

Министерство образования и науки Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего профессионального образования  
«Владимирский государственный университет  
имени Александра Григорьевича и Николая Григорьевича Столетовых»

Т. И. КОЙКОВА А. Ю. БОРИСОВА

ENGLISH FOR IT

АНГЛИЙСКИЙ ДЛЯ СТУДЕНТОВ,  
ИЗУЧАЮЩИХ ИНФОРМАЦИОННЫЕ  
ТЕХНОЛОГИИ

Учебное пособие



Владимир 2015

УДК 811.111  
ББК 81.2 Англ.  
К55

Рецензенты:

Кандидат филологических наук  
доцент кафедры иностранных языков профессиональной коммуникации  
Владимирского государственного университета  
имени Александра Григорьевича и Николая Григорьевича Столетовых  
*Л. В. Новикова*

Старший преподаватель кафедры русского и иностранных языков  
Владимирского института бизнеса  
*Н. В. Кудачкина*

Печатается по решению редакционно-издательского совета ВлГУ

**Койкова, Т. И.** English for IT = Английский для студентов,  
К55 изучающих информационные технологии : учеб. пособие /  
Т. И. Койкова, А. Ю. Борисова ; Владим. гос. ун-т им. А. Г. и  
Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2015. – 104 с.  
ISBN 978-5-9984-0616-4

Пособие содержит аутентичные тексты. Составлено в соответствии с требованиями программы по иностранным языкам для вузов неязыковых специальностей с целью развития у студентов способности анализировать и обрабатывать научно-техническую информацию, реферировать и аннотировать английский текст.

Предназначено для студентов старших курсов и магистров, изучающих информационные технологии.

Рекомендовано для формирования профессиональных компетенций в соответствии с ФГОС 3-го поколения.

Библиогр.: 18 назв.

УДК 811.111  
ББК 81.2 Англ.

ISBN 978-5-9984-0616-4

© ВлГУ, 2015

## **ПРЕДИСЛОВИЕ**

Пособие включает два раздела, первый составляет основную часть, где представлены тексты для аудиторного чтения; упражнения предусматривают работу с активным словарем, включая терминологию, принятую в сфере информационных технологий, задания, направленные на понимание и анализ прочитанного текста, а также задания, имеющие своей целью реферирование и аннотирование текста.

Второй раздел пособия включает тексты для внеаудиторного чтения, содержащие информацию познавательного характера и непосредственно связанные с тематикой текстов первого раздела. Эти тексты могут быть использованы как для самостоятельной работы студентов, так и в процессе подготовки в рамках научных конференций. Цель работы над данными текстами – развитие навыков компрессии текста.

Авторы выражают благодарность Н. В. Кудачкиной, старшему преподавателю кафедры русского и иностранных языков Владимирского института бизнеса, и Л. В. Новиковой, кандидату филологических наук, доценту кафедры иностранных языков профессиональной коммуникации (ИЯПК) ВлГУ, за ценные замечания, высказанные в процессе работы над рукописью, а также ассистенту кафедры ИЯПК Е. О. Борисовой за предоставленные ею материалы.

# PART I

## Chapter I

### THE LATEST DEVELOPMENTS IN COMPUTER SCIENCE

#### UNIT 1

#### Graphical user interface (part one)

#### Vocabulary

augment (v)	расширять
bitmapped	растровый
title bar	строка заголовка
overlap (v)	перекрывать
pop up (v)	выскакивать на экране
scroll bar	полоса прокрутки
pop up menu	всплывающее меню
envision (v)	предвидеть, рисовать в своем воображении
comprehension	понимание
derive (v)	извлекать
enhance (v)	усиливать, улучшать
overwhelm (v)	ошеломить
inevitable	неизбежный
demise	прекращение деятельности
conceive (v)	понимать, постигать
implementation	осуществление, реализация

(1) Like many developments in the history of computing, some of the ideas for a GUI computer were thought of long before the technology was even available to build such a machine. One of the first people to express these ideas was Vannevar Buch. In the early 1930s he first wrote of a device he called the “Memex”, which he envisioned as looking like a desk with two touch screen graphical displays, a keyboard, and a scanner attached to it. However, starting it about 1937 several groups around the world started constructing digital computers. The perfection and commercial production of vacuum tubes provided the fast switching mechanisms these computers needed.

(2) In 1962, Douglas Englebart published his ideas in an essay “Augmenting Human Intellect”. In this paper for human intellect, Douglas argued that digital computers could provide the quickest method to “increase the capability of a man to approach a complex problem situation, to gain comprehension to suit his particular needs, and to derive solutions to problems.” He envisioned the computer not as a replacement, but a tool for enhancing it. Douglas and his staff worked for years to develop the ideas and technology that finally culminated in a public demonstration in front of over a thousand computer professionals in 1968.

(3) The display was based on vector graphics technology and could display both text and solid lines on the same screen. Douglas’ hands operated three input devices: a standard typewriter-style keyboard and a small rectangular box with three buttons near the top, connected to the computer with a long wire. This was the mouse invented by Douglas himself and built by one of his engineers. Other input devices had been tried (such as touch screens and light pens), but user testing found the mouse to be the most natural way to manipulate an on-screen cursor. With the invention of the mouse came the invention of the mouse pointer, which in this system was a stick arrow, about the height of a single character, pointing straight up. This was called “a bug” by Douglas team, but this term did not survive into modern use.

(4) Douglas Englebart’s demonstration in 1968 overwhelmed many people. Xerox upper management, fearing the inevitable demise of their paper-based company in the ‘paperless” future, decided that they had better make sure they controlled this new technology. They formed the Palo Alto Research Center, or PARC, in 1970. PARC invented its own computer in 1973. The Alto was not a microcomputer as such, although its working components did fit under the desk. Its most striking feature was its display, which was the same size and orientation as a printed page, and featured full raster-based, bitmapped graphics at a resolution of 606 by 808. Each pixel could be turned on and off independently, unlike the vector-based terminals which could only display text and straight lines. It also had a keyboard and a modernized version of Englebart’s mouse, again with three buttons. The mouse cursor itself became a bitmapped image, and for the first time took the familiar diagonal-pointing arrow shape we know today.

(5) At this point the PARC researchers realized that a new visual code development environment had to be invented. This was Smalltalk, the first modern GUI. Smalltalk was conceived as a programming language and development environment so easy to use that a child could understand it, and in many respects was successful in this goal. Smalltalk was the world's first object-oriented programming language, where program code and data could be encapsulated into single units called objects that could then be re-used by other programs without having to know the details of the object's implementation. It first began to take shape around 1974, and was continuously updated and enhanced.

(6) Individual windows in Smalltalk were contained by a graphical border, and stood out against the grey pattern of the background below them. They each had a title bar on the top line of each window which could be used to identify the window and move it around the screen. The title bar did not stretch the full length of the window, but started at the top left and only extended as far as the title itself. Windows could overlap other windows on the screen. The concept of "icons" was also invented at this time – small representations of programs or documents that could be clicked on to run them or manipulate them. Pop-up menus were also invented at the same time – the user would click one of the mouse buttons and hierarchical menu would appear at the last position of the mouse cursor. Also appearing for the first time were scroll bars, radio buttons and dialog boxes. The combination of Smalltalk and the Alto was essentially a modern personal computer with a very similar graphical user interface to the ones we use today. Many of the PARC team wanted Xerox to market the new, cost-reduced Alto III as a commercial product but Xerox management declined.

**Exercise 1.** *Which of the following statements expresses the main idea of the text?*

1. The invention of the first GUI comes back to the 30-th of the twentieth century.
2. It took a long time to develop GUI.
3. Douglas Englebart made a major contribution to the development of GUI.

**Exercise 2.** *Give the number of the paragraph which says about:*

- a) the invention of a mouse;
- b) the idea of building a GUI computer;
- c) the origin of the first GUI;
- d) the construction of the first digital computer;
- e) Douglas's contribution to the development of input devices;
- f) the first computer display; the origin of a modern computer;
- g) the advantages provided by a digital computer;
- h) the invention of the concept of icons;
- i) the devices which provided a computer with fast switching mechanisms;
- j) the world's first object-oriented programming language.

**Exercise 3.** *Define whether the following statements correspond to the content of the text (yes, no).*

1. A computer has been designed to improve the intellectual abilities of a human being.
2. The first GUI was composed of two touch screen graphical displays and a keyboard.
3. A title bar was invented by Douglas Englebart.
4. PARC invented their own computer in order to control the technology being the latest one in 1968.
5. Pop-up menus were being invented along with a title bar and the concept of "icons". Windows on the computer screen cannot overlap each other.
6. The first object-oriented programming language was invented at the very end of the 20th century.
7. Fast switching mechanisms of a computer were provided by improving vacuum tubes.
8. It was Douglas Englebart who designed the device called mouse.
9. Originally, the mouse cursor did not have a diagonal-pointing arrow.
10. Douglas Englebart's inventions did not impress the world of business.
11. It took D. Englebart and his team quite a short time to make all their inventions.

**Exercise 4.** *Match the terms with their definitions.*

- |                       |  |
|-----------------------|--|
| 1. augment            | <b>a.</b> to lie over and partly cover something.  |
| 2. title bar          | <b>b.</b> a horizontal or vertical bar that contains a box that is clicked and dragged up, down, left, or right in order to scroll the screen. |
| 3. pop-up menu        | <b>c.</b> cessation of existence or activity.  |
| 4. derive             | <b>d.</b> to think of or create (something) in the mind.   |
| 5. bitmapped graphics | <b>e.</b> the section at the top of a window that contains the name or description of the window.  |
| 6. demise             | <b>f.</b> a rectangular pattern of parallel scanning lines followed by the electron beam on a television screen or computer.                   |
| 7. overlap            | <b>g.</b> obtain something from (a specified source).  |
| 8. implement          | <b>h.</b> to enlarge in size, number, strength, or extent.   |
| 9. overwhelm          | <b>i.</b> to appear very quickly or suddenly.  |
| 10. inevitable        | <b>j.</b> incapable of being avoided or prevented.   |
| 11. enhance           | <b>k.</b> to picture in the mind; imagine.   |
| 12. conceive          | <b>l.</b> to put into practical effect; carry out  |
| 13. raster            | <b>m.</b> a menu that appears on the display when the user changes the state of a button or makes a selection from a menu bar.                 |

- |                |   |
|----------------|---|
| 14. scroll bar | <b>n.</b> it differs from vector graphics which usually cannot be enlarged or reduced without producing jagged lines or distorted images. |
| 15. pop up     | <b>o.</b> to affect deeply in mind or emotion, to affect (someone) very strongly.   |
| 16. envision   | <b>p.</b> to make greater, as in value, beauty, effectiveness to picture in the mind.   |

**Exercise 5.** *Paraphrase the following statements simplifying their grammar.*

1. Some of the ideas for a GUI computer were thought of long before the technology was even available to build such a machine.
2. Douglas argued that digital computers could provide the quickest method to “increase the capability of a man to approach a complex problem situation, to gain comprehension to suit his particular needs, and to derive solutions to problems.”
3. With the invention of the mouse came the invention of the mouse pointer, which in this system was a stick arrow, about the height of a single character, pointing straight up.
4. Xerox upper management, fearing the inevitable demise of their paper-based company in the ‘paperless’ future, decided that they had better make sure they controlled this new technology.
5. Smalltalk was conceived as a programming language and development environment so easy to use that a child could understand it, and in many respects was successful in this goal.
6. Smalltalk was the world’s first object-oriented programming language, where program code and data could be encapsulated into single units called objects that could then be reused by other programs without having to know the details of the object’s implementation.

**Exercise 6.** *Give your own interpretation of the following words and word combinations used in the text:*

independently, replacement, rectangular box, encapsulate, enhance, identify, cost-reduced product, commercial product.

**Exercise 7.** *Answer the following questions.*

1. When did the first ideas for GUI computers originate?
2. What was the main purpose of inventing a digital computer in Douglas Englebart's opinion?
3. What is the difference between bitmapped and vector graphics?
4. What devices were invented by Douglas's team?
5. What were the advantages of the computer invented by PARC?
6. What developments led to the development of a modern personal computer?

**Exercise 8.** *Make up the plan of the text and render its content.*

## **UNIT 2**

### **Graphical user interface (part two)**

#### **Vocabulary**

pull down menu	разворачивающееся меню
checkmark	галочка
keyboard shortcut	клавишная комбинация быстрого вызова
widget	элемент интерфейса
tiled windows	«мозаичные» окна
shortcut	ярлык
squeeze (v)	сжимать
zoom (v)	увеличивать масштаб
trash	ненужная информация
abandon (v)	отменить
bevel	скошенный, косой
mimic (v)	имитировать
consistent	единообразные по стилю, по управлению
vendor	поставщик, производитель
survivor	сохранившийся, продолжающий существовать
lack (v)	испытывать недостаток

debut (v)	дебютировать
swipe (v)	скользить
font	шрифт

(1) The most important of GUI pioneers was a small startup founded in garage in 1976 by Steve Jobs and Steve Wozniak, called Apple Computer. Apple had built it on the wildly popular Apple computer, which displayed both text and graphics but had a traditional command line interface. Apple was a young company that found itself flush with money, and was more willing to take risks. Many former Xerox PARC engineers found new jobs with Apple to recreate their work on the Alto and Smalltalk but on a product that would actually see commercial release and potentially become very popular. Work on Apple's next-generation Lisa computer, which had started life as a traditional text-based command line computer for business use, was transformed by the influx of PARC people. The Lisa team eventually settled on an icon-based interface where each icon indicated a document or an application, and developed the first pull-down menu bar, where all menus appeared at the very top line of the screen. Other innovations from the Lisa team included the idea of checkmarks appearing next to selected menu items, and the concept keyboard shortcuts for the most frequently used menu commands. The Lisa also changed some PARC conventions, such as using proportionally-sized scroll bars instead of fixed-height ones, and added new conventions, such as a trash can for dragging documents scheduled for deletion, and the idea of "greying out" menu options if they were not currently available. The three-button mouse was simplified to have only one button for the Lisa. As the interface required at least two actions for each icon (selecting and running), the concept of double-clicking was invented to provide this functionality.

(2) In 1985 Bill Gates released a new competing product. In Windows each application had its own menu bar attached to it, just below the title bar. Another departure was the use of tiled, rather than overlapping windows. In 1987 Windows was updated to version 2.0, abandoning the tiled window approach in favour of the overlapping method and having maximizing widgets.

(3) Also in 1987, the UK-based company Acorn Computers introduced their first GUI called "Arthur" along with what was the world's first 32-bit

microcomputer, the Acorn A305/A310. This GUI used proportionally-sized scroll bars and introduced a new concept: a “Dock” or shelf at the bottom of the screen where shortcuts to launch common programs and tools could be kept. It is important to note that many of the GUIs released in the mid-80s supported proportionally-spaced fonts in applications, but they used a fixed-width font for the system (menus and icon labels) for the sake of clarity.

(4) 1988 saw the release of NeXTSTEP, the new GUI and opening system for Steve Jobs’ NeXT computer, his first major project after leaving Apple in 1985. NeXTSTEP which introduced a sharp, 3D beveled look to all of its GUI components, was the first to use the “X” symbol to indicate a close window widget, and introduced the idea of vertical menu strip in the upper left-hand corner, which could also be “torn off” at any point so that the user could leave specific menus at any point on the screen. NeXTSTEP also had a Dock that lived on any side of the screen.

(5) Just before the end of the 1980s, new GUIs started appearing on Unix workstations. These ran on top of a networked windowing architecture known as X, which would later be the foundation for GUIs on Linux. These were simple GUIs that attempted to mimic the appearance of Microsoft Windows but still allow access to the power of the Unix shell underneath. X also introduced a new GUI idea where merely moving the mouse cursor over a window would automatically activate it and allow the user to start typing in it.

