 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.
4. Мартынова Е.В. Active reading for students of IT and Computing / Е.В. Мартынова – Казань: Казан. ун-т, 2016. – 56 с.
5. Active_reading_for_students_of_IT_and_Computing_Martynova_E.V..pdfhttps://dspace.kpfu.ru/xmlui/bitstream/handle/net/107896/Active_reading_for_students_of_IT_and_Computing_Martynova_E.V..pdf?sequence=1
6. Радовель В. А. Р 15 Английский язык. Основы компьютерной грамотности: Учебное пособие / Радовель В. А. — Изд. 3-е. — Ростов н/Д: Феникс, 2006. — 224 с. — (Сам себе репетитор). ISBN 5-222-09193-7. - Текст: непосредственный.
7. Учебник английского языка: Информационная безопасность = English for Students of Information Security / О.В. Куликова. – М.: Издательство «Аспект Пресс», 2020. – 432 с.

APPENDIX 1

Phrases which help you to make a presentation:

Introduction

- -Good morning, everybody! (ladies and gentlemen).
- -Let me introduce myself. My name is.../I am a first year law student.
- -The topic of my presentation is.../Today I would like to tell you about...
- -I have chosen this topic because..., / The purpose of my presentation is to inform/ to persuade...
- -The form of my presentation is .../The body of my presentation consists of... parts.
- -It will take only 5-7minutes of your time.

2. Body

- -First..
- -I have divided my presentation into 2-3 parts.
- -Then... -After that I'd like to move on to... /-Next I'd like to move on to... /- Finally I'd like to move on to...

3. Conclusion

- -Let us summarize briefly what we have looked at.
- -Let us briefly summarize the main issues.
- -In conclusion I want to say. • -That is the end of my presentation.
- -Thank you for your listening/attention.

4. Inviting questions

- -You are welcome with your questions.
- -I am ready to answer any of your questions.
- -Could you repeat your question?
- -I am sorry, but I didn't follow your question.
- -If there are no more questions thank you again for your attention.

APPENDIX 2

Structure of an essay:

- Title
- Introduction
- Main part
- Conclusion

Useful phrases

Giving opinion:

I agree/ disagree

In my opinion, ... / From my point of view, ... / As far as I am concerned, ...

I believe that.../ It seems to me that...

I am in favour of... / I am against the idea of...

According to...

Some people say that...

It is said/believed that...

There is no doubt that...

It cannot be denied that...

It goes without saying that...

We must admit that...

Giving arguments:

The main argument against/in favour is...

First of all, I would like to consider...

The first thing I would like to consider is...

To begin with, .../ To start with, ...

Despite the fact that.../ In spite of the fact that...

On the one hand, ... /On the other hand, ...

Besides,.../ In addition,...

What is more, .../ Moreover, .../ More than that, ...

Finally, ...

However, ... / ..., though

...although...

Nevertheless,...

Logical links:

for this reason

therefore/that is why

thussth happened because of/as a result of/owing to/due to/as a consequence of

Examples:

For example

For instance

Such as

Like

Conclusion:

To sum up, ...

To conclude,

I would argue that...

On this basis, I can conclude that...

In conclusion, I would like to stress that...

All in all, I believe that...

APPENDIX 3

Plans for Rendering an Article:

I.

1. The title of the article.
2. The author of the article; where and when the article was published.
3. The main idea of the article.
4. The contents of the article. Some facts, names, figures.
5. Your opinion of/on the article.

1.

- a) The article is headlined
- b) The headline of the article I have read is ...

2.

- a) The author of the article is ...
- b) The article is written by ...
- c) It is (was) published in ...
- d) it is (was) printed in ...

3.

- a) The main idea of the article is ...
- b) The article is about ...
- c) The article is devoted to ...

- d) The article deals with ...
- e) The article touches upon ...
- f) The purpose of the article is to give the reader some information on ...
- g) The aim of the article is to provide the reader with some facts/material/data on ... 4.
- a) The author starts by telling (the reader) (about, that ...)
- b) The author writes (states, stresses upon, thinks, points out) that ...
- c) The article describes ...
- d) According to the text ...
- e) Further the author reports (says) that ...
- f) The article goes on to say that ...
- g) In conclusion ...
- h) The author comes to the conclusion that

5.

- a) I find/found the article topical=urgent (interesting, important, dull, of no value, too hard to understand ...) because
- b) In my opinion the article is worth reading because

II.

- 1. Some words about the author.
- 2. The main idea of the book (if you know).

(+ theme, problem)

3. The main idea of the extract (chapter).
4. The key of the passage.
5. A form of narration.
6. Choice of words.
7. The main characters of the extract.
8. The way of character drawing.
9. Retelling of the text with stylistic devices analysis.
10. Your own attitude to the chapter and to the main idea discussed in the passage.

APPENDIX 4

English-Russian Dictionary

A

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

a wide-area network (WAN) – глобальная компьютерная сеть

a zero day vulnerability – уязвимость нулевого дня

abacus — счеты

ability — способность, возможность

abolish — отменять, исключать

absolute - абсолютная величина

abuse – оскорбления

accept the risk - принять риск

acceptable - допустимое значение

acceptable level – приемлемый уровень

access ~ уровень доступа

access control - контроль доступа

access the Internet – иметь доступ в Интернет

access — доступ, обращение; обращаться, иметь доступ

accessibility program – программа доступности

accessible — доступный

accessories — реквизиты

accessory equipment — вспомогательные устройства

accomplish — завершать, заканчивать

accomplishment — завершение; выполнение

according — соответствующий

accordingly — соответственно, соответствующим образом

account — расчет, подсчет, счет (банковский); учитывать, подсчитывать

accountability - подотчетность

accounting - процедура учета

accumulate — накапливать (ся), суммировать, собирать

accumulator — сумматор; накапливающий регистр; устройство суммирования

accuracy — точность; правильность; четкость

accurate — точный, правильный

achieve — достигать, завершать

achievement — достижение, завершение

acquire — приобретать, получать

acquisition — приобретение, получение

act — действовать, работать

action — действие, работа, операция

activity — деятельность

actual content – действительный (текущий) контент

adapt — адаптировать(ся); настраивать(ся); приспособливаться

adapter — адаптер

adapter — терминальный адаптер

mode — терминальный режим

add — сложение, суммирование

additional - добавочная память

address - адресный регистр

adjacent — смежный; соседний; примыкающий

adjust — регулировать; настраивать

adjuster — регулятор

adjustment — регулировка; настройка; корректировка; подгонка; поправка

administrative control - административный контроль

advance — продвигаться(ся);

advanced — улучшенный; усовершенствованный; (более) эффективный

advancement — продвижение; улучшение; усовершенствование

advantage — преимущество; выгода

advantage of — воспользоваться

advice — совет; рекомендация

advise — советовать; рекомендовать; консультировать

adviser — консультант; справочник

adware – адвэр; бесплатный программный продукт с размещённой в нём рекламой

affect — влиять; воздействовать

affordable – недорогой, доступный

agenda – повестка дня; планы работ

agree — соответствовать; согласовывать (ся)

agreement — соглашение

aid — помощь; содействие

aids — средства; приспособления

aim — цель; нацеливать, направлять

algorithm — алгоритм

align — выравнивать, выстраивать в линию

allocate — распределять; размещать; предоставлять (доступ)

allocation — распределение; назначение; предоставление

allow — допускать; позволять

allowable — допустимый

all-purpose / general-purpose * универсальный язык

alphabetic - алфавитный порядок

alphanumeric - текстовый терминал

alter — (из)менять(ся)

alter data – изменять данные

alteration — изменение; перемена

alternating - переменная величина

ALU – арифметико-логическое устройство

amend — исправлять; улучшать

amendment — поправка; исправление

analogue technology – аналоговая технология

Analytical Engine – аналитическая машина

annually – ежегодно

an operating system... операционной системы...