(6) The initial design goal of the X Window System was merely to provide the framework for displaying multiple command shells and a clock on a single large workstation monitor. The philosophy of X was to “separate policy and mechanism” which meant that it would handle basic graphical and windowing requests, but left the overall look of the interface up to the individual program. To provide a consistent interface, a second layer of code, called a “window manager” was required on top of the X Window server. The window manager handled the creation and manipulation of windows and window widgets, but was not a complete graphical user interface. Another layer was created on top of that, called a “desktop environment” or DE, and varied depending on the Unix vendor. As the 90s began, other personal computing platforms fell off sharply in popularity, leaving only Windows and the Macintosh as the survivors of the GUI wars.

(7) Windows reached an unprecedented level of popularity with the release of version 3.0 in 1990 and 3.1 in 1992. While still lacking many of the features of the Macintosh (such as an icon-based file manager) it was sharp and had good looking icons, and sold millions of copies. The release of Windows 95 cemented Microsoft's lead in GUI sales, and became one of the most popular programs of all time. Windows 95 introduced the concept of the Start Menu, from which all programs could be launched, and the Task Bar where all running programs could be switched between. The next major release of Microsoft is operating system Windows 8 which officially debuted on October 26th, 2012. Windows 8 is a completely redesigned operating system developed with touchscreen use in mind as well as near-instant-on capabilities that enable a Windows 8 PC to load and start up in a matter of seconds rather than in minutes. Windows 8 replaces the more traditional Microsoft Windows OS look and feel with a new design system interface codenamed "Metro" that first debuted in the Windows Phone 7 mobile operating system. The Metro user interface primarily consists of a "Start screen" made up of "Live Tiles", which are links to applications and features that are dynamic and update in real time. Users can switch between apps in Metro by simply swiping across the screen.

**Exercise 1.** *Which of the following statements expresses the main idea of the text?*

1. The most important changes in GUI began in 1976.
2. The GUI advance was the result of efforts of some people.
3. It was Bill Gates who made the greatest contribution to the development of GUI.

**Exercise 2.** *Give the number of the paragraph which expresses the following ideas.*

1. Since then computer users have been able to leave specific menus somewhere on the screen.
2. Microsoft took a leading position on the market of GUI.
3. The first icon-based interface made its appearance in the late 1980s.
4. The preference was given to the tiled windows.
5. A complete graphical interface was not created at that time.
6. Some special button combinations were invented for the most frequently used menu commands.

7. The company took a risk due to the available finance.
8. The company with the head office in Great Britain developed its own microcomputer.
9. Computer users got the possibility to write in the windows.
10. This GUI gave the possibility to load and start up within seconds.

**Exercise 3.** *Define whether the following statements correspond to the content of the text (yes; no; not stated).*

1. The first significant GUI computer was designed in Xerox PARC.
2. In its early days Apple Company had a lot of sponsors.
3. Lisa computer was designed as an ordinary computer for that period of time.
4. Lisa computer was aimed at doing a scientific research.
5. While working with Lisa computer the Apple employees used PARC conventions.
6. A one-button mouse provided two functions: selecting and running.
7. The so-called “dock” was designed to keep shortcuts of common programs and tools.
8. NeXTSTEP GUI gave a user the opportunity to leave specific menus at any point on the screen.
9. GUI used in the UK-based company Acorn Computers made it possible to type in a window.
10. The window manager handled the creation and manipulation of a complete graphical user interface.
11. Before the end of the 1980s, new GUIs were installed on different types of workstations.
12. Windows became very popular when version 2.0 appeared.
13. Windows 3.1 did not have many features of the Macintosh.
14. Microsoft took the leading position in GUI sales after the appearance of Windows 95.
15. A new design system interface “Metro” was originally used in a mobile phone.

**Exercise 4.** *Match the terms with their definitions.*

- |              |  |
|--------------|--|
| 1. Smalltalk | a. a menu that appears when an item in a GUI is selected, usually below the item (it is also called drop-down menu). |
|--------------|--|

2. Alto **b.** a powerful multi-tasking, multi-user computer operating system.
3. widget **c.** a style of type.
4. checkmark **d.** a general term for a small gadget or device.
5. trash **e.** something that is reliable or in agreement.
6. abandon **f.** to imitate or copy in action, speech, etc.
7. Unix **g.** a programming language that was designed expressly to support the concepts of object-oriented programming.
8. consistent **h.** being at the disposal.
9. vendor **i.** litter bin.
10. survivor **j.** a person who sells something.
11. squeeze **k.** to pass a hand over the screen.
12. swipe **l.** the desktop computer from Xerox that pioneered the use/icon//desktop environment.
13. conventions **m.** ideas or actions intended to deal with a problem or situation.
14. approach **n.** a person or a thing who outlives the other or others.
15. font **o.** absence of something that should be there.
16. pull-down menu **p.** reference designations.
17. available **q.** worthless or discarded material or objects; refuse or rubbish.

- |               |  |
|---------------|--|
| 18. mimic     | r. to press forcibly together; compress.   |
| 19. lack      | s. to give up by leaving or ceasing to operate with e.g.the electronic work sheet. |
| 20. trash can | t. a mark indicating that something has been noted or completed etc.               |

**Exercise 5.** *Give your own interpretation of the following words and word combinations used in the text:*

flush with money, to take risks, set about, commercial release, influx, eventually, competing product, activate, unprecedented, initial, debut, near-instant-on capabilities, for the sake of clarity.

**Exercise 6.** *Paraphrase the following statements simplifying their grammar.*

1. Apple was a young company that found itself flush with money, and was more willing to take risks.
2. In 1987 Windows was updated to version 2.0, abandoning the tiled window approach in favour of the overlapping method and having maximizing widgets.
3. The philosophy of X was to “separate policy and mechanism” which meant that it would handle basic graphical and windowing requests, but left the overall look of the interface up to the individual program.
4. Windows 8 is a completely redesigned operating system developed with touchscreen use in mind as well as near-instant-on capabilities that enable a Windows 8 PC to load and start up in a matter of seconds rather than in minutes.

**Exercise 7.** *Answer the following questions.*

1. What kind of interface was developed by the Apple for its Lisa computer?
2. What innovations did PARC people introduce?
3. What was Bill Gates’ contribution to the further development of modern GUIs?
4. Who introduced the term “Dock”?
5. What is the objective of the “X” symbol?

6. What was done by the GUI developers for providing a consistent interface?
7. What were the reasons for the popularity of Windows 95?
8. What are the main features of Windows 8?

**Exercise 8.** *Make up the summary of the text.*

### **UNIT 3      Smartphones and mobile operating systems**

#### **Vocabulary**

track pad	сенсорная панель
stylus	перо
Wireless Application Protocol (WAP)	протокол мобильной интерактивной связи с Интернетом
QUERTY keyboard	стандартная клавиатура компьютера
keypad	клавишное поле
single-minded	имеющий узкое назначение
digital voice service	цифровая передача речевых сигналов
swipe	прокрутка; скольжение
tapping	касание
pinch	щипок
runtime performance	настройки быстродействия
Notification area	центр уведомлений
thumbnail	«миниатюра», контрольное изображение
parallax	видимое угловое смещение объекта
sluggish	зависающий
force quit (v)	принудительно завершить работу
source code	исходный код
reverse pinch	растягивание

haptic	осязаемый
boot	загрузка
toolkit	набор инструментальных средств
capacitive	емкостный

(1) Like a computer operating system, a mobile operating system is the software platform on top of which other programs run. When a user purchases a mobile device, the manufacturer will have chosen the operating system for that specific device. The operating system is responsible for determining the functions and features available on the device, such as keyboards, Wireless Application Protocol (WAP), synchronization with applications, e-mail, text messaging and more. The mobile operating system will also determine which third-party applications can be used on the device.

(2) The commercial success of smartphones and tablets has opened up a new and untapped market in mobile communications. Smartphone is a cellular telephone with built-in applications and Internet access. In addition to digital voice service, modern smartphones provide text messaging, e-mail, Web browsing, still and video cameras, MP3 player and video playback. In addition to their built-in functions, smartphones run myriad free and paid applications, turning the once single-minded cellphone into a mobile personal computer.

(3) Since 2007, touchscreen phones have come to dominate the mobile device market. Touchscreen display is a type of electronic display that senses physical touch by a person's hands or fingers, or by a device such as a stylus, and then performs actions based on the location of the touch as well as the number of touches. It is useful for interacting directly with a computer or electronic device, partially or even completely eliminating the need for intermediate input devices such as computer mice, track pads or keyboards.

(4) Smartphones, tablets, laptops and similar electronic devices can be based on one of the two primary types of touchscreen displays. Resistive touch displays distinguish and sense specific touch location when the two electrically charged layers of the touchscreen are pressed together with the physical force at a specific point. Capacitive touch screens distinguish and sense specific touch location based on the electrical impulses in a human

body, typically the fingertip. This enables capacitive touchscreens to not require any actual force to be applied to the screen's surface; at the same time, capacitive screens typically don't respond to styluses or gloved hands due to the lack of electrical impulses generated.

(5) The presence of touch functionality in smartphones and tablets clearly underlines the popularity of this interface. Touchscreen devices have also changed the whole way we look at mobile OS. Better technology, lower costs and heightened competition have increased the range of features and functionalities found on phones and tablets.

The four major smartphone operating systems are iPhone (iOS), Android, BlackBerry and Windows Phone.

(6) Symbian mobile OS was used by many major mobile phone brands, like Samsung, Motorola, Sony Ericsson, and above all by Nokia. Symbian had a native graphics toolkit. It was designed to be manipulated by a keyboard-like interface metaphor, such as the ~15-key augmented telephone keypad, or the mini-QWERTY keyboards. It was the most popular smartphone OS on a worldwide average until the end of 2010, when it was overtaken by Android. Although more Symbian smartphones have been sold worldwide than any other, in 2011, Nokia switched from its native Symbian to the Microsoft phone platform.

(7) Android is a Linux-based operating system designed primarily for touchscreen mobile devices such as smartphones and tablet computers. Initially developed by Android, Inc., it was financially backed by Google which later bought it in 2005. Android is an open-source code and its licensing allows the software to be freely modified and distributed by device manufacturers and enthusiast developers. Additionally, Android has a large community of developers writing applications that augment the functionality of devices, written primarily in a customized version of the Java programming language. In October 2012, there were approximately 700,000 apps available for Android, and the estimated number of applications downloaded from Google Play was 25 billion.

(8) Android's user interface is based on direct manipulation, using touch inputs that correspond to real-world actions, like swiping, tapping, pinching and reverse pinching to manipulate on-screen objects. The response to user input is designed to be immediate, often using the vibration capabili-

ties of the device to provide haptic feedback to the user. Android devices boot to the home screen which is similar to the desktop found on PCs. Android home screens are typically made up of app icons and widgets; app icons launch the associated app, whereas widgets display live, auto-updating content such as the weather forecast and the user's email inbox.

(9) IOS is a mobile operating system for Apple-manufactured devices. IOS runs on the iPhone, iPad, iPod Touch and Apple TV. IOS is best known for serving as the underlying software that allows iPhone users to interact with their phones using gestures such as swiping, tapping and pinching. These finger actions are typically performed on multi-touch capacitive touch screen displays, which provide fast response and accept inputs from multiple fingers.

(10) IOS comes with a lot of default apps, including an email client, a Safari Web browser, a portable media player (iPod) and the phone app. Developers can use the iOS software development kit (SDK) to create applications for Apple mobile devices. The SDK includes tools and interfaces for developing, installing, running and testing apps. Native apps can be written using the iOS system frameworks and the Objective-C programming language. Included in the iOS SDK are Xcode Tools, which include an integrated development environment (IDE) for managing application projects, a graphical tool for creating the user interface and a debugging tool for analyzing runtime performance. IOS 7 for iPhone 5 has recently appeared on the smartphone market. Its GUI has undergone some noticeable changes. First of all, iOS 7 gets rid of the black bars at top and bottom of the screen; you have the "slide to unlock" words highlighted by a helpful animated glow.

(11) A file sharing feature AirDrop is also available on mobile devices running the iOS 7. It's very simple: a "sharing" icon in an app lets you send a file, link or other piece of data to those willing to receive it. You choose AirDrop and you get a list of people in the vicinity. Press their icon and it's done. The receiver gets a message popping up on their screen where they can accept or reject the data – photo, file, link. Double-tapping the Home button brings up the list of apps used before. In iOS 6 and earlier, it was a row on the bottom of the screen; now it's a flat carousel in the screen centre. It has the style of thumbnails. If an app is sluggish, force quit the application by double tapping the Home button and flicking the app's window up. The home screen gets some goodies too. It and the lock screen can use dynamic or static wallpapers, and they can use panoramas

too. Wallpapers also benefit from a subtle parallax effect, so if you move the phone the wallpapers appear to move. The rest of iOS 7 emphasizes simplicity, so for example, the stitched leather is gone from Calendar and Notes don't pretend that they've been written on yellow legal pads. Simplifying iOS makes it feel much more modern and efficient.

**Exercise 1.** *Which of the following statements expresses the main idea of the text?*

1. IOS 7 is the latest state-of-the-art gadget.
2. Touchscreen phones are dominating on the mobile device market.
3. Modern smartphones are based on the advanced mobile operating systems.

**Exercise 2.** *Change the order of the following items according to the content of the text.*

1. Two primary types of touchscreen displays.
2. A Linux-based operating system designed primarily for touchscreen mobile devices.
3. The responsibility of operating systems for the functions and features of a mobile phone.
4. The most popular smartphone OS until the end of 2010.
5. The abilities provided by AirDrop.
6. Touchscreen displays and their functions.
7. The principle of Android's user interface operation.
8. Internetworking Operating System.
9. Smartphone as a mobile personal computer.
10. The iOS software development kit.

**Exercise 3.** *Define whether the following statements correspond to the content of the text (true – T; false – F; not stated – NS).*

1. It makes no difference what operating system is used in some particular device.
2. Smartphones became popular due to the application of new technologies.
3. Touchscreen displays provide the direct interaction with a computer.
4. The number of services provided by a smartphone is unlimited.

5. Resistive touch displays do not require any actual force to be applied to the screen's surface.
6. A capacitive touch screen is activated by the electrical impulses in a human body.
7. The change from one phone platform to another happened in 2011.
8. Android licensing meant that it was impossible to modify the software.
9. Home screens of Android devices and PC desktops are the same.
10. There are black bars at top and bottom of the screen with iOS 7 for iPhone5.
11. In iOS 7 the list of apps used before is a flat carousel in the screen centre.
12. Actually, iOS is used in all modern gadgets.

**Exercise 4.** *Match the terms in the left column with their definitions.*

- |                |   |
|----------------|---|
| 1. thumbnail   | <b>a.</b> a pointing and drawing device that is shaped just like a pen. It is used when operating digital tablets and touch screens devices such as smart phones and iPads.                               |
| 2. keypad      | <b>b.</b> a multi-touch touchpad from Apple that debuted on Mac laptops in 2009 and became a stand-alone pointing device for desktop computers in 2010.   |
| 3. home button | <b>c.</b> sliding a finger or stylus across a touch screen to scroll or move items around.  |
| 4. stylus      | <b>d.</b> a miniature representation of a page or image that is used to identify a file by its contents; may be used to rearrange the page order by dragging and dropping them into a different sequence. |

- 5. trackpad e. written by a programmer, but not directly executable by the computer. It must be converted into machine language by compilers, assemblers or interpreters.
- 6. swipe f. a small keyboard, for example on a telephone, computer, or calculator.
- 7. source code g. a reference to the main page of a site.

**Exercise 5.** *Say what terms are meant by the following descriptions?*

1. It is a collection of software used for developing applications for a specific device or operating systems. It typically includes an integrated development environment. Most of them contain a sample code, which provides developers with example programs and libraries. They also offer technical documentation, which may include tutorials and FAQs. Some of them may also include sample graphics, such as buttons and icons, which can be incorporated into applications.

2. The name comes from the first six letters (keys) appearing in the top left letter row of the keyboard, read from left to right. Its design is based on a layout created for the Sholes and Glidden typewriter and sold to Remington in the same year, when it first appeared in typewriters. It became popular with the success of the Remington No. 2 of 1878, and remains in use on electronic keyboards due to the network effect of a standard layout and a belief that alternatives fail to provide very significant advantages. Its use and adoption is often viewed as one of the most important case studies in open standards because of the widespread, collective adoption and use of the product, particularly in the United States.

3. It is an application that facilitates application development. In general, it is a graphical user interface GUI-based workbench designed to aid a developer in building software applications with an integrated environment combined with all the required tools at hand. Most common features, such as debugging, version control and data structure browsing, help a developer quickly execute actions without switching to other applications. Thus, it

helps maximize productivity by providing similar user interfaces (UI) for related components and reduces the time taken to learn the language. It supports single or multiple languages.

4. It defines a mechanism for accessing and delivering content over wireless networks. It is based on the layered OSI model, uses new networking protocols having functions similar to the Web protocols HTTP, SSL, and TCP. A nice feature of its browsers is that they can be implemented on small mobile devices such as cell phones, pagers, and PDAs. So, instead of coding content using HTML and JavaScript, programmers can use WML and WML Script. WML and its companion scripting language WML Script are tag-based markup languages designed after the HTML model. The advantages are that WML demands less memory and processing power from browsers, as compared to HTML and JavaScript. Another asset to WML is that it was designed to be used in relatively small display sizes so common in wireless devices such as PDAs.

5. It is the environment and data structures that keep track of everything that's going along as your program runs. In C, it is the environment variables and operating-system provided services that let the program interact with the rest of the system. In an object-oriented language, it's also all the tables of objects and classes and methods that get built to allow message passing to take place. In an interpreted language, it's the state of the interpreter, plus all of those other things. In general, it can be described as "everything that happens that you didn't explicitly write yourself".

---

a) Wireless Application Protocol; b) IDE; c) runtime; d) SDK; e) QWERTY keyboard.

**Exercise 6.** *Find the following words and word combinations in the appropriate paragraphs of the text and explain what they mean in the given context.*

third-party applications (1), untapped market (2), myriad (2), intermediate (3), underline (5), on a worldwide average (6), customized version (7), estimated number (7), haptic feedback (8), auto-updating content (8), "slide to unlock" words (10), gets rid of (10), a file sharing feature AirDrop (11), goodies (11), link (11).

**Exercise 7.** *Paraphrase the following statements simplifying their grammar.*

1. In addition to their built-in functions, smartphones run myriad free and paid applications, turning the once single-minded cellphone into a mobile personal computer.
2. This enables capacitive touchscreens to not require any actual force to be applied to the screen's surface.
3. Although more Symbian smartphones have been sold worldwide than any other, in 2011, Nokia switched from its native Symbian to the Microsoft phone platform.
4. It was the most popular smartphone OS on a worldwide average until the end of 2010, when it was overtaken by Android.

**Exercise 8.** *Answer the following questions.*

1. What makes iOS modern and efficient?
2. Who is responsible for the functions and features of a mobile phone?
3. What is a smartphone?
4. What is a touchscreen display?
5. What types of touchscreen displays are available nowadays?
6. Since when have touchscreen phones dominated the mobile device market?
7. What was the most popular smartphone OS in 2010?
8. What is meant by Android?
9. What operating system was primarily designed for touchscreen mobile devices?
10. What is Android's user interface based on?
11. What is iOS?
12. What can be used for creating applications for Apple mobile devices?
13. What abilities does a file sharing feature AirDrop provide?

**Exercise 9.** *Make up the summary and the abstract of the text.*

**Vocabulary**

heterogeneous	неоднородный
middleware	связующее программное обеспечение
sophisticate (v)	усложнять
scalable	наращиваемый
appropriate	подходящий, соответствующий
proprietary	патентованный
tenancy	владение
constituent group	клиентская группа
affordable	возможный, допустимый
customize (v)	переделывать, подгонять
pool (v)	объединять

(1) Technological developments are increasingly changing and getting sophisticated. Cloud computing is the latest development of client server applications and files are stored in the “cloud”. Cloud computing is a term that applies to applications and data storage that are delivered over the Internet or via wireless technology. The individual user's device (i.e. computer, cell phone, etc.) only provides an interface to interact with the computer programs and data. In brief, cloud computing is the product of Virtualization technology which offers to use the hardware or infrastructure or software applications either separately or combined without really having your own hardware. Cloud Computing refers to the delivery of computing and storage capacity as a service to a heterogeneous community of end-recipients. Cloud is a computing model providing web-based software, middleware and computing resources on demand. By deploying technology as a service, you give users access only to the resources they need for a particular task. You pay for what you use! It prevents you from paying for idle computing resources. Cloud computing can also go beyond cost savings by allowing the users to access the latest software and infrastructure offerings to foster business innovation. The users are actually using the cloud computing without realizing it. When you are using the Sky Drive,

Hotmail, Gmail, you are in the cloud. Cloud computing is to access resources that are somewhere over the Internet. It can be accessed for free, as is the case of emails or by premium subscription with a guaranteed service level. Virtually the power is infinite. Businesses use cloud computing with Rackspace. com to combine all their processes on one server.

(2) Cloud computing is mostly economic. If you are a very small company, it will launch a service without any capital investment in hardware. Thus, with cloud computing, virtually with no start-up software and hardware investment you are getting heavy equipment today. The second advantage is being able to benefit from economies of scale that have an economic impact. Resources that are not used by the Indian companies at night can be used by the companies being on the other side of the planet, such as U.S., as an example. Cloud computing is like a machine with unlimited resource that runs 24 hours and 7 days a week and all those resources are shared.

(3) Cloud computing is self-healing. In case of failure, the last backup of the application automatically becomes the primary copy. Cloud computing offers a high scalability. The whole architecture is predictable and efficient. It is not one computer or server; it is thousands of computers that can handle the situation. Cloud Computing is a Multipurpose Virtualization system. In Cloud Computing, it is not possible to know where your data is physically present. Among the characteristics of cloud computing is the availability of on-demand services. Due to this feature cloud services can be used automatically as needed and without human interaction from service provider. Cloud computing provides broad network access, i.e. the access to the remote systems via a network such as the Internet or intranet. Cloud computing assumes that all Network resources should be pooled. The resource of the cloud provider is designed to meet the need of Cloud users and is provided dynamically. The cloud provider is independent of location. The user does not have any control nor the knowledge where from the services are offered (geographically). The cloud systems have built-in control and measurement of resource consumption function depending on the type of cloud service. Thus, both parties, the cloud provider and the cloud user, ensure appropriate transparency in relation to the services utilized. It is API based and manipulation is not possible.

(4) So, Cloud Computing provides its users with a number of very important benefits. At the same time there are some reasons for criticizing

Cloud Computing. One of the drawbacks is that Cloud Computing increases the dependency of Internet usage. As appropriately said by Richard Stallman “One reason you should not use web applications to do your computing is that you lose control ... It’s just as bad as using a proprietary program.” (Reference of the quotation: The Gaurdian).

(5) Cloud computing can be divided into three groups: a public cloud, a private cloud and a hybrid cloud. Public clouds are owned and operated by companies that use them to offer rapid access to affordable computing resources to other organizations or individuals. With public cloud services, users don’t have to purchase hardware, software or supporting infrastructure, which is owned and managed by a provider. A private cloud is owned and operated by a single company that controls the way virtualized resources and automated services are customized and used by various lines of business and constituent groups. Private clouds exist to take advantage of many of cloud’s efficiencies, while providing more control of resources and steering clear of multi-tenancy. A hybrid cloud uses a private cloud foundation combined with the strategic use of public cloud services. The reality is that a private cloud can’t exist in isolation from the rest of a company’s IT resources and the public cloud. Most companies with private clouds will evolve to manage workloads across data centers, private clouds and public clouds – thereby creating hybrid clouds.

(6) Services which are offered by cloud computing are numerous and various. Cloud-based applications – or software as a service (SaaS) – run on distant computers “in the cloud” that are owned and operated by others and that connect to users’ computers via the Internet and, usually, a web browser. Platform as a service provides a cloud-based environment with everything required to support the complete lifecycle of building and delivering web-based (cloud) applications – without the cost and complexity of buying and managing the underlying hardware, software, provisioning and hosting. Infrastructure as a service provides companies with computing resources including servers, networking, storage, and data center space on a pay-per-use basis.

**Exercise 1.** *Which of the following statements expresses the main idea of the text?*

1. Cloud Computing is a computer technology which uses the Internet for storing data and applications.

2. Cloud Computing provides its users with a number of very important benefits.
3. Cloud Computing provides its users with the services which are free of charge.

**Exercise 2.** *Change the order of the following items according to the content of the text.*

1. Characteristics of cloud computing.
2. Types of Cloud Computing.
3. Benefits of cloud computing.
4. Main objective of a cloud computing.
5. Drawbacks of Cloud Computing.
6. Definition of a Cloud.
7. Definition of Cloud Computing.

**Exercise 3.** *Define whether the following statements correspond to the content of the text (true – T; false – F; not stated – NS).*

1. State-of-the-art technologies are becoming less sophisticated.
2. Cloud Computing provides hardware or infrastructure or software applications.
3. The term “cloud” comes from the direct meaning of the word.
4. The users do not realize the essence of Cloud Computing.
5. The resources of Cloud Computing are unlimited.
6. In case when Cloud computing fails, an expert makes the necessary debugging.
7. A user always knows who offers him cloud computing services.
8. Public clouds are accessible to every company.
9. A hybrid cloud was created by one of the private companies.
10. It is necessary to have a cloud-based environment in order to support the process of construction and delivery of cloud applications.

**Exercise 4.** *Match the terms in the left column with their definitions.*

- |        |   |
|--------|---|
| 1. API | a. use of a browser (thin client) to access a software application over the Internet to perform work. |
|--------|---|

- |                           |  |
|---------------------------|--|
| 2. Cloud Computing        | <b>b.</b> computing software that occupies a position in a hierarchy between the operating system and the applications.  |
| 3. Hybrid cloud computing | <b>c.</b> allows you to download images, vectors, and video clips in the highest definition available.   |
| 4. Web-based software     | <b>d.</b> it is an abbreviation for Application Program Interface.   |
| 5. middleware             | <b>e.</b> computer technology which uses the Internet for storing data and applications.   |
| 6. premium subscription   | <b>f.</b> a combination of public cloud storage and private cloud storage where some critical data reside in the enterprise's private cloud while other data are stored and accessible from a public cloud storage provider. |

**Exercise 5.** *Find the following words and word combinations in the appropriate paragraphs of the text and explain what they mean in the given context.*

to deploy a technology (1), cost savings (1), to foster business innovation (1), somewhere over the Internet (1), premium subscription (1), infinite (1), self-healing (3), scalability (3), handle the situation (3), remote systems (3), resource consumption (3), appropriate transparency (3), to take advantage (5), a pay-per-use basis (6).

**Exercise 6.** *Paraphrase the following statements simplifying their grammar.*

1. Cloud computing can also go beyond cost savings by allowing the users to access the latest software and infrastructure offerings to foster business innovation.

2. A private cloud is owned and operated by a single company that controls the way virtualized resources and automated services are customized and used by various lines of business and constituent groups.
3. Private clouds exist to take advantage of many of cloud's efficiencies, while providing more control of resources and steering clear of multi-tenancy.
4. Platform as a service provides a cloud-based environment with everything required to support the complete lifecycle of building and delivering web-based (cloud) applications – without the cost and complexity of buying and managing the underlying hardware, software, provisioning and hosting.

**Exercise 7.** *Answer the following questions.*

1. What is cloud computing?
2. What does the term “cloud” mean in the field of computer science?
3. What does it mean “to access resources by premium subscription”?
4. What are the benefits of cloud computing?
5. What is Cloud Computing criticized for?
6. What does Cloud Computing offer its users as services?

**Exercise 8.** *Make up the summary and the abstract of the text.*

## **UNIT 5**                      **What is “hybrid” cloud computing?**

### **Vocabulary**

lock down (v)	ограничить возможности
multi-tenant	многопользовательский
nascent	появляющийся, рождающийся
rage	сильное стремление, рвение
concern	озабоченность
test bed	испытательный стенд
business setup	предприятие
sales metrics	количественные показатели продаж

dummy	макет
vet	проверять
go live (v)	начать функционировать
craft (v)	изготавливать
hurdle	препятствие, помеха
up-front cost	полная стоимость
downtime	время бездействия (из-за неисправности)
outage	перерыв в работе
cross-contamination	взаимное ухудшение
mitigate (v)	смягчать
API	программный интерфейс приложения
SOP (Standard operating procedure)	стандартный порядок действий

(1) Hybrid cloud computing combines the benefits of so-called ‘public’ cloud resources where some IT functions are managed externally, while a defined percentage of a company’s IT stays on-premise in a ‘private’ cloud. The business benefits from the cost and flexibility advantages offered by public cloud computing and can apply that model to the data that it feels happy to manage externally. At the same time, the business is able to retain customer data (and other Intellectual Property) inside its own data centre.

(2) The ‘hybrid cloud’ has been described as the best of both worlds; it has certainly brought many new organisations to the cloud that had previously voiced fears relating to the data security of external public clouds. While a business might use the Rackspace cloud or Amazon Elastic Computer Cloud (EC2) for its general computing requirements, the private cloud remains in place for mission-critical sensitive data that needs to be locked down. This is not to say that public cloud computing resources are insecure, but some companies are wary of housing their data alongside that of their competitors in what is known as a multi-tenant cloud, i.e. one with several customers’ data stored inside.

(3) If you think about it, many (if not all) companies have made pretty significant investments in their own IT infrastructure already. The option to

still use the company network is generally viewed as a more practicable step than a complete jump to the cloud all at once. As for the hybrid model it maximises flexibility in the company's IT mix, as it can be a composition and combination of at least one private cloud and at least one public cloud.

(4) There are still problems lying ahead. The matter is that the hybrid cloud offers operational flexibility; it also offers scalability of peaks in data traffic; and yet it is a nascent technology and so is still being developed. There may be interconnectivity challenges on the road ahead as this new IT service delivery model is brought online, but the general feeling is that it's all very positive.

(5) Cloud computing has been the latest rage for several years, becoming more and more popular as distributed systems and easier access to services becomes the norm. Demand for cloud services has grown quickly, but many IT directors have expressed concerns over public cloud security issues and have instead moved towards private clouds, which are generally far more restricted and less distributed than are public systems. This means losing many of the advantages of the public cloud in the switch. A solution that has emerged is the hybrid clouds, which are often now the focus of IT management as they work to balance user needs, data access requirements, and security. In 2011 the survey by Unisys showed that 21 percent of IT organizations are focusing on hybrid clouds and a Sand Hill Group survey just before that showed that IT managers believed hybrid cloud use will continue a fast growth. The 2010 SHG survey predicted growth would triple, which happened by 2014.

(6) So what is the hybrid cloud, how does hybrid cloud computing work, and will it work for your organization? The hybrid cloud is a mixture of private and public cloud systems; hence its name. The private cloud can be self-hosted by the company (common in enterprise) or hosted by a paid third-party virtually, but kept private for the company's own use (common in smaller systems). The public cloud, of course, is public and off-premise. Users connect to the private cloud separately from the public one. Often, the setup has the public cloud hosting software, data and services that are non-critical with the rest on the private cloud. Many firms use the public cloud as a development test bed as well. In a small business setup, for example, the private cloud may hold valuable customer data and sales metrics

while the public cloud hosts the company's virtual phone network and communications system. In an enterprise, as another example, the public cloud may host the beta version of the company's proprietary in-house software for tracking and analysis with key test data (all dummies created for the testing) included. The private cloud hosts the actual software and data and will be upgraded once testing in the public cloud is complete. This saves valuable network and hardware resources for continued enterprise use while allowing the IT department to fully vet software-in-progress before going live and without fear of harming the current network. Some large networks have multiple private-public cloud mixtures, though this is generally only common in large enterprises with geographically global data centers and offices. Many financial institutions, for example, use multiple private-public cloud mixes. It is more common for enterprise to have a single private cloud and multiple public clouds for various services.