antivirus software program – антивирусная программа

Apple's iOS mobile – операционная система iOS для

appliances – бытовые электроприборы

application – приложение, прикладная программа

application software – прикладное ПО

appropriate — подходящий; соответствующий; свойственный; присущий

architecture — архитектура; структура

archive – архив

archiving – архивирование; сохранение

architect — разработчик архитектуры

arithmetic - последовательность арифметических операций

arithmetic and logical ~ арифметико-логическое устройство

armed guards – вооружённые гвардии

arrangement— размещение; расположение; упорядочение; устройство

artificial - искусственный язык

assembler - язык ассемблера

assembly ~ дефект сборки

assembly language – ассемблер (машинно- ориентированный язык низкого уровня)

assign a security classification - присвоить классификацию безопасности

at a time – в то время

at least – по меньшей мере

attach – прикреплять; подключать

attachments – присоединение (приложение) к письму

attachments to email – вложения в электронном письме

authentication - аутентификация (подтверждение подлинности)

authenticity - подлинность, достоверность

authorization- авторизация (разрешение)

authorize - разрешать

authorized user – авторизованный (полномочный) пользователь

automatic scanning – автоматическое сканирование

automatic updates – автоматическое обновление

availability - доступность

available – доступный; готовый к использованию

avoid signature detection —

избегать обнаружения под маскирующими признаками

aware – осведомлённый, знающий

awareness - осознание

В

back up – делать резервные копии

backdoor – «чёрный ход», доступ с чёрного хода

background — фон; предпосылка, основа; подготовка; квалификация; навыки (работы)

background screen – фоновый экран

backup - резервная копия

backup site – резервный узел; резервное производственное помещение

backup unit — устройство получения резервных копий на магнитной ленте

banner ads – баннерная реклама

bar — стержень; полоса; строка

bar-code - устройство считывания штрих-кода

bard-cory - распечатка; данные, выведенные на печать

base — база; основа; основание;

base station – базовая станция

based — основанный

batch — пакет; пакетный файл

batch ~ пакетный файл

BCC (blind carbon copy) – скрытая копия (письма) (отправляемая другому адресату в дополнение к основному, так что другие получатели письма не знают, что этому адресату отправлена копия)

be added – единственное, что нужно добавить..

be authorized - иметь право доступа (к информации)

be caught in the crossfire – оказаться между двух огней

be common - быть общеизвестным

be out of range – быть вне зоны действия (вне диапазона)

benefit from – извлекать пользу или преимущество

binary - двоичная последовательность

binary - двоичное значение

binary ~ двоичная система

binary information – двоичные данные; информация в двоичной форме

bipolar - биполярный полупроводник

bit — бит; двоичный разряд

blackhathacker – “чёрный” хакер

blatantly – демонстративно, откровенно

blood vessels – кровеносные сосуды

Bluebugging – «блюбагинг»; несанкционированная передача или изменение данных, осуществление телефонных звонков и прослушивания

Bluesnarfing – «блюснарфинг»; хакерская атака, использующая технологию Bluetooth для доступа к данным, содержащимся в сотовых телефонах

Bluetooth – Блютус; технология беспроводной ближней связи, позволяющая объединять устройства разных типов для передачи речи и данных

board — панель; пульт; плата

body – текстовая часть письма

boot sector virus – вирус сектора загрузки

bootstrapping — начальная загрузка

branch — ветвь; раздел; отделение; разветвляться; переходить

breach of confidentiality - нарушение конфиденциальности

break - клавиша прерывания

break — разрыв; прерывание; пауза; прерывать; нарушать (работу);

breakdown - отказ, поломка

breakdown — разрушение; поломка

break-in – взлом; взламывать

brief— краткий;

broadband technology – широкополосная технология; технология широкополосных передач

broadcast – транслировать, вещать

browse - кнопка просмотра

browsing — просмотр

buffer — буфер; заносить в буфер

bug — ошибка; дефект; недоработка

bug-free — не содержащий ошибок

bug-test — проверять на наличие ошибок

builder — разработчик; изготовитель; создатель

building — разработка; построение; формирование; создание

bulletin board — электронная доска объявлений

burden — издержки; затраты; обязанности;

bus - гнездо для подключения к шине

bus — шина; канал; линия (передачи данных); соединять шиной

business – (зд.) предприятие, фирма

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

business environment - бизнес среда

business-oriented - язык для (программирования) экономических задач

button — кнопка сброса

by exploiting security flaws – используя изъяны в системе безопасности

by hijacking – (зд.) заманивая

by downloading apps – скачивая приложения и дополнения

byte – байт

С

cable broadband – кабельные широкополосные соединения

data encryption - шифрование данных

data loss – потеря данных

data registry – реестр данных

data safety – безопасность данных

database — база данных; заносить в базу данных

database - базаданных

deal — иметь дело; работать

dealer — посредник; поставщик

debug — отлаживать (программу)

debugger — отладчик

debugging — отладка; наладка

cache — кэш; файл для хранения (данных); хранить; сохранять

calculate — вычислять; рассчитывать

calculating device — вычислительное устройство

calculations – вычисления

calibrate — градуировать; выверять; настраивать

call — вызов; обращение; вызывать; обращаться; называть

call center – телефонный информационный центр

call for — требовать; предусматривать

cancel — отменять; аннулировать; отмена; аннулирование

cancer – онкология

capability – способность, возможность, умение

capacitor — конденсатор

capacity – ёмкость; пропускная способность

capture — собирать (данные); переносить; записывать (в память)

card — плата; карта; карточка

cardfile — картотека

carrier — носитель; держатель; сеть передачи данных

carry — нести; переносить

cartridge — кассета; картридж

cash - кассовый аппарат

cash - кассовый аппарат

cathode-ray tube —электроннолучевая трубка

cause — заставлять; вынуждать; быть причиной; причина; основание

CC (carbon copy) – копия (письма) (отправляемая другому адресату в дополнение к основному, так что всем получателям письма становятся известны адреса друг друга

CD-ROM drive – дисковод для компакт-дисков

CD-RW drive – [многократно] перезаписываемый компакт-диск

cell — ячейка; элемент

cellular connectivity – сотовое подключение

cellular phone – сотовый телефон; мобильный телефон

central processing - центральный процессор

centralprocessingunit (CPU) – центральныйпроцессор

chain — цепь; цепочка; последовательность

challenge — трудность; препятствие; представлять трудность

change — изменение; замена; изменять(ся); сменять(ся)

character - значение кода символа

character - устройство считывания / распознавания знаков

character / string - порядок следования символов

chart — диаграмма; график; схема; таблица;

check - контрольное значение

cholesterol – холестерин

choose — выбирать

chunks of information – куски информации

cipher - шифр

circuit — цепь; контур; электрическая схема

circuitboard – печатная (схемная) плата

circuitry — (электронные) схемы

circumvent – обходить; обманывать; перехитрить

classification label- классификационная метка, знак

classification policy - политика классификации

classified information = – засекреченная информация;

clear — чистый; стертый; удаленный; очищать; стирать; удалять

clearance - допуск к секретной информации

clock – генератор синхроимпульсов; кварц

clock - счетчик времени; таймер

clutter – загромождать

coaxial cable – коаксиальный кабель

code — код; кодировать; программировать; система команд

codify - приводить в систему

coding — программирование

cold (warm, hot) backup site – «холодный» («тёплый», «горячий») резервный узел

collectinformation - собиратьинформацию

color - цветной сканер

column — столбец; колонка; графа

COM or EXE files – файлы с расширением .exe и .com; исполнимые файлы

command / instruction - порядок выполнения команд

command / Instruction - регистркоманд

commercial advertising – коммерческая реклама

commit identity theft – совершать хищение персональных данных

common - распространенная версия

communicate — сообщать(ся); связывать

communication — связь; сообщение; взаимодействие

communication and feedback – коммуникация и обратная связь

communications - архитектура средств связи

companion virus – сопутствующий вирус, вирус-компаньон

comparative — сравнительный

compare — сравнение; сравнивать; соотноситься

comparer / comparator — компаратор; устройство сравнения

compatibility — совместимость

competitive edge – конкурентное преимущество

competitor – конкурент

compiler — компилятор

compiler - язык компилятора

complete — полный; целый; заверченный; завершать; заканчивать

completely — полностью; целиком

compress data – сжимать (уплотнять) данные

compression utility – сервисная программа для сжатия

computation — вычисление; расчет

computational - алгоритм вычислений

compute — вычислять; рассчитывать

computer — компьютер; вычислительная машина

computer crime – компьютерная преступность (преступление)

computer network – компьютерная сеть

computer security - компьютерная безопасность

computer system failure – авария компьютерных систем

computer telephony integration – компьютерная телефония (интеграция телефонных систем с компьютерами)

computer virus – компьютерный вирус

computer/server malfunction - неисправность компьютера/сервера

computing - вычислительное устройство

computing facilities - вычислительные средства

concept — понятие; принцип; концепция

concern – (зд.) проблема

condition — условие; состояние; режим

confidentiality - конфиденциальность

configure – конфигурировать; задать конфигурацию

confirm — подтверждать

confirmation — подтверждение

connector – соединитель, разъём, коннектор

considerably — значительно

consistency - согласованность

consume — потреблять; расходовать

consumer — потребитель; абонент

consumption — потребление; расход

content – контент, информационное наполнение, содержание; смысл

continued operation – непрерывная работа

continuous - непрерывная величина

contrast — контраст; противоположность

contribute — содействовать; способствовать; вносить вклад

contribution — вклад; содействие

control — управление; регулирование; управлять; регулировать

control system – система контроля и управления

control unit – устройство контроля;; блок управления

controller – микроконтроллер, управляющее устройство

convenience — удобство; пригодность

convenient — удобный; пригодный

conversion — преобразование

convert – преобразовывать

convert — преобразовывать

converter — преобразователь; конвертор

convey — передавать; сообщать

conveying — передача (информации) copy — копия; экземпляр; копировать

copy – копировать

copyrighted software – программы, охраняемые авторским правом

core - оперативная память

core — ядро; оперативная память; суть; основная часть

correct — верный; правильный; нужный; требуемый; исправлять

correct - правильное значение

correction — исправление; устранение (неисправности); коррекция

corrective — корректирующий

corrector — корректор; блок или программа корректирования

corrupt — разрушать; портить; искажать; искаженный

corrupt data – повреждать данные

corrupted — искаженный; запорченный

corruption — разрушение; искажение; порча; повреждение

cost effectiveness - экономическая эффективность

countermeasure - контрмера

coverage area – зона действия сети; диапазон

CPU – центральный процессор

cracker – “крэкер”; взломщик компьютерных систем

crashed disk rescue – восстановление повреждённого диска

cripple – повреждать; приводить в негодность

cross-site scripting virus – межсайтовый скриптинг-вирус

crucial – критический; жизненно-важный

cryptographic key – криптографический ключ

cryptography – криптография

cryptography - криптография, шифрование

customized Web pages – настроенные (заказные)

cybercriminal – киберпреступник

cyber-squatting – «киберсквоттинг»; регистрация доменных имён, содержащих торговую марку, принадлежащую другому лицу с целью их дальнейшей перепродажи или недобросовестного использования

cyberstalking – виртуальное преследование

D

damage — повреждение; разрушение

data — данные; информация

data backup – резервное копирование информации

data center – вычислительный центр

data encryption - шифрование данных

decide — решать; принимать решение

decipher - расшифровывать

decision — решение

decline – снижаться; падать

decode — декодировать

decoder – декодер, дешифратор

decrease — уменьшение; снижение; уменьшать; снижать

decryption - дешифрование

decryption – расшифровка

default — по умолчанию; подразумеваемый; умолчание; стандартный параметр

deficiency — недостаток; нехватка; отсутствие

delay — задержка; запаздывание; задерживать; откладывать

delete — удалять; стирать; очищать

deleter — программа удаления

deletion — удаление; стирание

deliberate attempt – преднамеренная попытка

delivery — подача; доставка; поставка

demagnetize — размагничивать

demand — требование; запрос; требовать; запрашивать

democracy - демократия

denial-of-service - отказ в обслуживании

denial-of-service – отказ в обслуживании

density — плотность

deny the risk - отвергать риск

depend — зависеть от (чего-либо)

depend on – зависеть от чего-либо

dependence — зависимость

dependent — зависимый; зависящий

depending — в зависимости от

deposit — помещать; размещать

depository — склад; хранилище

design — проектирование; конструирование; разработка; построение

design - проектная недоработка

desktop – рабочий стол

desktop computer – настольный ПК

destruction – уничтожение, разрушение

detail — деталь; подробность

detect — обнаруживать; выявлять

detect tampering - обнаружить подделку

detection — обнаружение; выявление

detection mechanism – устройство (способ) обнаружения

detector — детектор; средство обнаружения; датчик

device — устройство; прибор; аппарат; приспособление

diabolical nature – злая, дьявольская сущность

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

Difference Engine – разностная машина

digit – цифра; знак; разряд

digital - числовое значение

Digital Audio Broadcasting – цифровое аудиовещание (стандарт наземного цифрового радиовещания)

digital signature - цифровая подпись

digital subscriber line (DSL) – цифровая абонентская линия

digital technology – цифровая технология

digital transmission methods – способы передач цифровых сигналов

directory – каталог

disaster – бедствие; авария; катастрофа

disaster recovery – восстановление после бедствия

disclosure – раскрытие

discrete - дискретная величина

discretionary approach-дискреционный подход (предоставляемый по усмотрению лица, имеющего соответствующие полномочия)

disk - дисковод

disk - структура диска

display - аппаратные средства вывода на экран

display / video ~ техника отображения; способ вывода на экран

disrupt – нарушать, приводить к срыву

disruption – срыв; нарушение

DNA biochips – ДНК-биочипы; ДНК-чипы; специальные чипы, используемые для выявления генетических мутаций или сдвигов, диагностики заболеваний

DNA computers – ДНК-компьютеры

domain name – имя домена в электронной почте

dormant – бездействующий, неактивный

dot-matrix - точечно-матричный принтер

download — загружать; считывать; считывание (файлов) с сервера

download programs or data – загружать (скачивать) программы или данные

drive — привод; дисковод; запоминающее устройство

drop-down menu – спускающееся (ниспадающее) меню

due to — благодаря; из-за; вследствие

dump — разгрузка; дамп; вывод; разгружать сбрасывать; выводить

duplication — дублирование; копирование

duplicator — копировальное устройство

durable – прочный, долговечный

DVD drive – цифровой многофункциональный диск

DVD-RW drive – цифровой перезаписываемый видеодиск

Е

eavesdrop – подслушивать

edit — редактировать;

editor — редактор; программа редактирования

effect — действовать; оказывать воздействие; влияние; эффект

efficiency — эффективность; коэффициент полезного действия

efficient – эффективный

effort — усилия; работа

eject — выбрасывать; выталкивать; выдавать (данные); выброс;

elaborate — разрабатывать; развивать

elaborate – сложный; усовершенствованный

elaboration — развитие; разработка

electronic - электронная версия

electronic bulletin board – электронная доска объявлений

eliminable — устранимый

eliminate – устранять, ликвидировать

eliminate — устранять; удалять; отменять; ликвидировать

eliminate risk - устранить риск

email address – электронный адрес

email virus – почтовый вирус (передаваемый по электронной почте)