(7) The hybrid cloud allows IT to take advantage of the benefits of the private and public cloud. Some of the risks associated with these systems are also included, however, so the mixture is not always just positives. The challenge for the IT manager is to find the proper balance between the risks and rewards to craft a hybrid cloud that works well for the corporation's needs. There are Pros and Cons of Hybrid Cloud Computing. Among the former are the following benefits. First: Public clouds allow for a low investment hurdle to activate and can be cheaply scaled to more or less servers and network connections as needed. In a hybrid cloud, this flexibility is retained for all services put onto the public cloud, giving a lot of operational flexibility. Second: Private clouds have fewer security concerns and the enterprise retains control over the data center and its contents. In the hybrid cloud this remains so. Among the latter are the following downsides of the hybrid cloud. First: The flexibility of the private cloud is very limited and the up-front costs and continued maintenance requirements can be expensive. Management will have to budget for needs as well as the occasional unforeseen downtime or outage. Second: Mismanagement of the two systems can lead to cross-contamination, with data from the private (secure) cloud being ported to the public cloud. This is mitigated with intelligent SOPs.

(8) The goal of a hybrid cloud system is to provide as many benefits of the public and private cloud as possible while not incurring the risks associated

with them. Most of this will be done in the design and implementation stages, of course, and proper API between the two (if any connections are to be had at all) will be critical in that process. Since the primary concern in a hybrid cloud is the accidental crossing of critical data from private to the public, having no or very few and tightly controlled connections is important. Generally speaking, the hybrid cloud will increase the complexity of a network environment. The benefits, however, often outweigh this issue of complexity and are enough to override the initial planning costs.

**Exercise 1.** *Which of the following statements expresses the main idea of the text?*

1. Hybrid Cloud Computing has more advantages than drawbacks.
2. The hybrid cloud allows IT to take advantage of the benefits of the private and public cloud.
3. The hybrid cloud is characterized by a great complexity.

**Exercise 2.** *Match the following titles to the appropriate paragraph.*

1. The challenge that lies ahead.
2. The objective of a hybrid cloud system.
3. The Pros and Cons of Hybrid Cloud Computing.
4. Two types of cloud used by companies.
5. The main idea of ‘hybrid’ cloud computing.
6. Best of both worlds.
7. Hybrid cloud makes business sense.
8. Hybrid Cloud Architecture.

**Exercise 3.** *Define whether the following statements correspond to the content of the text (true – T; false – F; not stated – NS).*

1. Hybrid cloud computing takes the advantages of “public” cloud resources only.
2. The emergence of the ‘hybrid cloud’ made many companies join the cloud.
3. The leading international companies use Amazon Elastic Computer Cloud.
4. Some companies are afraid of using a public cloud for storing their data.

5. All the problems relating to the Hybrid model have been solved.
6. The first ideas of cloud computing emerged in 70s-80s of the XX century.
7. Hybrid cloud is the most popular technology with business management.
8. Public clouds usually contain critical sensitive data.
9. Many financial institutions use a single private cloud and multiple public clouds for various services.
10. Every IT manager has to make a sensible use of the mixture of the private and public clouds.
11. Hybrid Cloud Computing is lack of operational flexibility inherent in the Public cloud.
12. It is very important to manage cloud computing systems in a proper way.

**Exercise 4.** *Match the terms in the left column with their definitions.*

- |                |   |
|----------------|---|
| 1. up-front    | <b>a.</b> a platform for experimentation of large development projects.                                     |
| 2. outage      | <b>b.</b> an imitation of a real or original object, intended to be used as a practical substitute.         |
| 3. test bed    | <b>c.</b> money given immediately upon the completion of a financial agreement.                             |
| 4. flexibility | <b>d.</b> obstacle; a difficult problem to be overcome.   |
| 5. matrices    | <b>e.</b> something that interests you because it is important or affects you.                              |
| 6. dummy       | <b>f.</b> an interruption or failure in the performance of some operation (supply of power, as an example). |
| 7. hurdle      | <b>g.</b> the ability to change or be changed easily to suit a different situation.                         |
| 8. concern     | <b>h.</b> a set of figures or statistics that measure results.  |

**Exercise 5.** *Say what terms are meant by the following descriptions?*

1. It can occur in an information system when classified information is found on a computer system which is not supposed to be there. This can happen by accident, by transmission of insecure data, because the information was changed to a different classification rating, because users did not follow protocol and transferred information through insecure methods such as floppy disks or thumb drives. It can also occur through a computer virus or other form of malware.

2. It is a type of software delivery model that is installed and operated from a customer's in-house server and computing infrastructure. It utilizes an organization's native computing resources and requires only a licensed or purchased copy of software from an independent software vendor. It is known as shrink wrap.

3. It is a set of commands, functions, and protocols which programmers can use when building software for a specific operating system. It allows programmers to use predefined functions to interact with the operating system, instead of writing them from scratch.

4. This concept is used in numerous fields such as cybernetics, biology, ecology, network theory, and non-linear dynamics. The concept can be summarized as all parts of a system interact with and rely on one another simply by the fact that they occupy the same system, and that a system is difficult or sometimes impossible to analyze through its individual parts considered alone.

---

1) API; 2) condemnation; 3) interconnectivity; 4) On-Premise Software.

**Exercise 6.** *Find the following words and word combinations in the appropriate paragraphs of the text and explain what they mean in the given context.*

to stay on-premise (1); to voice fears (2); mission-critical sensitive data (2); to be wary of (2); alongside (2); a multi-tenant cloud (2); to be self-hosted by the company (6); to be off-premise (6); investment hurdle (7); continued maintenance requirements (7); to budget for needs (7); to override the initial planning costs (8).

**Exercise 7.** *Paraphrase the following statements simplifying their grammar.*

1. The business benefits from the cost and flexibility advantages offered by public cloud computing and can apply that model to the data that it feels happy to manage externally.
2. This is not to say that public cloud computing resources are insecure, but some companies are wary of housing their data alongside that of their competitors in what is known as a multi-tenant cloud.
3. This saves valuable network and hardware resources for continued enterprise use while allowing the IT department to fully vet software-in-progress before going live and without fear of harming the current network.
4. Public clouds allow for a low investment hurdle to activate and can be cheaply scaled to more or less servers and network connections as needed.
5. The goal of a hybrid cloud system is to provide as many benefits of the public and private cloud as possible while not incurring the risks associated with them.

**Exercise 8.** *Answer the following questions.*

1. What are two types of cloud used by companies?
2. How do public and private clouds differ by their functions?
3. Why does hybrid cloud make business sense?
4. What challenge does the hybrid cloud offer?
5. What is 'hybrid' cloud computing?
6. What is the "hybrid cloud"?
7. What do companies use public and private clouds for?
8. When is the public cloud used as a test bed?
9. Why should IT managers be careful with the mixture of public and private clouds?
10. What are the benefits of the hybrid system?
11. What are the downsides of the hybrid system?
12. What is the goal of a hybrid cloud system?

**Exercise 9.** *Pick up from the text all the information relating to the public and private clouds. Prepare a short utterance about a) the public cloud; b) the private cloud.*

**Exercise 10.** *Make up the summary and the abstract of the text in the writing.*

**Vocabulary**

crawl (v)	медленно двигаться, ползти
reciprocal links	взаимные ссылки (связи)
search engine	поисковая система
spider	поисковый агент
URL	унифицированный указатель информационного ресурса
supplement (v)	дополнять
rank (v)	ранжировать, располагать (в определенном порядке)
bid on/for (v)	делать заявку на что-то, предлагать
verbiage	фразеология; словесное выражение
meet a criteria	отвечать критериям
to refine (v)	уточнять, детализировать
“Brick-and-Mortar”	традиционная торговля через обычные магазины

(1) A Search Engine is not an engine in the normal sense, but it is actually a software program that searches websites, documents, images, and even videos for specific keywords. It returns a list of results where the keyword or search term you typed was found. A Search Engine is actually a system, the system which is made up of the hardware and software components of a computer. Google and Yahoo are considered systems because they are computers with software running on them. Search Engines are very complex and the search algorithms are updated continuously.

(2) Search Engines use computer robot programs called spiders to gather and store the information you're searching. Spiders find the pages and then pass the information on to another program for indexing. The spider identifies the data and then stores it in the search engines database. The spiders crawl along the web and find information about content by following other links that have previously been crawled. This is why it's important to have links to useful content on your website, and also have other website link

back to you. This process of linking is called reciprocal links, or back linking. If you launch a website, but never link to other pages, your site will more than likely not be found by the spiders. If your page has fresh content on it, then the spiders will find you eventually, although it takes more work and you have to manually submit the new Uniform Resource Locator to the search engines indexing program.

(3) URL is the Uniform Resource Locator for a website. It can also be referred to as a domain name. Domains with rich keywords that get searched a lot have a better chance at success in the search engines. The URL for Google is google.com, and Microsoft has live.com. One popular search engine, Ask Jeeves, has recently changed its name to Ask.com. Shorter domains have more brand power and have sold for millions of dollars on the open domain market. Short, three or four letter domains are very rare and are owned by major players in the online world.

(4) Search Engines have become a very important aspect of commerce online. Companies use Commerce or online commerce to support and supplement their traditional “Brick and Mortar” locations. Search Engines are used to find specific products that consumers are looking for to buy online. Having your website come up in the search listings and providing the customers with the product or information they are searching for is a key. People are paying top dollar to be ranked at the top of the search engines.

(5) Keywords are the terms that you type in the search engine. If it matches the content that the search engine has stored in the database, the results are returned. Short keywords like “Car” will return millions of results. To find more specific, targeted results you can use long tail keywords which are also used when the website wants to refine search terms. If you were searching cars, for instance, you might want to include the brand name or city you want to buy it from. This will return more specific search results for your specific need. Working with long tail keywords successfully means that a publisher needs to know which long tail keywords actually get hits or are searched for on the major search engines. Research is the only way to know if long tail keywords will work or not. Google offers advertising where you can bid on specific keywords. This type of advertising is called Pay-Per-Click Advertising. When the terms are searched, your ad

shows up and you pay every time someone clicks your ad. PPC is a very popular form of advertising in Search Engines. Keyword research tools help with finding the specific terms that people are searching. They also tell you the average monthly volume for a specific keyword, and the amount of competition there is for that word as well. Click Through Rate is the average percentage of clicks vs the average times your ad was actually viewed. Ad copy and verbiage play a very important role as to how effective your Search Engine advertisements are.

(6) Ranking in a search engine is also very important. This is referred to as the rank or position of the results returned by the Search Engine. When you enter a term or keyword in Google for instance, the most relevant results appear first. Ranking high in the search engines is a science in itself and high ranks mean big money for businesses. If you can rank constantly on the first page of the results, your success is almost guaranteed. The Search Engines use a variety of criteria that the websites and other data types must meet in order to rank high in the given Search Engine for a given term. Social marketing is also another way to get ranked. Search Engines love websites like MySpace.com, YouTube.com, and Digg.com because they always have fresh content to be indexed and have a multitude of links to follow. Every time someone submits a new article or blog posting, the spiders are there to index it. This is why social profiles are generally indexed in the Search Engines even before a site that just launched. Search Engines play a vital role in everyday life. People use them to study, work and play. Specialists in computers have made studying and mastering Search Engines a daily journey, constantly learning new things about how they function and how to get top rankings.

**Exercise 1.** *Which of the following statements expresses the main idea of the text?*

1. A Search Engine is the system which is made up of the hardware and software components of a computer.
2. Search Engines are very complex.
3. Search Engines have become a very important aspect of commerce online.

**Exercise 2.** Give the number of the paragraph which says about:

- a) the functions of computer robot programs;
- b) the special tools designed to find the specific terms that people are searching;
- c) the definition of a search engine;
- d) the role of search engines in everyday life;
- e) the complexity of search engines;
- f) the role of search engines in developing trade;
- g) major players in the online world;
- h) the aspects influencing ads efficiency;
- i) the environment providing profit in business.

**Exercise 3.** Define whether the following statements correspond to the content of the text (true – T; false – F; not stated – NS).

1. A Search Engine is a system, the system which is made up of the hardware components of a computer.
2. The search algorithms are updated once a day.
3. The only function of spiders is to find the necessary information.
4. Uniform Resource Locator is the same as a domain name.
5. Search engines are actively used in online commerce.
6. Research is one of the ways to know if long tail keywords will work or not.
7. The term "social marketing" was coined in 1971 by Kotler and Zaltman.
8. When someone submits a new blog posting, they are indexed by spiders.

**Exercise 4.** Match the terms in the left column with their definitions.

- |                |   |
|----------------|---|
| 1. CTR         | <b>a.</b> the software that gathers specific information in an automated and orderly way from the Internet. |
| 2. advertising | <b>b.</b> contains a group of computers that can be accessed and administered with a common set of rules.   |

- |                     |  |
|---------------------|--|
| 3. verbiage         | c. is the highest amount being paid for a commodity or service.                                |
| 4. a domain         | d. selling goods, services or an idea that promotes the overall welfare of a community.        |
| 5. blog             | e. a way of measuring the success of an online advertising campaign.                           |
| 6. web spider       | f. When the context involves a software or hardware system, this refers to documentation.      |
| 7. social marketing | g. the promotion of goods or services for sale through impersonal media (radio, TV, Internet). |
| 8. top dollar       | h. a website containing short articles called posts that are changed regularly.                |

**Exercise 5.** *Find the following words and word combinations in the appropriate paragraphs of the text and explain what they mean in the given context.*

to update continuously (1), to identify the data (2), to crawl along the web (2), to manually submit (2), a domain (3), to match the content (5), targeted results (5), get hits (5), show up (5), constantly (6), blog posting (6), to master Search Engines.

**Exercise 6.** *Say what terms are meant by the following descriptions?*

1. A conceptual two-point segment of an end-to-end circuit that connects two end users and enables them to communicate, even when two separate physical paths are used. In a satellite radio link, for example, there is an uplink from the Earth station (i.e., antenna) to the satellite and a downlink from the satellite to the Earth station.
2. Hyperlinks placed between two web pages in exchange for the other page linking back. They are an important part of search engine optimization as engines like Google rank the web pages in their results by the num-

ber of different pages link to yours. By participating in link exchanges, a site can increase its rank within the search engine's results.

3. A computer program that searches documents, especially on the World Wide Web, for a specified word or words and provides a list of documents in which they are found.

4. A formatted text string used by Web browsers, email clients and other software to identify a network resource on the Internet. Network resources are files that can be plain Web pages, other text documents, graphics, or programs.

5. A great way to quickly start generating traffic and solid sales to your website. When a user searches in “Google”, “Yahoo”, “Bing”, Social Media network or their affiliate websites, you can bid for a search term and have an ad displayed in the results. These ads are displayed on the top side of search results.

---

1) URL; 2) search engine; 3) link; 4) Pay-Per-Click Advertising.

**Exercise 7.** *Paraphrase the following statements simplifying their grammar.*

1. If you launch a website, but never link to other pages, your site will more than likely not be found by the spiders.

2. If your page has fresh content on it, then the spiders will find you eventually, although it takes more work and you have to manually submit the new Uniform Resource Locator to the search engines indexing program.

3. Domains with rich keywords that get searched a lot have a better chance at success in the search engines.

4. Having your website come up in the search listings and providing the customers with the product or information they are searching for is a key.

5. Working with long tail keywords successfully means that a publisher needs to know which long tail keywords actually get hits or are searched for on the major search engines.

6. Specialists in computers have made studying and mastering Search Engines a daily journey, constantly learning new things about how they function and how to get top rankings.

**Exercise 8.** *Answer the following questions.*

1. What is meant by the computer term “Search Engine”?
2. What are the functions of computer spiders?

3. What is the principle of a computer spider operation?
4. Who usually possesses shorter domains in online world?
5. What is the difference between online and “Brick and Mortar” commerce?
6. What is the role of keywords?
7. When is it necessary to work with long tail keywords?
8. What does the efficiency of your Search Engine advertisements depend on?
9. What is ranking and what does high ranking mean for business?
10. Why are specialists in computers continuously working at learning Search Engines?