embarrass – приводить в замешательство

emerge - появляться, возникать

emoticon – эмотикон; пиктограмма, изображающая эмоцию

emphasize security – придавать особое значение обеспечению безопасности

employee – служащий; работник

enable – давать возможность; делать возможным

encode = to encipher = to scramble – шифровать, кодировать

encrypt - зашифровать

encryption - шифрование

encryption – шифрование

end ~ клавиша перехода в конец

enforce (confidentiality) - усилить (конфиденциальность)

engine — механизм печати

enter ~ клавиша ввода

ensure – обеспечивать, гарантировать

equal — равный; одинаковый

equality — равенство

equation — уравнение;

equip — оборудовать; оснащать

equipment — оборудование; приборы; аппаратура; (аппаратные)

equipment malfunction – неисправность оборудования

erase - клавиша удаления

erase — стирать; удалять

erase data – стереть данные

erasing — стирание; удаление; очистка

error — ошибка; погрешность

error - скорость исправления ошибок

error - управление обработкой ошибок

error - уровень ошибки

error ~ поиск ошибок

error-correcting - процедура / алгоритм исправления ошибок

escape - клавиша выхода

estimated cost – подсчитанные затраты

ethics - этика

evaluate - оценить

event — событие; случай; исход

examination — исследование; рассмотрение; просмотр; проверка

examine — исследовать; проверять

except for — за исключением

exchange — обмен; замена

exchange — скорость обмена –

executable - исполняемая версия

execute – выполнять, исполнять

execute — выполнять; исполнять

execution — выполнение; исполнение

execution ~ скорость выполнения (программы)

execution sequence – последовательность выполнения программы

executive — диспетчер; управляющая программа; операционная система

exit — выход; выходить

exotic curiosities – экзотическая редкость, диковинка

expand — расширять(ся); увеличивать; наращивать (возможности)

expansion - разъем для модуля расширения

expansion — расширение; увеличение;

expansion ~ дополнительное аппаратное обеспечение

expansion card – плата расширения, расширительная плата

expansion slot – гнездо для платы расширения

experience — опыт; квалификация; испытывать (трудности)

exploit – (зд.) вторжение

exploit computers – использовать в своих интересах; осуществлять компьютерное вторжение

exploit networks – осуществлять вторжение в сети; использовать в злонамеренных целях

exponentiation — возводить в степень

expose – раскрывать, открывать

extend — расширять; удлинять

extended - дополнительная память

extension — расширение; дополнение; удлинение; продление

external - внешняя память

external source – внешний источник

external storage device – устройство внешней памяти, внешнее запоминающее устройство

extract — выделять; извлекать

extraction — извлечение; выборка; выделение

extranet – экстранет

extremely — чрезвычайно; крайне;

F

fabricate — изготавливать

fabrication — изготовление

facilities — оборудование; приспособления; возможности не удаваться

facility — устройство; средство; удобство

failure — отказ; повреждение; дефект; сбой; ошибка; неудача

fall in the range – находиться в диапазоне

fault — неисправность; дефект; отказ; сбой; давать сбой; отказывать

fault - поиск неисправностей

feasibility — возможность; осуществимость; выполнимость

feasible — возможный; выполнимый; осуществимый'

feature – (зд.) функция; характеристика; свойство

feature — свойство; признак; особенность; характерная черта

feed — подавать; питать; заправлять (бумагу); вводить (данные)

feedback — обратная связь

fiber-optic – волоконно-оптический

fiber-optic – волоконно-оптический

field — поле; область; зона; сфера (деятельности)

figure — цифра; число; вычислять;

figure out — вычислять; определять

file — файл; заносить в файл

file virus – вирус, заражающий файл (добавляющий себя к содержимому файла)

firewall – межсетевой защитный экран, брандмауэр

firmware — встроенное программное обеспечение

First Generation phones – телефоны первого поколения

flaw – недостаток, изъян

flexibility — гибкость; адаптируемость; настраиваемость; изменяемость

flexible — гибкий; адаптируемый; настраиваемый; изменяемый

floppy — гибкий диск; дискета

floppy disk drive – дисковод для гибких дисков; флоппи-дисковод

flow — ход выполнения (программы); последовательность; проходить

folder – папка

football scores – результаты футбольных матчей

formatting - процедура / процесс форматирования

formatting - способ форматирования

fraud – мошенничество

fraudulent – обманный, мошеннический

free-running - режим свободного доступа

frequency — частота

front side bus – шина FSB; шина, связывающая процессор с ОЗУ

fulfill — выполнять; осуществлять; завершать

fulfillment — выполнение; осуществление; завершение

fundamental — основной; существенный; фундаментальный;

furnish — поставлять; снабжать

G

gadget — приспособление; вспомогательное устройство

gain — достигать; извлекать пользу; выигрывать; выгода; усиление

gain access – получать доступ

gather — собирать(ся)

general — общий; универсальный;

general-purpose - регистробщегоназначения

generate — генерировать; создавать; производить

generation — создание; формирование; образование; поколение

genuine software – настоящее (подлинное) ПО

get rid of – избавиться от чего-либо

give back — возвращаться

give out — выдавать; предоставлять

give up — отказывать (об устройстве); не справляться; отказываться

go on a rampage – «творить беспредел», бесчинствовать

gov – правительство

GPC navigation – навигация GPS (Global Positioning System); навигация с использованием спутниковой системы

grade — степень; ранг; класс; сорт; упорядочивать; размещать по рангу

grading — классификация; упорядочивание; выравнивание

grantaccess - разрешить доступ

grapher — самописец

graphic / light - световое перо

graphic(al) — графический

graphical / image ~ графический принтер

graphics — графика

groundwork — основа; основание

guard — защита; защищать; предохранять

GUI – графический интерфейс пользователя

guidance — управление; наведение (на цель); руководство

guide — руководство; инструкция; справочник

Н

habit — навык; привычка; свойство

hack into – взламывать; проникать

hand / manual - ручной сканер

handheld computer – карманный (ручной) ПК

handling — обработка; управление; регулирование

hand-operated — управляемый вручную

hand-printed — машинописный

handset – телефон-трубка; мобильная трубка

hang (up) — «зависать»; блокировать

harassment – домогательство, действия досаждающего характера

hard disk – жёсткий диск

hard disk imaging – создание резервного образа диска

hard image – резервный образ диска; образ дисковой памяти

hardware – аппаратное обеспечение; «железо»

hardware - аппаратный уровень

hardware — аппаратура; оборудование; аппаратное обеспечение /средства

hardware - документация по аппаратному обеспечению

hardware - метод аппаратного решения

hardware ~ документация по аппаратному обеспечению

harm — вред; ущерб; повреждение

harmful — вредный

harmless — безвредный (о вирусе)

header – заголовок; верхний колонтитул

heading — заголовок

headset – наушники с присоединённым микрофоном

healthy — исправный; работоспособный (о системе);

help — подсказка; справка; помощь

help - справочное руководство

help ~ файл подсказок

hereafter — далее; в дальнейшем

hereby — таким образом; тем самым

hidden program – скрытая программа

hierarchy — иерархия

high (low)-level language – язык высокого (низкого) уровня

high-capacity — большой емкости

high-capacity - память большой емкости

high-density — с высокой плотностью

high-fidelity (Hi-fi) — с высокой точностью воспроизведения

high-frequency — высокочастотный

high-level - язык высокого уровня

historical - хронологическая последовательность

hold instructions – содержать инструкции

home - клавиша перехода в начало

host – хост – общий термин, описывающий нечто, содержащее ресурс и предоставляющее к нему доступ

host – хост; общий термин, описывающий нечто содержащее ресурс и предоставляющее к нему доступ.

host program – главная (основная) программа

I

IBM – International Business Machines – одна из старейших компьютерных компаний в мире. Мировой лидер в области компьютерных технологий и по объёмам продаж.

icon – иконка, пиктограмма, значок

icon —условный символ; пиктограмма; изображать условно

ICT – информационные и коммуникационные технологии

identification - идентификация

identifier —идентификатор; имя; обозначение

identify — идентифицировать; распознавать; выявлять (ошибку)

identify risk – распознать риск

identity theft – хищение (кража) персональных данных

ignorance — незнание

ignorant — несведущий; не знающий

illegal transactions – незаконные сделки

illicit benefit – незаконнаявыгода

image - качество изображения

imbed — встраивать; внедрять; включать

immunity — невосприимчивость; нечувствительность

impact - воздействие

impact – воздействие

impact" контактный принтер

implement – выполнять, осуществлять, проводить

implement — выполнять; осуществлять

implementation — реализация; осуществление; разработка; внедрение

implementcontrol - осуществлять контроль

implementor — конструктор; разработчик

impostorfiles – обманные файлы

improper — непригодный; недопустимый; неправильный; неподходящий

improve — улучшать; уточнять (данные)

improvement — улучшение; усовершенствование; уточнение (данных)

in - используемый; задействованный

in - последовательно; по порядку

in a - в некотором отношении; до известной степени

in a close proximity – в тесной близости, вблизи

in a nutshell – вкратце; в общих чертах

in any - любым способом; как угодно

in different -s разными способами; по-разному

in great demand – пользоваться большим спросом

In its entirety – во всей полноте; полностью

in the same - так же; таким же образом

in the vicinity – поблизости

in the wild – на практике; практически

in transit – в пути; в процессе передачи

in по - ни в коей мере; никак

inaccurate – неточный

inaccurate — неточный; ошибочный

inadequate — несоответствующий; непригодный; неприемлемый

inbox – входящие сообщения

incapable — неспособный

include — включать; содержать

incompatible — несовместимый

inconsiderable — незначительный

incorporate — включать; содержать; встраивать; внедрять

increase — увеличивать; возрастать; увеличение; повышение

increasing ~ возрастающая последовательность

independent — независимый

indispensable – незаменимый

infect – заражать, инфицировать

infection – заражение

inferior — низший; худший (по качеству)

inflictharm - нанести вред

influence — влияние; воздействие; влиять; воздействовать

information asset - информационный актив

information asset - информационный актив

information security - информационная безопасность

information assurance - гарантия информации

inject – вводить; вставлять; инжектировать

ink-jet * струйный принтер

inoperable – неработающий, нефункционирующий

input ~ входной файл

insert - клавиша вставки

insert a code – вставлять программу

inspection – инспекция: проверка

installation - процедура / процесс установки (системы)

instruction set - структура системы команд

integrate – объединять

integrated circuit – интегральная микросхема

Integrated Services Digital Network – цифровая сеть с комплексными услугами; сеть ISDN

integrity - целостность

Intel – американская корпорация, проектирующая и создающая основополагающие технологии, которые служат фундаментом для вычислительных устройств во всём мире.

interact – взаимодействовать

intercept (information) - перехватывать (информацию)

interconnected – взаимосвязанный

internal ~ внутренняя память

Internet service provider – провайдер услуг Интернета

interpret – интерпретировать; истолковывать

interpreter – интерпретатор; переводчик

interrupt – прерывание; прерываться

into account / consideration – учитывать; принимать во внимание

intranet – интранет

intricate – сложный; запутанный

intruder – злоумышленник; нарушитель

intrusion detection system - система определения вторжения

intrusion detection – обнаружение вторжения

invade – вторгаться; проникать

invalid - неверное, недопустимое значение

invalid – неверный; недопустимый; недействительный; необоснованный

iPhone – айфон

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

it involves downtime – происходит время простоя

item – 1) элемент данных 2) позиция (списка)

J

jack — гнездо

jam — заедание; заклинивание

job — работа; задание; работать

join — соединение; соединять

joystick — джойстик (рычажковое устройство)

JUMP command – команда резкого перехода, броска

junction — соединение; стык

junk email – макулатурная почта; «мусор»

justification — выравнивание (данных); обоснование; доказательство

justify — выравнивать; обосновывать; доказывать; оправдывать

K

keep pace with – неотставать; поспевать

key — клавиша; кнопка; переключатель

keyboard — клавиатура; клавишный

kind — вид; разновидность

know-bow — технология; методика; знания; приемы; жарг. ноу-хау

knowledge — знания; осведомленность

L

lack — отсутствие; недостаток

lagging — отставание; запаздывание

language — язык

laptop – лэптоп; переносной ПК

laser - лазерный принтер

laser - лазерный сканер

latent - скрытый дефект

launch — запускать (программу); вводить в действие

launch attacks – начинать атаки

layout — размещение; распределение

lead [led] — свинец

learn-on-line — обучаться с помощью компьютера

legality - законность

letter — буква; символ

letter-quality - принтер с типографским качеством печати

level — уровень; выравнивать

lifetime — срок службы 1ше — строка; линия; шина; канал

line (at-a-time) - принтер с построчной печатью

link — связь; соединение; связывать; соединять

link – соединять, связывать

list — список; перечень; таблица

locate vulnerabilities – определять местонахождение уязвимостей

location – (определённое) место; место размещения

log - регистрировать(ся)

log file - файл регистрации

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

log system use – регистрировать пользование системой

logic bomb – логическая бомба

logical control - логический контроль

loss of an asset - потеря актива

low-level - язык низкого уровня

LTE – Long Term Evolution – технология построения сетей беспроводной связи поколения, следующего за 3G, на базе IP-технологий, отличающаяся высокими скоростями передачи данных

М

machine language (code) – машинный язык

macro virus – макровирус (распространяемый через макрокоманды)

magnetize — намагничивать

mail — (электронная) почта

mail server – почтовый сервер, сервер электронной почты

mailbox – почтовый ящик электронной почты

mailing list – почтовый список

main — главный; основной

main ~ основная память

maintain — поддерживать; сохранять; эксплуатировать

make - ссылаться; упоминать

make -of— применять; использовать

malcode generator – генератор вредоносного кода

malfunction — сбой; отказ; неисправность; отказывать; давать сбой

malicious intentions – вредоносные (преступные) намерения

malware – вредоносная программа

malware – вредоносный код; вредоносная программа

manage — управлять; организовывать

management — управление; регулирование; организация

manipulate — управлять; манипулировать; обрабатывать

manipulation — управление; работа; обработка; преобразование

manipulator — блок обработки

man-made disaster – техногенная авария (катастрофа)

manual — руководство; справочник; инструкция; описание

manufacture — изготавливать; производить; разрабатывать

manufacturer — изготовитель; производитель; разработчик

mark — признак; метка; знак; помечать; обозначать

measurement — измерение; размер

measuring - измерительная техника

media integration – интеграция средств передачи информации

media player – программа воспроизведения данных мультимедиа; медиа-плеер

medium (pi media) — среда; носитель; средство; способ; средний

meet — удовлетворять (условию); отвечать; соответствовать

meet a specific need – удовлетворять определённые потребности

memory — память; запоминающее устройство

memory - скорость доступа к памяти; скорость выборки

memory (RAM) — память с произвольным доступом

memory / storage ~ регистрпамяти

menu – меню(список команд или вариантов ответа, выводимый программой на экран)

menu bar – полоска (линейка) меню

merge — слияние; объединение; сливать(ся); объединять(ся)