**Exercise 9.** 1) *Make up the plan of the text;*

2) *Make up the summary and the abstract of the text.*

## *Charter II*

### **INFORMATION TECHNOLOGY SECURITY**

#### **UNIT 7            What is information technology security?**

#### **Vocabulary**

sensitive information	секретная информация
decipher (v)	шифровать
encryption	кодирование, шифрование
unauthorized access	несанкционированный доступ
legitimate	законный
confidentiality	конфиденциальность
integrity	целостность
vulnerability	уязвимость
robustness	устойчивость
compromise (v)	подвергать риску
remote access	удаленный доступ
availability	доступность

tradeoff  
usability

компромисс  
практичность

(1) Security is a basic human concept that has become more difficult to define and enforce in the Information Age. In primitive societies, security was limited to ensuring the safety of the group's members and protecting physical resources, like food and water. As society has grown more complex, the significance of sharing and securing the important resource of information has increased. Before the proliferation of modern communications, information security was limited to controlling physical access to oral or written communications. The importance of information security led societies to develop innovative ways of protecting their information. For example, the Roman Empire's military wrote sensitive messages on parchments that could be dissolved in water after they had been read. Military history provides another more recent example of the importance of information security. Decades after World War II ended, it was revealed that the Allies had gained an enormous advantage by deciphering both the German and Japanese encryption codes early in the conflict. Recent innovations in information technology, like the Internet, have made it possible to send vast quantities of data across the globe with ease. However, the challenge of controlling and protecting that information has grown exponentially now that data can be easily transmitted, stored, copied, manipulated, and destroyed.

(2) Within a large organization information technology generally refers to laptop and desktop computers, servers, routers, and switches that form a computer network, although information technology also includes fax machines, phone and voice mail systems, cellular phones, and other electronic systems. A growing reliance on computers to work and communicate has made the control of computer networks an important part of information security. Unauthorized access to paper documents or phone conversations is still an information security concern, but the real challenge has become protecting the security of computer networks, especially when they are connected to the Internet. Most large organizations have their own local computer network, or intranet, that links their computers together to share resources and support the communications of employees and others with a legitimate need for access. Almost all of these networks are connected to the Internet and allow employees to go "online."

(3) Information technology security is controlling access to sensitive electronic information so only those with a legitimate need to access it are allowed to do so. This seemingly simple task has become a very complex process with systems that need to be continually updated and processes that need to constantly be reviewed. There are three main objectives for information technology security: confidentiality, integrity, and availability of data. Confidentiality is protecting access to sensitive data from those who don't have a legitimate need to use it. Integrity is ensuring that information is accurate and reliable and cannot be modified in unexpected ways. The availability of data ensures that is readily available to those who need to use it.

(4) Information technology security is often the challenge of balancing the demands of users versus the need for data confidentiality and integrity. For example, allowing employees to access a network from a remote location, like their home or a project site, can increase the value of the network and efficiency of the employee. Unfortunately, remote access to a network also opens a number of vulnerabilities and creates difficult security challenges for a network administrator.

(5) Information Security involves a Tradeoff between Security and Usability: There is no such thing as a totally secure system – except perhaps one that is entirely unusable by anyone! Corporate Information Security's goal is to provide an appropriate level of security, based on the value of an organization's information and its business needs. The more secure a system is, the more inconvenience legitimate users experience in accessing it.

**Exercise 1.** *Which of the following statements expresses the main idea of the text?*

1. Information technology security is simply the process of keeping information secure.
2. Protecting sensitive information and the security of computer networks is the main concern of ITS.
3. ITS provides appropriate level of security.

**Exercise 2.** *Give the number of the paragraph which says about:*

Organization of information technology security within large companies; main objectives of information technology security; basic concept of security; totally secure computer systems; legitimate need for access; balanc-

ing the demands of users versus the need for data confidentiality; availability of data; protecting the security of computer systems; origins of information technology security; local computer networks.

**Exercise 3.** *Match the terms with their definitions:*

1. Integrity
  2. Vulnerability
  3. Information security
  4. Encryption
  5. Confidentiality
  6. Availability
- a. Application of cryptography to make information unintelligible, i. e. translating plaintext into ciphertext using a prescribed algorithm and a key.
  - b. Not permitted, accepted or agreed by management.
  - c. One of the three core elements of information security, along with availability and integrity. It essentially concerns secrecy or privacy.
  - d. The preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
  - e. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to violate system security policy and result in a security breach.
  - f. Property of completeness and accuracy of information. Protected through controls such as referential integrity, data entry validation, digital signatures, honesty, ethics and trust. One of the three core elements of information security, along with confidentiality and availability.

7. Unauthorized

g. One of the three core elements of information security, along with confidentiality and integrity. It concerns the requirement for information, IT systems, people and processes to be operational and accessible when needed.

**Exercise 4.** *Define whether the following statements correspond to the content of the text (yes, no).*

1. Security is a basic human concept that is easy to define.
2. Information security is limited to controlling physical access to oral or written information.
3. The requirements for controlling and protecting information have grown exponentially.
4. Control of computer networks is an important part of ITS.
5. Protecting the security of computer networks, especially when they are connected to the Internet, has become the real challenge.
6. Information technology security is controlling access to all electronic information.
7. There are three main objectives for ITS: confidentiality, integrity and availability of data.
8. Allowing employees to access a network from a remote location can decrease the number of vulnerability.
9. Information technology security is a responsibility only of those who are directly concerned with it.

**Exercise 5.** *Paraphrase the following statements simplifying their grammar.*

1. Decades after World War II ended, it was revealed that the Allies had gained an enormous advantage by deciphering both the German and Japanese encryption codes early in the conflict.
2. Unauthorized access to paper documents or phone conversations is still an information security concern, but the real challenge has become protecting the security of computer networks, especially when they are connected to the Internet.
3. Information technology security is controlling access to sensitive electronic information so only those with a legitimate need to access it are allowed to do so.

4. This seemingly simple task has become a very complex process with systems that need to be continually updated and processes that need to constantly be reviewed.
5. Allowing employees to access a network from a remote location, like their home or a project site, can increase the value of the network and efficiency of the employee.

**Exercise 6.** 1) *Give the definitions of the following terms:*

- a) Intranet; b) confidentiality; c) integrity; d) availability of data.

2) *Deduce your own definition of ITS.*

**Exercise 7.** *Answer the following questions:*

1. Did the problem of security exist in primitive societies?
2. Why has the significance of sharing and securing the important resources of information increased in a modern society?
3. What examples of the importance of IS are given in the text?
4. What has made the control of computer networks an important part of ITS?
5. What is the most important task of ITS?
6. Who is allowed to get access to sensitive electronic information?
7. What are the 3 main objectives of ITS?
8. What are the advantages and disadvantages of an access from a remote location?
9. Are there any totally secure systems?

**Exercise 8.** *Arrange the following headings in the logical order. Match them with the paragraphs of the text. Make up the summary of the text.*

1. The demands of users versus the need of data confidentiality and integrity;
2. Responsibility for ITS;
3. History of information security;
4. Main objectives of ITS;
5. ITS in the digital era.

## UNIT 8

## Data classification

### Vocabulary

sensitivity	степень конфиденциальности
top secret	совершенно секретный
secret	секретный
confidential	данные ограниченного пользования
security clearance	проверка на отсутствие нарушений секретности
public information	информация, доступная неограниченному кругу лиц
level of protection	уровень защиты
backup	резервное копирование
adequate security control	соответствующий контроль безопасности
fraudulently obtained	полученный обманным путем

(1) One of the foundational elements of an information security program is the existence of and adherence to a formal data classification scheme. Yet, many organizations—even those that profess a commitment to protecting company and customer information—fail to implement data classification. We will look at the reasons that data classification can be difficult and offers several practical guidelines to overcome these obstacles.

### *What is data classification?*

(2) Data classification is a simple concept. It is a scheme by which the organization assigns a level of sensitivity and an owner to each piece of information that it owns and maintains. In a hospital, for example, a data classification scheme would identify the sensitivity of every piece of data in the hospital, from the cafeteria menu to patient medical records. The most widely recognized data classification scheme is the one used by governments, such as the U.S., which assigns classifications such as:

- Top secret
- Secret
- Confidential

(3) When a document, letter, memo, or other piece of information is created, the owner assigns to it a classification level, which among other things, defines the security clearance of individuals that can access that information.

(4) Similarly, in business, organizations adopt data classification schemes to define the levels of confidentiality that are required for each piece of information created or maintained by the organization. A corporate data classification scheme might comprise information classifications such as:

- Company confidential
- Private
- Sensitive
- Public

(5) Such a scheme greatly facilitates data security, because it instantly identifies and communicates the level of protection required for any piece of data as well as the audience that may view it. For example, a document that is tagged as "company confidential" is easily recognized as not to be released outside of the company. Further, it limits those who may access the information to a defined group.

(6) A good data classification scheme also includes a time-element, to allow a piece of information to change its status on a certain date. An example would be a public company's earnings announcement, which might be company confidential until the date of the earnings announcement, at which time it becomes "public."

(7) There are many other attributes to data classification schemes, but these few points are sufficient to establish why data classification is fundamental to information security. Without a data classification scheme, an organization treats all information the same. This increases the probability that sensitive data will not have adequate security controls, increasing the risk of sensitive data being compromised. It also means that less sensitive data will have more security controls than necessary, leading to unnecessary restrictions and loss of efficiency for operational personnel.

#### *Consequence of failure in data classification*

(8) Two high profile cases in 2005 show the severe losses that can arise when data is not properly classified, the scheme is not adhered to in prac-

tice, or the scheme is not used to drive security controls appropriate for each class of data.

(9) In early 2005, ChoicePoint, a U.S. firm that provides information on consumers to insurance companies and other types of businesses and government agencies, revealed that criminals had fraudulently obtained valid customer accounts that enabled access to approximately 150,000 consumer names, addresses, Social Security numbers, and credit reports. Clearly, the security controls that ChoicePoint had in place for its new customer account setup process were not adequate for the class of data that it allowed such customers to access.

(10) Around the same time, Bank of America disclosed that it lost several backup tapes in transit to a backup center. The tapes contained financial information on 1.2 million government employees that were members of the U.S. government's SmartPay credit card program. Although the Bank's data classification scheme may have recognized the confidential nature of such information when residing on the Bank's primary systems, it did not, in this case, appear to extend to the same information when it was contained on backup media.

(11) Although ChoicePoint and Bank of America can be faulted for not adequately protecting confidential information, it is likely that both organizations had a data classification scheme in place. The problem was that they did not have adequate security controls based on the classification, at least in these instances.

(12) Many organizations have an even more fundamental problem: they do not have any data classification scheme at all. If data classification is a foundational requirement for information security, what explains this failure?

(13) First, data classification is one place where the old maxim is true: perfection is the enemy of the good. Some security professionals insist upon a scheme that is perfect in theory, but difficult to implement. For example, if most users are ignorant of basic security practices, successfully implementing a robust data classification scheme will be extremely challenging. A data classification program will only be effective if employees are willing to properly classify each piece of information and maintain the classifica-

tion. An organization will be better served by a simple data classification scheme that is put into practice – even one that is theoretically imperfect – than the perfect scheme that exists in name only.

(14) Second, the development and implementation of data classification can be downright expensive. The costs are two-fold: the cost of developing the data classification scheme with appropriate controls based on each class of data and then training all employees to recognize and classify data accordingly. The development and training effort can be significant, but there is even more effort required to classify existing data and to continue to classify new data on an on-going basis. For healthcare organizations, financial services firms, and others that are required by law to classify data, the cost of these efforts may be rationalized in terms of regulatory compliance. But for non-regulated organizations, it is often difficult for management to justify such efforts as a necessary part of doing business.

Finally, the leaders of the security program – the chief information security officer, and others – often lack the authority to drive a data classification program through to full implementation. In many companies, the security program does not have the political clout required to gain acceptance for such an ambitious initiative.

**Exercise 1.** *Which of the following statements expresses the main idea of the text?*

1. Data classification is one of the foundational elements of information security.
2. Each piece of information created should be assigned its classification level.
3. Without a data classification scheme an organization might suffer from constant security breaches.

**Exercise 2.** *Give the number of the paragraph which says about:*

not adequate security control based on the classification of data; time – element; cost of development and implementation of data classification; definition of data classification; classification of data that might be compromised; most widely recognized data classification scheme; security clearance; data classification as fundamental to information security; data classification as a foundational requirement for information security.

**Exercise 3.** *Define whether the following statements correspond to the content of the text (yes, no).*

1. Data classification is of the least concern for many organizations.
2. Data classification is a scheme by which an organization defines an owner to each piece of information.
3. According to the classification used by the US government all information can be assigned as top secret, secret and public.
4. After creating any piece of information the owner should assign to it a classification level.
5. Most corporate data classification scheme might comprise the following levels of confidentiality – company confidential, private, sensitive, public.
6. Data classification scheme limits access to the information.

**Exercise 4.** *Match the terms with their definitions:*

- |                   |  |
|-------------------|--|
| 1. Sensitive      | <b>a.</b> Highly sensitive internal documents that could seriously damage the organization if such information were lost or made public. It has very restricted distribution and must be protected at all times. Security at this level is the highest possible. |
| 2. Public         | <b>b.</b> The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.   |
| 3. Top secret     | <b>c.</b> Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level is minimal.  |
| 4. Confidential   | <b>d.</b> Privileged or proprietary information which if compromised by corruption, alteration, loss or misuse, could cause serious harm to the organization owing it.   |
| 5. Access control | <b>e.</b> It is not available or disclosed to unauthorized individuals.  |

**Exercise 5.** *Paraphrase the following statements simplifying their grammar.*

1. When a document, letter, memo, or other piece of information is created, the owner assigns to it a classification level, which among other things, defines the security clearance of individuals that can access that information.
2. A document that is tagged as “company confidential” is easily recognized as not to be released outside of the company.
3. It increases the probability that sensitive data will not have adequate security controls, increasing the risk of sensitive data being compromised.
4. Although the Bank’s data classification scheme may have recognized the confidential nature of such information when residing on the Bank’s primary system, it did not, in this case, appear to extend to the same information when it was contained on backup media.
5. The development and training effort can be significant, but there is even more effort required to classify existing data and to continue to classify new data on an ongoing basis.

**Exercise 6.** *Give your own interpretation of the following words and word combinations used in the text:*

- a) Data classification; b) a classification level; c) a corporate data classification scheme; d) a time-element; e) adequate security control.

**Exercise 7.** *Answer the following questions.*

1. What is one of the foundational elements of an information security program?
2. What is data classification?
3. What is the most widely recognized data classification scheme?
4. When should a document be given its classification level?
5. What classification levels does a corporate data classification scheme comprise?
6. How can you explain the term “a time-element”?
7. Why is data classification fundamental to information security?
8. How did the criminal obtain the access to valid customers’ accounts of ChoicePoint insurance company?
9. Was the Bank of America data classification scheme properly organized?

10. What were the consequences of failure in data classification in Choice-Point and Bank of America?
11. Why is implementing of data classification difficult?
12. What does the cost of implementation of data classification include?

**Exercise 8.** *Divide the text into logical abstracts and give each of them its logical name. Write at least 4 sentences to each item of your plan. Make up the summary of the text.*

## **UNIT 9**

### **How does a computer virus work?**

#### **Vocabulary**

Intricate	запутанный, замысловатый
Cell	клетка
Loophole	лазейка
Bragging right	повод для гордости
Rely on (v)	надеяться, полагаться
Shut off (v)	отключать
Crack down on (v)	расправиться

(1) You might be surprised to find out that computer viruses are in reality marvels of the Information Age! So let us have a look at how computer viruses work... Although computer viruses are very simple computer programs, a properly engineered virus can have a devastating effect, causing information loss and damages of billions of dollars. For example, the Melissa virus (March 1999) forced Microsoft and other corporations to completely shut off their email system. That was a wonder of modern programming and nothing could stop it at that time.

(2) Computer viruses work much the same way that biological viruses work. This is actually why they are called viruses. However, instead of a computer virus being passed from one person to another, they are passed from one computer to another. A biological virus requires a virus to attach itself to another cell in the body and pass the virus into the cell. The virus

will then use the components of the healthy cell to reproduce itself. In this case, the cell will either become so full of the replicated virus cells that it eventually bursts, releasing the virus on to other cells, or the cells of the virus will simply use the healthy cell to launch the virus cells to other healthy cells one at a time. A computer virus works much the same way.

(3) Viruses are small pieces of software that attach themselves to real software (or even media, like photos, mp3s, or movies). Whenever a user runs the infected file(s), the virus comes to life and can either replicate and infect other programs and files, or explode with its full power. That in general is how a computer virus works. Nowadays viruses are mainly focused on replication. Otherwise, they would be useless. Of course, they can erase the entire hard disk of your computer, but that is all.

(4) Once the healthy program starts running, the computer virus will then be able to run, attach itself to other programs, and cause major destruction. Computer viruses, unlike biological viruses, are created by people. People write code that contains a computer virus, then test it to make sure that it works, and attach some form of action to the virus. That action is whatever the virus will do once it lands on a computer. Attaching this action is when the virus creator either makes the virus come up with a happy face on someone's computer or erase their entire hard drive. There are a few reasons why people write such destructive viral codes. One is simply because they know how. And when they find a security loophole in a computer, they want to take advantage of it before someone else does. Others do it just for the thrill, just like others draw graffiti or break into cars simply for a thrill. And of course, there's always bragging rights that go along with creating a particularly intricate and complicated virus that's hard to crack. However, because government officials are starting to crack down on these virus creators that cause so much damage, those bragging rights might become a thing of the past!

(5) There are two phases in how a computer virus works. The first phase is the infection phase. Once the user runs the infected entity, the virus will load into memory. It then scans for other programs and attempt to spread and infect them as well. It does this by modifying the program to add its code. Depending on its complexity, the computer virus might also attempt to search for, and infect, PCs linked to the infected computer, throughout

the network. After the replication, the virus launches the real program, so the user has no knowledge of the infection. If this were the only thing a computer virus can do, nobody would hate them so much. However, now comes the dangerous phase.

(6) Most viruses have an attack phase, which causes the damage. This attack phase is triggered by a random event. For example, one might open Windows Media Player and trigger the virus. Other triggers, such as a specific date, or a specific number of replications are also used. Some viruses also react to antivirus software or to different files on the hard drive. There are viruses know to disable antivirus tools to make sure they are free to do whatever they were programmed to do. In the attack phase, the virus can do virtually anything from printing a message on the screen to a total erase of the user's hard disk.

(7) This gives you a basic idea of how a computer virus works and the results can be catastrophic to the user. In a manner of seconds, you can lose months of work or, worse, lose your entire computer. There are viruses that are so aggressive that they render computers unusable. Well, at least until some parts of them are replaced. One might be lucky and end up with a silly message on the screen or a few mp3s deleted, but these are very friendly viruses. But all hope is not lost and people don't simply have to rely on the hope that a virus doesn't land on their computer. There are many security measures that any computer user can take to protect themselves against computer viruses. Traditional viruses, although less common now, can be protected against by running a more secure operating system such as Unix on a computer. Viruses on these types of operating systems are virtually unheard of because no one except the authorized user ever has access to the hard drive. For operating systems such as MAC or Windows, it's extremely important to place some virus protection such as Norton or McAffey on the computer to keep it safe and protected against viruses. It's also important to never open any executable attachments that come with email messages. Files that have EXE, COM, or VBS are executable programs. Once you open them, you give them free access to your computer, allowing them to do whatever they wish. Programs found on the Internet are much more vulnerable to viruses than programs that are purchased on CD. Because of this, buying software from manufacturers that comes on its own CD is sure to be a better safeguard against viruses than downloading

programs online. Lastly, it's also very important to stay informed on what new security patches can be downloaded to protect PCs. By taking these few simple steps, you can be sure that you are doing what you can to save yourself major headaches down the road.

**Exercise 1.** *Which of the following statements expresses the main idea of the text?*

1. Most viruses have two phases of work – an attack and infection phase.
2. Viruses are created by people for different reasons.
3. Programs found on the Internet are much more vulnerable to viruses than programs that are purchased on CD.

**Exercise 2.** *Give the number of the paragraph which says about:*

2 phases of a computer virus work; the reasons why people write destructive viral codes; an attack phase of a virus; resemblance of a computer virus to a biological virus; general ways of a computer virus work.

**Exercise 3.** *Define whether the following statements correspond to the content of the text (yes, no).*

1. Computer viruses are rather complicated computer programs.
2. Whenever a user runs the infected file(s), the virus comes to life and can either replicate and infect other programs and files, or explode with its full power.
3. All viruses have two phases – an attack phase and an infection phase.
4. In the attack phase, the virus can do virtually anything from printing a message on the screen to a total erase of the user's hard disk.
5. There are viruses known to disable antivirus tools to make sure they are free to do whatever they were programmed to do.
6. Traditional viruses, although less common now, can be protected against by running a more secure operating system such as Unix on a computer.
7. Once you open executable programs, you give them free access to your computer, allowing them to do whatever they wish.
8. Downloading programs from the Internet is safe.

**Exercise 4.** *Match the terms with their definitions.*

- |                       |  |
|-----------------------|--|
| 1. to replicate       | <b>a.</b> A process of loading a virus into computer memory  |
| 2. viral code         | <b>b.</b> A mechanism that starts a series of events   |
| 3. an infection phase | <b>c.</b> To create a copy of something  |
| 4. an attack phase    | <b>d.</b> A code that contains a virus   |
| 5. trigger            | <b>e.</b> A piece of software designed to update a computer program, or its supporting data                                  |
| 6. executable program | <b>f.</b> A process of causing damage to software/hardware   |
| 7. security loophole  | <b>g.</b> a file containing a program that will run as soon as it is opened  |
| 8. patch              | <b>h.</b> A vulnerability in software, typically in the operating system, that enables an attacker to compromise the system. |

**Exercise 5.** *Paraphrase the following statements simplifying their grammar.*

1. That action is whatever the virus will do once it lands on a computer.
2. There are viruses know to disable antivirus tools to make sure they are free to do whatever they were programmed to do.
3. Depending on its complexity, the computer virus might also attempt to search for, and infect, PCs linked to the infected computer, throughout the network.
4. Viruses on these types of operating systems are virtually unheard of because no one except the authorized user ever has access to the hard drive.
5. Buying software from manufacturers that comes on its own CD is sure to be a better safeguard against viruses than downloading programs online.

**Exercise 6.** Give your own interpretation of the following words and word combinations used in the text:

A computer virus; a devastating effect; a healthy program; replication; a security loophole; an intricate virus; a friendly virus.

**Exercise 7.** Answer the following questions.

1. What problems can a computer virus cause?
2. Why are computer viruses called so?
3. What is a virus?
4. How do computer viruses spread?
5. What is the difference between a biological virus and a computer virus?
6. What are the reasons for creating viruses?
7. What are the two phases of a computer virus work?
8. What is done during the attack phase?
9. What is done during the infection phase?
10. What measures should be take for protecting your computer from virus attacks?

**Exercise 8.** Make up the plan of the text and render its content.

## **UNIT 10                      How does antivirus software work?**

### **Vocabulary**

With a clean sweep	с полной заменой
Registry folder	папка реестров
Common sense	здравый смысл
Keylogger	логгер клавиатуры
Odd	странный
Questionable	сомнительный
Alert (v)	предупреждать об опасности

(1) Antivirus software is practically a requirement for anyone using the Windows operating system. While it's true you can avoid computer viruses

if you practice safe habits, the truth is that the people who write computer viruses are always looking for new ways to infect machines. There are several different antivirus programs on the market - some are free and some you have to purchase. Keep in mind that free versions often lack some of the nicer features you'll find in commercial products.

(2) Let's start with the assumption that you're able to run antivirus software. Assuming your antivirus software is up to date, it should detect malware on your machine. Most antivirus programs have an alert page that will list each and every virus or other piece of malware it finds. You should write down the names of each malware application your software discovers.

(3) Many antivirus programs will attempt to remove or isolate malware for you. You may have to select an option and confirm that you want the antivirus software to tackle the malware. For most users, this is the best option - it can be tricky removing malware on your own. If the antivirus software says it has removed the malware successfully, you should shut down your computer, reboot and run the antivirus software again. This time, if the software comes back with a clean sweep, you're good to go. If the antivirus software finds different malware, you may need to repeat the previous steps. If it finds the same malware as before, you might have to try something else.

(4) If you can't access your antivirus software or you keep seeing the same malware pop up scan after scan, you may need to try and start your computer in Safe Mode. Many computer viruses will store files in your Windows registry folder. This folder acts like a database of instructions and tells your operating system important information about the programs you have on your computer. It can also tell viruses to activate as soon as the operating system loads. Starting your computer in Safe mode allows you to work with your machine using only the core elements of the Windows OS.

(5) Try running your antivirus software in this mode. If you see new malware pop up, you may have hit upon your solution. Some malware exists only to download other kinds of malware and install them on your machine. If you can remove all of these applications, you'll be in good shape. If for some reason your antivirus software can't remove the virus on its own, it's time to do a little more research. Remember when we said you

should write down the names of all the malware applications that your software discovered? Here's where that comes into play. You'll need to re-search each of those files online using the appropriate Internet security firm. Make sure to use the same firm that produces the antivirus software you're using. That's because different firms sometimes give the same virus different names. Not all firms will refer to the same virus the same way.

(6) Most Internet security firms will list all the files associated with a particular virus and tell you where you can expect to find those files. You may have to do some digging to find each file. Before you delete any files, you should save a backup copy of your Registry folder. If you accidentally delete the wrong file, you may make it difficult or impossible to run your computer properly. Delete all the files associated with the malware on your list. Once that's done, you'll need to reboot your computer and run your antivirus software again. Hopefully nothing else will pop up. You may want to update your login information for your various accounts online. Some malware has keylogging software that can send your passwords and information to a remote user. It's better to be safe than sorry.

(7) There are some simple rules you can follow that will help you avoid computer viruses. Most of these fall under the category of common sense.

- Don't open strange e-mail attachments or click on hyperlinks in e-mail. Virus programmers love to trick people into clicking on links that will lead them to malicious software. Let people know that you don't click on hyperlinks in e-mail unless the sender includes a description of the link and what it leads to. If your e-mail client supports autolaunch, turn it off. Otherwise you might automatically activate a computer virus just by opening the e-mail.

- The same applies to other messages you might encounter. Hyperlinks in message boards, Facebook messages or instant messages can sometimes lead to malware. Pay attention to the source of the message. Look for any unusual signs like misspellings or odd sentence structure, particularly if the person who sent you the message normally avoids errors. If you do see an odd link, you may want to let the sender know – he or she might be the victim of a hacked account.

- Don't visit questionable Web sites. This includes everything from software and music to video piracy sites. Many current Web browsers will alert you if you try to go to a site that is known for hosting malware. Pay attention to these warnings and stay away from those sites.

- Pay close attention to any windows that pop up while you surf the Web. If you see a notification claiming that you need to download the latest video driver to watch something, use caution. This is a common tactic used to distribute malware.

- Run your antivirus software at least once a week. You should also make sure your antivirus software and OS remain current by downloading updates and patches on a regular basis. Most antivirus software updates at least once a week as security firms add more virus information to their databases.

- Avoiding viruses might sound like a lot of work but keep in mind it's easier than fixing a computer that's been hit with a virus.

**Exercise 1.** *Which of the following statements expresses the main idea of the text?*

1. If you run your antivirus software regularly your computer will be save from malicious programs.
2. Antivirus software is practically a requirement for anyone using the Windows operating system.
3. You should follow a certain set of rules to keep your computer virus free.

**Exercise 2.** *Give the number of the paragraph which says about:*

Safe mode; Windows registry folder; information on an alert page; different kinds of antivirus software; hyperlinks that might lead to malware; rebooting and running antivirus software after removing malware; different names for the same viruses.

**Exercise 3.** *Define whether the following statements correspond to the content of the text (yes, no).*

1. If you practice safe habits, you can avoid computer viruses.
2. You have to purchase all antivirus software programs.

3. All antivirus software programs have an alert page that will list each and every virus or other piece of malware it finds.
4. Many antivirus programs will attempt to remove or isolate a virus without your assistance.
5. You should always reboot your computer after the malware has been deleted successfully.
6. Many computer viruses will store files in your Windows Registry folder.
7. All malware exists only to download other kinds of malware and install them on your computer.
8. Before deleting any files you should save a backup copy of your Registry folder.
9. You may automatically activate a computer virus just by clicking on unknown links.
10. All current Web browsers will alert you if you try to go to a site hosting malware.
11. You should always make sure your antivirus software and operating system remain current by downloading updates and patches.

**Exercise 4.** *Match the terms with their definitions.*

- |                              |   |
|------------------------------|---|
| 1. malware                   | a. to remove power from a computer's main components in a controlled way.   |
| 2. to shut down the computer | b. a running computer system is restarted, either intentionally or unintentionally.   |
|                              | c. any type of software used to disrupt computer operation, or gain access to private computer.   |
| 3. rebooting                 | d. a file sent with an e-mail message   |
| 4. registry folder           | e. a way for the Windows operating system to run with the minimum system files necessary.   |
| 5. keylogging                | f. to start a computer automatically.   |
| 6. attachment                | g. the practice of covertly recording and monitoring keystrokes on a remote computer, typically using a dedicated software applications or piece of implanted hardware. |

- 7. autolaunch                      h. database used by Microsoft Operating system to store configuration information installed on a computer
- 8. safe mode                        i. and extra part or extension that is or can be sent along with an e-mail

**Exercise 5.** *Paraphrase the following statements simplifying their grammar.*

1. While it's true you can avoid computer virus if you practice safe habits, the truth is that the people who write computer viruses are always looking for new ways to infect machines.
2. Starting your computer in Safe mode allows you to work with your machine using only the core elements of the Windows OS.
3. Virus programmers love to trick people into clicking on links that will lead them to malicious software.
4. If you see a notification claiming that you need to download the latest video driver to watch something, use caution.
5. Many current Web browsers will alert you if you try to go to a site that is known for hosting malware.

**Exercise 6.** *Give your own interpretation of the following words and word combinations used in the text:*

Antivirus software; an alert page; reboot a computer; safe mode; clean sweep; login information; message board; questionable site; to remain current.

**Exercise 7.** *Answer the following questions.*

1. Is antivirus software a compulsory requirement for anyone using the Windows Operating System?
2. What information is listed on an alert page?
3. What is the best option for most users after a virus has been spotted on your computer?
4. What should be done if you keep seeing the same malware pop up scan after scan?
5. Where do many computer viruses store their files within an operating system?
6. Why is it important to write down the names of all the malware applications that your software discovered?

7. Do all firms use the same names for all the viruses?
8. Why should a backup copy of your Registry folder be saved?
9. How does keylogging software act?
10. How often should you run antivirus software?

**Exercise 8.** *Make up the plan of the text and render its content.*

## **UNIT 11**            **Types of computer crimes and their impact**

### **Vocabulary**

bundled software	стандартное ПО (поставляемое в комплекте с ПК)
original equipment	изготовитель комплексного оборудования
unbundling	разукомплектование
soft lifting	рассеивание ПО, незаконное размножение ПО
to counterfeit (v)	фальсифицировать, подделывать
peer-to-peer	пиринговый, децентрализованный
shareware	условно-бесплатное ПО
executable file	файл, содержащий исполнимый код
replicate (v)	копировать, тиражировать
backdoor (trapdoor)	«лазейка» (доступ в обход системы безопасности)
to disrupt (v)	подрывать, нарушать
retaliation	расплата, возмездие
ping of death	эхо-запрос нестандартного размера
to round down (v)	округлять в меньшую сторону
cumulative	совокупный
bogus	фиктивный

(1) Cyber crime is faster growing crime in the world with millions of people affected every day. The effects of one successful attack on a corporation can have far-reaching implications, including financial losses at the corporate level, to stock losses and money lost for consumer or stock hold-

ers. According to the Congressional Research Service, several computer security consulting firms estimate global financial losses from viruses, worm attacks and other hostile computer-based attacks to be between \$13 and \$226 billion. Laws have been swiftly put into place to halt these types of attacks, but criminals find haven in countries with lax cyber crime law. According to crime-research.org, as early as 2003 the United States was already leading the world in percentage of cyber attacks at 35,4 percent, followed by South Korea at 12,8 percent. Countries with high rates of computer piracy, such as Russia, have reacted slowly to cyber crime. Cyber attacks come in several forms, with the hacker varying his methods depending on the target, the situation and what he is seeking.