message — сообщение; запрос; посылать сообщение

message digest - краткая, сжатая форма сообщения

metal-oxide - структура металл-оксид полупроводник

meter — измерительный прибор; датчик; счетчик

metering — измерение

mirror image – зеркальный образ

misdirection routine – подпрограмма неправильного указания направления; дезориентации

misleading – вводящий в заблуждение; обманный

mitigate the risk - уменьшить риск

mode — способ; метод; режим

modelling / simulation - язык моделирования

modification – модификация, видоизменение

motherboard – системная (материнская) плата

multilane communications highway – многополосная коммуникационная магистраль

multimedia – мультимедиа; система с комплексным представлением информации

multi-purpose – многоцелевой

multitasking – многозадачность, многозадачный режим

multi-tier classification system - многоступенчатая система классификации

multi-touch screen – мульти-сенсорный экран

N

nanobot – нанобот; нанотехнологический

nanocomputer – нанокomпьютер; компьютер с быстродействием 10 операций в секунду

nanometer – нанометр (1/1000 микрона)

nanotechnology – нанотехнология; технология изготовления и измерения микроскопического размера

natural disaster – стихийное бедствие

need —потребность; необходимость; требовать(ся); быть необходимым

need-to-know principle - принцип необходимости знания информации (получения доступа к информации)

network – (вычислительная, компьютерная) сеть

network - пропускная способность

network - сетевая архитектура

network — сеть; схема; контур

newsgroup – группа новостей; телеконференция

newsgroups – тематические конференции в Интернете

noncomparable — несравнимый

noncompatible — несовместимый

noncomputable — невычисляемый

noncontrollable —неуправляемый

non-discretionary approach - недискреционный подход

non-profit institution – некоммерческая организация

non-repudiation - неотказуемость

notation — запись; представление; обозначение

notepad — блокнот

notes — записывать; регистрировать

number — число; количество; цифра

numeric - числовое значение

numeric — числовой; цифровой

numerical - метод числовых вычислений

numerous — многочисленный

O

objective — цель; целевая функция; требование

observation — наблюдение; отслеживание

observe — наблюдать; следить; соблюдать (правила)

obtain — получать; достигать

occur — происходить; случаться

of	measurement	—	единица	измерения

of	memory	—	блок	памяти

arithmetic - арифметическое устройство

of paramount importance – первостепенной важности

of response — быстрота реакции

on-board — расположенный на плате; встроенный; бортовой

ongoing — продолжающийся; постоянный; непрерывный

on-line — неавтономный; подключенный к компьютеру

online data backup – резервное копирование в системе

onset — начало; ввод в действие

open — открывать; начинать; размыкать

operand - регистр операнда

operating ~ рабочий режим

operating system (OS) – операционная система

operating system мобильных устройств фирмы Apple

operation - руководство по эксплуатации

operational - работающее устройство

optical / visual - оптический сканер

origin – начало; происхождение

original - первоначальный вариант

out of - не по порядку

outline — контур; очертание; схема; план; краткое изложение

out-of-order — неисправный

output — вывод; выход; устройство вывода; выводить

output – выводить (данные)

outsider – постороннее лицо

overlook - упустить из виду

Р

package — пакет; блок; модуль

packaged software — готовое программное обеспечение

page (at-a-time) ~ принтер с постраничной печатью

page up ~ клавиша листания назад

page-down - клавиша листания вперед

parental controls – родительский контроль

partition – раздел (диска)

password – пароль

password — пароль

patch – «заплата», вставка в программу с целью исправления или изменения

patch – исправлять программу с помощью подпрограммы

path – путь, маршрут

pattern — шаблон; образец; форма

pause ~ клавиша останова (паузы)

payload – (зд.) вредоносная нагрузка, вредоносное информационное наполнение

PDA – Personal Digital Assistant – КПК; персональный цифровой секретарь
– тип сверхлёгкого миниатюрного ПК

penetrate – проникать

perform — выполнять; осуществлять; работать; действовать

performance — (рабочая) характеристика; производительность;

performance - степень быстродействия

peripheral – периферийное устройство

permanent – постоянный

personal area network – персональная (личная) сеть

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

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

phishing – фишинг; способ незаконного получения важных сведений путём отправки подложных электронных сообщений

phone carrier – поставщик услуг коммуникаций по телефонным линиям

phone plugs – телефонные разъёмы

phonebook – телефонная книга

physical control - физический контроль

pictorial / picture ~ графическое представление

piracy – компьютерное пиратство

plethora of attacks – огромное количество атак

plotting tables — графические планшеты

plug – подключать

pointer – указатель; адресная ссылка

pointer — указатель; стрелка

point-of-sale - кассовый терминал

polymorphic genetics – полиморфные (самоизменяющиеся) вирусы

polymorphic toolkits – полиморфные экземпляры

polymorphic virus – полиморфный (самоизменяющийся) вирус

pop-up – всплывающий элемент

pop-up blocker – блокировщик всплывающих окон

port – порт (устройство, с помощью которого компьютер соединяется с периферией)

portable / removable - съемный носитель

pose a threat – представлять угрозу

possession - владение, обладание

post evidence – отправить доказательства

potent — могущественный; мощный; убедительный

power — мощность; энергия; питание

power (supply) - блок питания

power failure – нарушение электроснабжения

power outage - отключение эл. питания

power outage – отключение электроэнергии

power-line Internet – Интернет по линиям электропередач

predefined symbols — заранее заданные символы

predict — предсказывать; прогнозировать

predominant — преобладающий

predominate — преобладать; доминировать

prepare — подготавливать; составлять

presentation ~ уровень представления

pressure — давление

prevent – предотвращать, предупреждать

prevent — предотвращать; предохранять препятствовать

prevention — предотвращение; предупреждение

primarily — главным образом; преимущественно; в основном

principle of least privilege - принцип наименьших привилегий

print — печатать; выводить на экран

print out — распечатка; вывод на печать или экран

printed receipt - напечатанный чек

printer — принтер; печатающее устройство

printer - средство вывода на печать

privacy — индивидуальная сфера жизни

private (information) - частная, личная (информация)

procedural handling control - контроль за процедурой обращения (с информацией)

procedure — процедура; процесс; метод; алгоритм

process — обрабатывать

process information - обрабатывать информацию

processing — редактирование текстов

processing - устройство обработки; процессор

processing program — текстовый редактор

processor — быстродействие процессора

processor — процессор

productivity - производительность

productivity – производительность; продуктивность

professional developer – профессиональный разработчик

programming - режим программирования

programming / development ~ язык программирования

programming language – язык программирования

propagate – размножаться, распространяться

protection / security - уровень / степень защиты

protection requirements - требования защиты

protective measures – меры защиты

public (information) - для всеобщего пользования, общедоступная (информация)

public key - открытый ключ

public key encryption - шифрование с открытым ключом

pull-down menu – опускающееся, вертикальное меню

Q

qbits (quantum bits) – квантовый бит

quality — качество; свойство; характеристика

quantity — количество; число; величина; значение

quantum computer – квантовый компьютер

quarantine – подвергать карантину; изолировать

query – запрос;

quit — выход (из программы); выходить (из программы)

quitting — выход (из программы)