### *Software piracy*

(2) Most retail programs are licensed for use at just one computer site or for use by only one user at any time. By buying the software, you become a licensed user rather than an owner. You are allowed to make copies of the program for backup purposes, but it is against the law to give copies to friends and colleagues.

(3) Some common types of software piracy include counterfeit software, OEM unbundling, softlifting, hard disk loading, corporate software piracy, and Internet software piracy. OEM (original equipment manufacturer) unbundling involves disassembling the bundled software that is sold in conjunction with OEM hardware and installing it on other machines. soft lifting occurs when users share their software with other users who are not authorized to have access by the End-user License Agreement. Hard disk loading takes place when an unauthorized copy of commercial software is installed onto a computer system. The end user, or purchaser in this case, will then use the computer system with pirated software, often not realizing that the software that was pre-installed on the computer system is not legitimate. This type of piracy is most common with operating systems, especially older Microsoft branded operating system such as Windows 95 and Windows 98.

(4) Counterfeit software occurs when fake copies of software are produced in such a way that they appear to be authentic. Counterfeit software would include CD or DVD along with any accompanying manuals that the origi-

nal legitimate software was sold with, but sold at a price well below that of the legitimate software. Internet software piracy involves illegally obtained software, through Internet channels, usually through peer-to-peer file sharing systems or downloaded from pirate Web sites. Corporate software piracy occurs when corporations underreport the number of software installations acquired through volume purchase agreement.

(5) Originally, software companies tried to stop software piracy by copy-protecting software. This strategy failed, however. An entirely different approach to software piracy, called shareware, acknowledges the futility of trying to stop people from copying software and instead relies on people's honesty. Shareware publishers encourage users to give copies of programs to friends and colleagues but ask everyone who uses a program regularly to pay a registration fee to the program's author directly.

#### *Viruses, Worms and Trojan Horses*

(6) Viruses, worms and Trojan horses are all malicious programs that can cause damage to the computer, but there are differences among them.

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Some viruses may only cause annoying effects while others can damage your hardware, software or files. Almost all viruses are attached to an executable files, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, such as running an infected program, to keep it going.

(7) A worm is similar to a virus and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has capability to travel without any human actions. The biggest danger with a worm is its capability to replicate itself on your system. Your computer could send out hundreds or thousands of copies of the worm to everyone listed in your email address book, creating a huge devastating effect. In most cases the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding. In recent worm attacks are designed to allow malicious users to control the computer remotely.

(8) A Trojan Horse, at first glance, will appear to be useful software but actually do damage once installed or run on your computer. Though some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons), others can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

### *Denial of service attacks*

(9) The Denial of Service attack is primarily designed to disrupt the availability of the target server or network. Many times hackers launch DoS attacks in retaliation for a company's policies, or against a government for its actions. The main goal in a DoS attack is to make the target's resources unavailable to users. The "Ping of Death" is a common DoS attack method which the attacker sends a flood of "ping" commands to the target, eventually overwhelming it with requests.

### *Salami slicing*

(10) Salami slicing was employed successfully by criminally inclined IT staff to acquire large sums of money, by means of very small amounts. In a small example, a bank employee could always round down on transactions and pocket the difference. A few pennies here and there in small transactions is hard to spot, but the cumulative effect across numerous transactions could be significant. Salami slicing usually comes to light when the individuals involved are observed to be living well beyond their salary levels with no visible other means of support.

### *Spoofing*

(11) The word "spoof" means to hoax, trick or deceive. Therefore, in the IT world, spoofing refers to tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet. Spoofing can place on the In-

ternet in several different ways. One common method involves sending messages from a bogus e-mail address or faking the e-mail address of another user. IP spoofing involves masking the IP address of a certain computer system. Because IP spoofing makes it difficult to track the sources of a transaction, it is often used in denial-of-service attacks that overload a server. This may cause the server to either crash or become unresponsive to legitimate request. Finally, spoofing can be done by simply faking an identity, such as an online username. For example, when posting on a Web discussion board, a user may pretend he is the representative for a certain company when he actually has no association with the organization. In online chat rooms, users may fake their age and location.

### *Hijacking*

(12) Hijacking is a type of network security attack in which the attacker takes control of a communication between two entities and masquerades as one of them. In one type of hijacking, the criminal takes control of an established connection while it is in progress. The attacker intercepts messages in a public key exchange and then transmits them, substituting their own public key for the requested one, so that the two original parties still appear to be communicating with each other directly. The attacker uses a program that appears to be the server to the client and appears to be the client to the server. This attack may be used simply to gain access to the message, or to enable the attacker to modify them before retransmitting them.

(13) Another form of hijacking is browser hijacking, in which a user is taken to a different site than the one the user requested. The attacker gains access to DNS (Domain name system) records on a server and modifies them so that requests for the genuine Web page will be redirected elsewhere – usually to a fake page that the attacker has created. This gives impression to the viewer that the Web site has been compromised, when in fact, only a server has been.

**Exercise 1.** *Which of the following statements expresses the main idea of the text?*

1. Cyber crimes is faster growing crime in the world which cause enormous financial losses.

2. All types of cyber crimes are united by their goals.
3. Viruses, Trojan Horses and worms are the main types of malicious software.

**Exercise 2.** *Give the number of the paragraph which says about:*

Trojan Horses; shareware; IT spoofing; impact of cyber attacks; counterfeit software; malware designed to disrupt the availability of the target server or a network; common types of software piracy; a worm; corporate software piracy.

**Exercise 3.** *Define whether the following statements correspond to the content of the text (yes, no).*

1. Cyber crimes can be rather annoying, but hardly ever result in financial losses.
2. Computer criminals are hiding from law and justice by migrating into foreign countries.
3. Rates of cyber crimes in the USA are particularly low.
4. Viruses cannot damage computer hardware.
5. A virus cannot infect a computer unless a user runs or opens the malicious program.
6. Trojan horses are notorious for their ability to replicate themselves and send multiple copies to other computers.
7. A criminal involved into salami slicing can be easily spotted by the police.
8. Denial of the service attack is frequently preceded by IP spoofing.
9. Browsers hijacking results in redirecting users to a bogus site on the Internet.

**Exercise 4.** *Match the terms with their definitions.*

- |               |   |
|---------------|---|
| 1. Virus      | a. A concealed instruction to a computer that appears to be a useful application but actually does something destructive in the background. |
| 2. Phishing   | b. An illicit program that allows unauthorized entry.   |
| 3. DoS attack | c. Gaining an unauthorized access by using IP address of a trusted host.  |

- |                      |  |
|----------------------|--|
| 4. Trojan horse      | d. A person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject                                      |
| 5. Salami slicing    | e. A process of attempting to acquire confidential information such as username, passwords, and credit card details, by masquerading in an electronic communication. |
| 6. Trapdoor          | f. Programs sold with a computer or other hardware as a part of a package.   |
| 7. Software piracy   | g. A malicious program that can reproduce itself and cause damage to the computer software.  |
| 8. Spoofing          | h. Violating a license agreement by installing a legally purchased software on multiple unauthorized computers.  |
| 9. Hacker            | i. A file in a format that the computer can directly execute.  |
| 10. Cyber crime      | j. An act of illegally using, copying or distributing software without purchasing.   |
| 11. Bundled software | k. Making an imitation of something valuable with intention to deceive.  |
| 12. Softlifting      | l. Paralyzing a computer network by flooding it with large number of requests or data sent simultaneously from many individual computers.                            |
| 13. Counterfeit      | m. A criminal dealing with computers and networks.   |
| 14. Executable file  | n. A number of small illegal activities that creates a serious crime.  |

**Exercise 5.** *Paraphrase the following statements simplifying its grammar.*

1. The end user, or purchaser in this case, will then use the computer system with pirated software, often not realizing that the software that was pre-installed on the computer system is not legitimate.

2. Counterfeit software would include CD or DVD along with any accompanying manuals that the original legitimate software was sold with, but sold at a price well below that of the legitimate software.
3. An entirely different approach to software piracy, called shareware, acknowledges the futility of trying to stop people from copying software and instead relies on people's honesty.
4. In most cases the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding.
5. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised.

**Exercise 6.** *Give your own interpretation of the following words and word combinations used in the text:*

Cyber crime; counterfeit software; bundled software; shareware; softlifting; to fake user's age and location; to spread a virus without a human action; to compromise information.

**Exercise 7.** *Answer the following questions.*

1. What is the rate of growth of cyber crimes in the world?
2. What are the main types of cyber crimes?
3. What are the common types of software crimes?
4. What types of malware can you name?
5. What is the difference between a virus and a worm?
6. Trojan Horses are designed to be more annoying than malicious, aren't they?
7. What is the main goal of Denial of Service Attack?
8. What was Salami Slicing designed for?
9. What methods does spoofing involve?
10. What are the two main forms of hijacking?

**Exercise 8.** *Write at least 4 sentences to each heading given in the text and complete the summary of the text.*

## PART II

### TEXT 1

### Father of information theory

American mathematician Claude Elwood Shannon was born in Gaylord, Michigan on April 30, 1916. Shannon's father Claude was a judge in a small town of Gaylord, and his mother Mabel was the principal of the local high school. When a child, Shannon turned out to be mathematically precocious and received scientific encouragement from his grandfather, who



*Claude Shannon*

was an inventor and a farmer and whose inventions included the washing machine and farming machinery. From an early age, Shannon showed an affinity for both engineering and mathematics, and graduated from Michigan University with degrees in both disciplines. For his advanced degrees, he chose to attend the Massachusetts Institute of Technology. At the time, MIT was one of the prestigious institutions conducting research that would eventually formulate the basis for what is now known as the information sciences. Its faculty included mathematician Norbert Wiener, who would later coin the term cybernetics to describe the work in information theories that he, Shannon, and other leading American mathematicians were conducting. It also included Vannevar Bush, MIT's dean of engineering, who in the early 1930s had built an analog computer called the Differential Analyzer which was developed to calculate complex equations. It was a mechanical computer, using a series of gears and shafts. Its only electrical parts were the motors used to drive the gears. This work formed the basis for Shannon's influential 1938 paper "A Symbolic Analysis of Relay and Switching Circuits," in which he put forth his developing theories on the relationship of symbolic logic to relay circuits.

Shannon graduated from MIT in 1940 with both a master's degree and doctorate in mathematics. After graduation, he spent a year as a National Research Fellow at the Institute for Advanced Study at Princeton University. In 1941, Shannon joined the Bell Telephone Laboratories, where he became a member of a group of scientists charged with the tasks

of developing more efficient information transmitting methods and improving the reliability of long-distance telephone and telegraph lines. While working at the Bell Labs they started to develop the theory of the error-correcting code.

One of the most important features of Shannon's theory was the concept of information entropy. Entropy happened to be equivalent to a shortage in the information content in a message and this fact was proved by Shannon. According to physics' second law of thermodynamics, entropy is the degree of randomness in any system which increases over a period of time. Thus, many sentences can be significantly shortened without losing their meaning. Moreover a signal proved to be sent without distortion. So this concept has been developed over the decades into sophisticated error-correcting codes that ensure the integrity of the data on which society interacts. While studying the relay switches on the Differential Analyzer, Shannon noted that the switches were always either open or closed, or on and off. This led him to think about a mathematical way to describe the open and closed states. Shannon theorized that according to a binary system a switch in the on position would equate to one and in the off position, it would be a zero. Reducing information to a series of ones and zeros, he noticed that it could be processed by using on-off switches. He believed that information was no different than any other quantity and therefore could be manipulated by a machine.

In the late 1940s, Shannon's research was presented in "The Mathematical Theory of Communications". It was in this work that Shannon first introduced the word 'bit,' comprised of the first two and the last letter of 'binary digit' to describe the yes-no decision that lay at the core of his theories. Shannon's most important scientific contribution was his work on communication. In 1941 he began a serious study of communication problems, partly motivated by the demands of the war effort. This research resulted in the classic paper entitled "A mathematical theory of communication" in 1948. Combining mathematical theories with engineering principles he set the stage for the development of the digital computer and the modern digital communication revolution. The results were so breathtakingly original, that it took some time for the mathematical and engineering community to realize their significance. But soon his ideas were picked up, elaborated upon, extended, and complemented with new related ideas. As a

result a brand-new science had been created in the form of Information theory, with the publication of that single paper, and the frame work and terminology he established remains standard even today.

During the World War II, Alan Turing, a leading British mathematician spent a few months working with Shannon. Both scientists were interested in the possibility of building a machine that could imitate the human brain. In the 1950s, Shannon continued his efforts to develop what was then called "intelligent machines" – mechanisms that emulated the operations of the human mind to solve problems.

Shannon's information theories saw application in a number of disciplines in which a language is a factor, including linguistics, phonetics, psychology and cryptography. His theories also became a cornerstone of the developing field of artificial intelligence, and his famous conference at Dartmouth College in 1956 was the first major effort in organizing artificial intelligence research. He wrote a paper entitled "Programming a computer for playing chess" in 1950, and developed a chess playing computer.

Shannon's interest did not stop with these. He was known to be an expert juggler who was often seen juggling three balls while riding a bicycle. He was an accomplished clarinet player, too.

"Shannon was the person who saw that the binary digit was the fundamental element in all of communication," said Robert Gallager, a professor of electrical engineering who worked with Shannon at the Massachusetts Institute of Technology. "That was really his discovery, and from it the whole communications revolution has sprung," considered Marvin Minsky of M.I.T., who as a young theorist worked closely with Shannon.

Shannon received a plenty of numerous honorary degrees and awards. His published and unpublished documents (a total of 127) cover an unbelievably wide spectrum of areas. Many of them have been a priceless source of research ideas for others. One could say that there would be no internet without Shannon's theory of information; every modem, every compressed file, every error correcting code owes something to Shannon. Shannon died at age 84 on February 27, 2001 in Medford, Mass., after a long fight with Alzheimer's disease.

## ***EXERCISES***

**Exercise 1.** *What do these figures refer to?*

1930s, 1940, 2001, 1941, late 1940, 1956, 1950, 1916, 1938.

**Exercise 2.** *Agree/disagree with the following statements:*

- a) Claude Shannon showed a keen interest in sciences from an early childhood.
- b) In the 1930's Massachusetts Institute of Technology was one of the most prestigious scientific and research institutions conducting the work in information theories.
- c) The Differential Analyzer was the first electronic computer.
- d) Shannon graduated from MIT with the Master's degree.
- e) Shannon's concept of entropy was applied to probability theory.
- f) Shannon was the first who introduced the word "bit" to describe the "yes-no" decision.
- g) Shannon stopped his scientific activity in the early 1950's.
- h) Nowadays we have an opportunity to use the Internet due to Shannon's theory of information.
- i) Claude Shannon is one of the most outstanding scientists of the 20th century.

**Exercise 3.** *Answer the following questions.*

- 1. What was Shannon's family background?
- 2. Who had a strong scientific influence on young Shannon?
- 3. What fields of science was he interested in?
- 4. Where did he receive his higher education?
- 5. What was Shannon's early work devoted to?
- 6. What job was he involved in working at the Bell Telephone Laboratories?
- 7. What was his most significant scientific achievement?
- 8. What kind of mechanism did he try to develop in the 1950's together with Alan Turing?
- 9. What other sciences was his information theory applied to?
- 10. What is the title of his most famous paper?