R

radio waves – радиоволны

raid – рейдерски захватывать; грабить

raise — поднимать; повышать; увеличивать; подъем; повышение

RAM (random access memory) – оперативное запоминающее устройство (с произвольной выборкой)

random - случайный сбой /ошибка

random — случайный; произвольный

random-access - (RAM) — оперативное запоминающее устройство (ОЗУ)

range — диапазон; область; интервал

range – колебаться

range – радиус действия

rate — степень; скорость

reader - считывающее устройство

reading — чтение; считывание

read-only - (ROM) — постоянное запоминающее устройство (ПЗУ)

read-only - режим доступа к данным без возможности их изменения

reason — причина; основание; довод; обосновывать; заключать

reasonable — разумный; допустимый

reassessment - переоценка

receive — принимать; получать

receiver — приемное устройство

recipient – получатель, адресат

recognition — распознавание образов

record — запись; регистрация; записывать; регистрировать

recorder — устройство / программа регистрации; самописец

recovery — восстановление файла

recreate – воссоздавать

red — катушка; бобина

reduce — уменьшать; сокращать; понижать; сжимать

reduce risk - уменьшить риск

reduction — уменьшение; сокращение; понижение; сжатие (данных)

reel — катушка; бобина

reference — ссылка; сноска; справочник; руководство

referenced — вызываемый; указываемый

regardless — несмотря на; независимо от

register — регистр; устройство регистрации; счетчик; датчик

release – (зд.) версия

release – выпускать; ставить

reliable – надёжный

remote - удаленный терминал

remote storage facility = off-site storage facility –
удалённое хранилище данных

remotely – дистанционно, удалённо

removable – съёмный

remove — удалять; устранять; убирать

rename — переименовывать

replace – заменять

replace — заменять; замещать

replacement — замена; замещение; смена; подстановка

replica – точная копия

replicate – тиражировать, копировать

represent — представлять representation — представление

reproduce – воспроизводить

reproduction routine – подпрограмма воспроизведения

require — требовать

requirement — требование; необходимое условие; потребность

reseal (a letter) - запечатывать снова (письмо)

research — исследование; изучение; исследовать

reset - кнопка сброса

reset — сброс; восстановление; возврат в исходное состояние;

residualrisk - остаточныйриск

respect — отношение; учитывать; принимать во внимание; соблюдать

respond to – реагировать, отвечать (на что-либо)

response - ответ, отклик

responsibility - ответственность

restore – восстанавливать

restricted (information) - для ограниченного пользования (информация)

result in – кончаться, иметь результатом

risk assessment - оценкариска

risk evaluation - оценкариска

riskmanagement - управлениерисками

roaming – роуминг

ROM (read only memory) – постоянноезапоминающееустройство

routine — (стандартная) программа / операция; (установленный) порядок

routine – подпрограмма

ruggedness — прочность

rule — правило; управлять; руководить

ruler — (масштабная) линейка

run — выполнять, запускать (программу); работать; запуск; прогон;
выполнение

run a program – запускать программу

running — запуск; выполнение; работа

running ~ рабочая характеристика

run-time version — исполняемая версия

S

safe — безопасный; надежный

safety — безопасность; надежность

save — сохранять; сберегать

scale — шкала; масштаб

scaling — масштабирование

scam – надувательство, обман

scan — просмотр; сканирование; развертка; просматривать

scanner — сканер; устройство оптического считывания

scanning — просмотр; поиск; развертка; считывание; сканирование

schedule — план; расписание; график

scheduled – предусмотренный расписанием; запланированный

scheduling — составление расписания или графика; планирование

science — наука; теория

scientific — научный

scramble information - зашифровывать информацию

scripting language – скриптовый язык, язык подготовки сценариев

secondary ~ вторичная память

security ~ средство защиты

security breach – (зд) взлом системы безопасности

security implications – последствия нарушения безопасности

security and reliability of information systems

безопасность и надежность информационных систем

security design and implementation - проектирование и осуществление безопасности

security management - управление безопасностью

seize control – захватить контроль

selectivity — избирательность

self-contained – самостоятельный; самодостаточный

self-explanatory – самообъясняющий; информативный

semiconductor — полупроводник

sensibility — чувствительность

sensitive — чувствительный

sensitive (information) - деликатная, конфиденциальная (информация)

sensitive information секретные сведения

sensor — датчик

separate — отделять(ся); отдельный; изолированный

separation — разделение; отделение

separation of duties - разделение обязанностей

sequence — последовательность

serve — обслуживать; служить

server — сервер; обслуживающая / сервисная программа

service — обслуживание; услуги;

set off the alarms – запускать сигналы тревоги

shape — форма; придавать форму

share — совместно использовать; делиться (информацией); часть; доля

share data – совместно использовать ресурс; делиться данными

share the common goals - разделять общие цели

sharing — совместное использование; коллективный доступ; разделение

shift - клавиша переключения регистров

shift — сдвигать; перемешать; сдвиг; смещение; смена регистра

shortcoming — недостаток; изъян; дефект

short-range – ближнего радиуса действия

side-effect - побочный эффект

sign — знак; символ

signature – комплекс признаков и отличительных особенностей

significance — значимость; важность; значительность; значение; смысл

silicon — кремний

SIM card – SIM-карта

Symbian OS – ОС для сотовых телефонов, смартфонов и коммутированных

similar — подобный; аналогичный

similarity — сходство; подобие

similarly — подобным образом; так же

simple-to-use — простой в использовании

simplicity — простота

simplify — упрощать(ся)

simulate — моделировать; имитировать

simulation — моделирование; имитация

simulator — имитатор; тренажер; программа моделирования / имитации

simultaneously – одновременно

skip — пропускать; переходить

slide — скользить; сдвигать; смещать

slide in – «проскальзывать», проникать тайком

smart phone – смартфон

smileys – смайл(ик); эмограмма, улыбающееся лицо

snail mail – обычная почта; «улиточная почта» (в противоположность электронной; высмеивает медлительность обычной почты, которая доставляет корреспонденцию со скоростью улитки)

soar – резко возражать

social networking – социальные сети

society – общество

soft-copy ~ данные, выведенные на экран

software – программное обеспечение (ПО)

software - программное обеспечение

software glitch – сбой программного обеспечения

solution - алгоритм решения

sophistication – изощрённость; сложность

spam – спам; принудительные сообщения, посылаемые через электронную почту

spam filter – фильтр для спама

spammer – «спаммер»; рассылающий сообщения электронной почты, бесполезные для её получателя

spot – опознавать, обнаруживать

spreadsheet – электронная таблица

spyware – шпионское ПО

spyware detection – обнаружение (выявление) шпионского ПО

SSL connections – (Secure Scale Integration) - SSL соединения (уровень защищённых гнёзд, протокол безопасных соединений)

start-up companies – вновь созданные, начинающие компании

stay resident – постоянно находиться

storage ~ ресурс памяти

storage device – [внешнее] устройство хранения данных

store information - хранить информацию

subject – тема

subset – подгруппа

succeed – преуспевать

suite – программный комплект, комплекс, пакет

supply — источник питания

support ~ вспомогательное аппаратное обеспечение

supposedly – предположительно

surftheWeb – лазить по сайтам

survival – выживание

susceptible – восприимчивый; уязвимый

system administrator – системный администратор

system unit – системный блок

system utilities – сервисные программы системы

systems software – системное программное обеспечение

T

table — таблица

tabulate — табулировать; заносить в таблицу

tabulation — занесение в таблицу

take — брать; выбирать (команду); принимать (вид, значение)

tape - запись на (магнит.) ленту

tape — магнитная лента

targeted attacks – целевые атаки

task - управление ходом выполнения задач

technique — метод; способ; техника; технические приемы; методика

technique – технический приём, методика, метод

technology — технология; техника; методика; методы; способы

template — шаблон; маска; образец; форма

temporarily — временно

tempt – склонять, заманивать, искушать

terminal — терминал; зажим; вывод; конец

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

the demands /requirements — удовлетворять нужды, потребности

the performance of – кроме сбоев в функционировании

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

the Windows Animated Cursor – дистанционное выполнение программы Remote Execution function курсора с анимацией Windows

these types of exploits... – эти виды эксплойтов (вредоносных кодов, эксплуатирующих уязвимости программных компонентов компьютера)

thief – вор

thin-film magnetic medium — тонкопленочный магнитный носитель

threat - угроза

threat – угроза

time - начало отсчета времени

tiny bits of light – крошечные частицы света

to ~ out — обнулять

tool — средство; инструмент

top-level domain – домен верхнего уровня; последняя часть доменного адреса в Интернете, например,

total — общий; суммарный; совокупный; итоговый; весь; целый

touch pad — сенсорная панель

touch screen – сенсорный экран

tracing — слежение; поиск; выявление; определение; трассировка

track — след; траектория; путь; следить; прокладывать путь

trackball — трекбол

transaction - операция, сделка

transfer – передавать, переносить

transfer — передача; пересылка; переход; передавать; пересылать; переносить

transfer the risk - передать риск

transform — преобразовывать; превращать; трансформировать

transformation — преобразование; трансформация

transformational, transformative — трансформационный; связанный с преобразованием

transformer — преобразователь; устройство преобразования;
трансформатор

transition — переход; превращение; модификация

translate — транслировать; преобразовывать; переводить

translator — транслятор; преобразователь

transmission — передача; пересылка; распространение; пропускание

transmission - уровень передаваемого сигнала

Transmission Control Protocol (TCP) – протокол управления передачей

transmit – передавать

transmit — передавать; посылать; пропускать

transmit information - передавать информацию

transmitter — передатчик; датчик; преобразователь

transparent — прозрачный; незаметный

transparently — с соблюдением прозрачности; незаметным образом

trapping — вылавливание; перехват

tribes – племена

trickery – обман, надувательство

trigger – запускать, приводить в действие

trigger — пусковая кнопка

trigger routine – подпрограмма запускающего события

Trojan horse – троянский конь, троянская программа

trouble — неисправность; р./нарушения; неполадки; трудности;

troubleshoot — искать неисправности; диагностировать; отыскивать ошибки

true computer viruses – истинные вирусы

tuner — ручка настройки; программа настройки (параметров)

tuning — настройка; регулирование

typewriter — печатающее устройство

U

unable — неспособный

unacknowledged — неподтвержденный (о приеме сообщений)

unaided eye — невооруженный глаз

unattached — неподсоединенный

unauthorized access - несанкционированный доступ

unauthorized destruction - несанкционированное уничтожение

unauthorized disclosure - несанкционированное раскрытие

unauthorized disruption - несанкционированное разрушение

unauthorized inspection - несанкционированный просмотр

unauthorized modification - несанкционированное изменение

unauthorized perusal - несанкционированное прочтение

unauthorized recording - несанкционированная запись

unauthorized use - несанкционированное использование

unauthorized user – несанкционированный;

unbelievable — невероятный; неправдоподобный

unchanged — неизменный; неизмененный

uncontrollable — неуправляемый; нерегулируемый; неконтролируемый

underline — подчеркивать

undertake — предпринимать

undo — отменять; отмена

unify – объединять

unit — устройство; модуль; механизм; узел; блок; элемент

unknown - неизвестная величина

unplugging — отсоединение; отключение

unpredictable – непредсказуемый

unscrambleinformation - расшифровыватьинформацию

unsolicited mail – непрошенная почта

unsuitable — неподходящий; непригодный

update – обновлять

upgrade - повышение технических возможностей (компьютера)

up-to-date — самая последняя версия программы

usage — использование; применение; эксплуатация

USB – универсальная последовательная шина

USB flash drive – флэш-накопитель; флэш-диск

use — польза; использовать; применять

used — используемый; применяемый

useful — полезный; пригодный

useless — бесполезный

user — пользователь; абонент

user - руководство для пользователя

user - файл пользователя —

user-friendly – удобный для пользователя

utility - полезность

utility — полезность; пригодность; (сервисная) программа; вспомогательное средство

utilize — использовать

utilize – утилизировать, использовать

V

valid — правильный; допустимый

validate - подтверждать

validity — правильность; адекватность; допустимость; пригодность

valuable — ценный; полезный

value — значение; величина; значимость

valueofinformation - ценность информации

valueofinformationresource - ценность информационного ресурса

variable ~ переменная величина

variety — разнообразие;

verifier — устройство / программа проверки

verify - верифицировать (проверить, подтвердить)

verify — проверять; контролировать

versatile — разносторонний; многофункциональный; универсальный

versatility — разносторонность; многофункциональность; универсальность

version — версия; вариант

victim – жертва

view — вид; представление; просмотр

viewer – абонент

viewpoint — точка зрения

viewport — окно просмотра / вывода

violation – нарушение

violation – нарушение; преступление

virtual — виртуальный; нереальный; несуществующий

visible – визуальный; видимый

vital – жизненно важный

volatile memory – энергозависимая память

voltage — (электрическое) напряжение

volume — объем; величина; количество

vulnerability - уязвимость

vulnerability — уязвимость; чувствительность; подверженность

vulnerable – уязвимый

vulnerable — чувствительный; уязвимый; подверженный

W

wafer — пластина; подложка

wait — ожидание; ждать, ожидать

want — недостаток; нехватка; потребность; недоставать;

wanted — нужный; необходимый

wanting — предупреждение

watchdog — сторожевая программа

waveguide — волновод

wavelength — длина волны

way — путь; способ; средство; возможность

Web gateways – Интернет-шлюзы

width — ширина; разрядность (шины, памяти)

Wi-Fi (wireless fidelity) – беспроводная точность

wireless – беспроводной

withdraw — удалять; убирать; вынимать

withdrawal — удаление; выемка; изъятие

without - to — независимо от

WLAN – беспроводная ЛВС

word — слово; текстовый

word processing program – программа обработки текстов

work wonders – творить чудеса

worksheet — электронная таблица

workstation – рабочая (технологическая) станция

world wide — глобальный; всемирный

World Wide Web – всемирная паутина, сеть

worm — (компьютерный) червь

writer — записывающее устройство; программа записи; автор;

X

xerocopy — ксерокопия

xerox — ксерокопировать

Y

yet — тем не менее; все же; еще

yield — выход (результатов); выдача; выдавать; получать (значение)

Z

zero — ноль; нулевой; обнулять

zero day – нулевой день (уязвимость различных программ, на которую проводят атаки в тот же день, когда она обнаружена, т.е. пока отсутствует «заплата»)

zone — зона; область; полоса

Оглавление

РАЗДЕЛ 1. Компьютер и системы компьютерной обработки данных

РАЗДЕЛ 2. Программное обеспечение и интернет-технологии

РАЗДЕЛ 3. Компьютерные сети
РАЗДЕЛ 4. Программирование: языки, методы и технологии

РАЗДЕЛ 5. Понятие и проблемы информационной безопасности

РАЗДЕЛ 6. Виды и методы защиты данных. Криптографическая защита данных

РАЗДЕЛ 7. Вредоносные компьютерные программы и защита от их воздействия

РАЗДЕЛ 8. Классификация преступлений. Компьютерные преступления.

РАЗДЕЛ 9. Киберпреступность. Кибертерроризм и экстремизм: определение, виды

РАЗДЕЛ 10. Информационные и телекоммуникационные компьютерные технологии в расследовании преступлений

Учебное издание

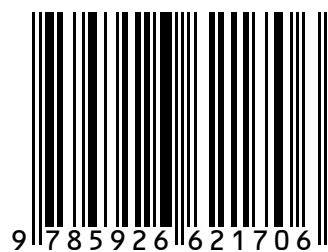
**Профессионально ориентированные материалы
для углубленного изучения английского языка в сфере
информационно-телекоммуникационных технологий**

Учебное пособие

Составители:
Борисова Светлана Викторовна
Гончарова Виктория Аркадьевна

В авторской редакции

ISBN 978-5-9266-2170-6



Подписано в печать 18.07.2025. Формат 60x84 1/16.
Усл. печ. л. 15,0. Тираж 60 экз. Заказ 383.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.