**Exercise 4.** *Sum up the content of the text using the following key points:*

1. Family background.
2. Education (degrees).
3. Areas of scientific and research activity.
4. Major achievements.

**Exercise 5.** *Comment on the statements:*

1. Claude Shannon is considered to be “the father of information theory”.
2. Shannon’s scientific and research contribution to the world science is enormous.
3. There would be no internet without Shannon's theory of information.

**Exercise 6.** *Briefly retell the text.*

## **TEXT 2**

## **Google**

Google is an American multinational corporation specializing in Internet-related services and products, which include search, cloud computing, software, and online advertising technologies. Google began in January 1996 as a research project by Larry Page and Sergey Brin when they were both PhD students at Stanford University in Stanford, California.

While conventional search engines ranked results by counting how many times the search terms appeared on the page, Page and Brin theorized about a better system that analyzed the relationships between websites. They called this new technology PageRank. PageRank determined a website’s relevance by the number of pages, and the importance of those pages, that linked back to the original site. Page and Brin originally nicknamed their new search engine “BackRub”, because the system checked backlinks to estimate the importance of a site. Eventually, they changed the name to Google, originating from a misspelling of the word “googol”, the number one followed by one hundred zeroes, which was picked to signify that the search engine was intended to provide large quantities of information.

The domain name for Google was registered on September 15, 1997, and the company was incorporated on September 4, 1998. It was based in a

garage of Susan Wojcicki, the friend of Page and Brin. In March 1999, the company moved its offices to Palo Alto, California, which is home to several prominent Silicon Valley technology startups.

In 2003, after outgrowing two other locations, the company leased an office complex from Silicon Graphics at 1600 Amphitheatre Parkway in Mountain View, California. The complex became known as the Googleplex. Three years later, Google bought the property from SGI for \$319 million. By that time, the name “Google” had found its way into everyday language, causing the verb “google” to be added to the Merriam-Webster Collegiate Dictionary and the Oxford English Dictionary, denoted as “to use the Google search engine - to obtain information on the Internet”. Since then, Google has grown and expanded. It bought and absorbed many firms, turning their developments into new services and projects.

Google produces a lot of products and services, such as Web-based products, Operating systems, Desktop and Mobile applications, and Hardware products. Web-based products can be divided into Search tools (Google Search, which is Google’s core product, Google News, Google Video, etc.), Advertising services (Google AdSense, Google AdWords, etc.), Communication and Publishing tools (YouTube, Gmail, Google Docs, etc.), Development tools (Google App Engine, Google Web Toolkit, etc.), Map-related products (Google Maps, Google Sky, Google Mars, etc.), and Statistical tools (Google Analytics, Google Consumer Surveys, etc.)

Google’s Operating Systems are Android (for mobile devices), Chrome OS (runs on the Chrome book and Chrome box), and Google TV (a smart TV platform). Examples of Desktop and Mobile applications are Google Chrome (web browser), Google Earth ( virtual 3D globe that uses satellite imagery, aerial photography, GIS from Google’s repository), Google Keep (it allows you to quickly create, access and organize notes, lists and photos), Google Now (a built in application that acts as your personal assistant through voice commands), etc.

Some of Google’s Hardware products are Nexus smartphones and tablets running the Android OS, Google TV, Chrome book (laptop PC running Chrome OS), Google Glass ( a wearable computer with an optical head-mounted display and camera that allows the wearer to interact with various applications and the Internet via natural language voice commands), and Google driverless car.

By 2014 Google remained one of the most important and powerful corporations, which annually received numerous awards. It's difficult now to imagine our life without products and conveniences donated to us by Google.

## ***EXERCISES***

**Exercise 1.** *What do these figures refer to?*

1996, 1997, 1998, 1999, 2003, 2014, \$319 million.

**Exercise 2.** *Agree/disagree with the following statements.*

1. Google is just one of the five most popular websites in the world.
2. Google was originated by American PhD students.
3. The name Google was given to estimate the importance of a site.
4. The name of the site "Google" and the company of the same name were registered simultaneously.
5. The company "Google" was originally based in Palo Alto, California.
6. The name "Google" had found its way into everyday language by 2010.
7. Google has grown and expanded since 2006.
8. Google Web-site products are divided into 6 groups.
9. Android is the only operating system used by Google.
10. By 2014 Google had become one of the most major world companies specializing in Internet-related services and products.

**Exercise 3.** *Answer the following questions.*

1. What does Google specialize in?
2. How was the company "Google" originated?
3. What was the research of Page and Brin aimed at?
4. What is the main idea of PageRank technology?
5. Why did Page and Brin originally name their new search engine "BackRub"?
6. What does the word "googol" mean?
7. When was the domain name for Google registered?
8. Since when has Google grown and expanded?
9. What products and services does Google produce?
10. What is Google's main product?

**Exercise 4.** *Comment on the statements:*

1. While conventional search engines ranked results by counting how many times the search terms appeared on the page, Page and Brin theorized about a better system that analyzed the relationships between websites.
2. Eventually, they changed the name to Google, originating from a misspelling of the word “googol”, the number one followed by one hundred zeroes, which was picked to signify that the search engine was intended to provide large quantities of information.
3. By that time, the name “Google” had found its way into everyday language, causing the verb “google” to be added to the Merriam-Webster Collegiate Dictionary and the Oxford English Dictionary, denoted as “to use the Google search engine – to obtain information on the Internet”. Since then Google has grown and expanded.

**Exercise 5.** *Make up a plan of the text and sum it up.*

**TEXT 3**

**Steve Jobs**

When you think of the name “Steve Jobs”, you probably think of “Apple”, “Macintosh computers”, “money” and “success”. But, did you know that his life hasn’t always been easy? This is the biography of Steve Jobs.

Steve Job’s mother was a college graduate when she found herself alone and pregnant. Feeling like she had no other choice in the matter, the young woman chose to put her baby up for adoption. Steven Paul Jobs was born in San Francisco, California on February 24, 1955. But, it would be a few months later until he got to go home with his new parents, Clara and Paul Jobs. His biological mother agreed to her son’s adoption, but there was one stipulation: his new parents had to give her their word he would graduate from high school and attend college. The family lived in Mountain View within California’s Silicon Valley. Clara worked as an accountant and Paul was a Coast Guard veteran and machinist. As the Jobs raised their son, father Paul took the time to teach young Steve a variety of things in the family garage. His father also taught him electronics, although his

knowledge was limited. As Steve Jobs was being raised in Silicon Valley – a metropolis of “high tech” – it was relatively easy for him to explore the interest in electronics his father sparked. A neighbour named Larry Lang, who worked as an engineer at the Hewlett-Packard Company taught Steve a great deal about the subject.

Steve Jobs has always been an intelligent and innovative thinker. It could sound strange but during his first years at school Steve had a tough time. It was until a teacher named Mrs.Hill realized Steve had an exceptional mind when he was in the fourth grade. Job’s tests were so well that administrators wanted to skip him ahead to high school – a proposal his parents declined. After Steve Jobs had graduated from high school, he enrolled at Reed College. He still had no clue what he wanted to do with his life, so he quit attending his scheduled classes six months later. Steve continued to hang out at the campus for several months longer, but he took only classes, such as Calligraphy, that he enjoyed and which developed his love of typography.

In 1974, Jobs took a position as a video game designer with Atari. Several months later he left Atari to find spiritual enlightenment in India, traveling about the continent and experimenting with psychedelic drugs. In 1976, when Jobs was just 21, he and Wozniak started Apple Computers. The duo started in the Jobs garage, and funded their entrepreneurial venture after Jobs sold his Volkswagen bus and Wozniak sold his beloved scientific calculator.

Jobs and Wozniak are credited with revolutionizing the computer industry by democratizing the technology and making the machines smaller, cheaper, intuitive, and accessible to everyday consumers. The two conceived a series of user-friendly personal computers that they initially marketed for \$666.66 each. Their first model, the Apple I, earned them \$774,000. Three years after the release of their second model, the Apple II, sales increased 700 percent to \$139 million dollars. In 1980, Apple Computer became a publically traded company with a market value of \$1.2billion on the very first day of trading. Jobs appointed the marketing expert John Scully of Pepsi-Cola to play the role of Apple’s President.

However, the next several products from Apple suffered significant design flaws resulting in recalls and consumer disappointment. IBM suddenly surpassed Apple sales, and Apple had to compete with an IBM/PC dominated business world. In 1984 Apple released the Macintosh, market-

ing the computer as a piece of a counter culture lifestyle: romantic, youthful, creative. But despite positive sales and performance superior to IBM's PCs, the Macintosh was still not IBM compatible. Scully believed Jobs was hurting Apple, and executives began to phase him out.

In 1985, Jobs resigned as Apple's CEO to begin a new hardware and software company called NeXT, Inc. The following year Jobs purchased an animation company from George Lucas, which later became Pixar Animation Studios. Believing in Pixar's potential, Jobs initially invested \$50 million of his own money into the company. Pixar Studios went on to produce wildly popular animation films such as *ToyStory*, *Finding Nemo* and *The Incredibles*. Pixar's films have netted \$4 billion. The studio merged with Walt Disney in 2006, making Steve Jobs Disney's largest shareholder.

Despite Pixar's success, NeXT, Inc. floundered in its attempts to sell its specialized operating system to mainstream America. Apple eventually bought the company in 1997 for \$429 million. The same year, Jobs returned to his post as Apple's CEO.

Much like Steve Jobs instigated Apple's success in the 1970s, he is credited with revitalizing the company in the 1990s. With a new management team, altered stock options, and a self-imposed annual salary of \$ 1 a year, Jobs put Apple back on track. His ingenious products such as the iMac, effective branding campaigns, and stylish designs caught the attention of consumers once again.

In 2003, Jobs discovered he had a neuroendocrine tumor, a rare but operable form of pancreatic cancer. Instead of immediately opting for surgery, Jobs chose to alter his diet while weighing Eastern treatment options. For nine months Jobs postponed surgery, making Apple's board of directors nervous. Executives feared that shareholders would pull their stocks if word got out that their CEO was ill. But in the end, Job's confidentiality took precedence over shareholder disclosure. In 2004, he had a successful surgery to remove the pancreatic tumor. Early in 2009, reports circulated about Job's weigh loss, some predicting his health issues had returned, which included a liver transplant. Jobs responded to these concerns by stating he was dealing with a hormone imbalance.

In respect to his personal life, Steve Jobs remained a private man who rarely disclosed information about his family. It is known that in March of 1991 he married Laurene Powell, an MBA student of Stanford business school and there were three children in his family.

Jobs' creation, the Apple company, introduced such revolutionary products as the Macbook Air, iPod, iPhone, all of which have dictated the evolution of modern technology. In 2008, iTunes became the second biggest music retailer in America-second only to Wal-Mart. On October 5, 2011, Apple Inc. announced that co-founder Steve Jobs had died. He was 56 years old at the time of his death.

## ***EXERCISES***

**Exercise 1.** *What events do these dates refer to?*

1955, 1974, 1976, 1980, 1984, 1985, 1991, 1997, 2003, 2004, 2006, 2008, 2011.

**Exercise 2.** *Answer the following questions.*

1. What did you learn from the text about Job's birth and his family life?
2. What did Jobs do after completing a high school (including the time at college and the origin of Apple Company)?
3. Why did Jobs depart from Apple?
4. What was Jobs' occupation after his leaving Apple?
5. What favoured Apple's revitalization in 1990s?
6. What are the recent innovations of Apple?
7. What was the reason for Jobs' early death?

**Exercise 3.** *Comment on the statements:*

1. Jobs and Wozniak are credited with revolutionizing the computer industry by democratizing the technology and making the machines smaller, cheaper, intuitive, and accessible to everyday consumers.
2. The next several products from Apple suffered significant design flaws resulting in recalls and consumer disappointment.
3. Scully believed Jobs was hurting Apple, and executives began to phase him out.
4. With a new management team, altered stock options, and a self-imposed annual salary of \$1 a year, Jobs put Apple back on track.

**Exercise 4.** *Make up the summary of the text and reproduce it orally.*

## **TEXT 4**

### **The history of information security**

The history of information security begins with the history of computer security. The need for computer security – that is, the need to secure physical locations, hardware, and software from outside threats – arose during World War II when the first mainframes, developed to aid computations for communication code breaking were put to use. Multiple levels of security were implemented to protect these mainframes and secure data integrity. Access to sensitive military locations, for example, was controlled through the use of badges, keys, and the facial recognition of authorized personnel by security guards. The growing need to maintain national security eventually led to more complex and more technologically sophisticated computer security safeguards.

During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage. One of the first documented security problems that was not physical in nature occurred in the early 1960s, when a systems administrator was working on a MOTD (message of the day) file, and another administrator was editing the password file. A software glitch mixed the two files, and the entire password file was printed on every output file.

In the 1960s during the Cold War, many more mainframes were brought online to accomplish more complex and sophisticated tasks. It became necessary to find a way to enable these mainframes to communicate with each by means of a less cumbersome process than mailing magnetic tapes between computer centers. In response to this need, the Department of Defense's Advanced Research Project Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the military's exchange of information. Larry Roberts, known as the founder of the Internet, developed the project from its inception. This project, called ARPANET, is the origin of today's Internet.

During the next decade, the ARPANET became popular and more widely used, and the potential for its misuse grew. In December of 1973, Robert M. "Bob" Metcalfe, who is credited with the development of the Ethernet, one of the most popular networking protocols, identified fundamental problems with ARPANET security. Individual remote users' sites

did not have sufficient controls and safeguards to protect data from unauthorized remote users. Other problems abounded: the vulnerability of password structure and formats; lack of safety procedures for dial-up connections; nonexistent user identification and authorization to the system. Phone numbers were widely distributed and openly publicized on the walls of phone booths, giving hackers easy access to the ARPANET. Because of the range and frequency of computer security violations and the explosion in the numbers of hosts and users on the ARPANET, network security was referred to as network insecurity. In 1978, a famous study entitled “Protection Analysis: Final Report” was published. It focused on a project undertaken by ARPA to discover the vulnerabilities of operating system security. For a timeline that includes this and other seminal studies of computer security.

The movement toward security that went beyond protecting physical locations began with a single paper sponsored by the Department of Defense, the Rand Report R-609, which attempted to define the multiple controls and mechanisms necessary for the protection of a multilevel computer system. The document was classified for almost ten years, and is now referred to as the paper that started the study of computer security.

The security – or lack thereof – of the systems sharing resources inside the Department of Defense was brought to the attention of researchers in the spring and summer of 1967. At that time, systems were being acquired at a rapid rate and the problem of securing them was a pressing concern for both the military and defense contractors. In June of 1967, the Advanced Research Projects Agency formed a task force to study the process of securing classified information systems. The Task Force was assembled in October of 1967 and met regularly to formulate recommendations, which ultimately became the contents of the Rand Report R-609. The Rand Report R-609 was the first widely recognized published document to identify the role of management and policy issues in computer security. It noted that the wide utilization of networking components in information systems in the military introduced security risks that could not be mitigated by the routine practices then used to secure these systems. This paper signaled a pivotal moment in computer security history – when the scope of computer security expanded significantly from the safety of physical locations and hardware to include the following:

- Securing the data,

- Limiting random and unauthorized access to that data,
- Involving personnel from multiple levels of the organization in matters pertaining to information security.

## ***EXERCISES***

**Exercise 1.** *What do these figures refer to?*

1960s, 1973, 1978, 1967, 609.

**Exercise 2.** *Agree/disagree with the following statements.*

1. The need for computer security arose during World War II when the first mainframes, developed to aid computations for communication code breaking were put into use.
2. One of the first documented security problems occurred when a software glitch mixed two files, and the entire password file was printed on every output file.
3. Bob Metcalfe created the project called ARPANET, the origin of today's Internet.
4. The paper sponsored by the Department of Defense, the Rand Report R-609 started the history of computer science and was the first to identify the role of management and policy issue in computer security.
5. Pivotal moments in computer security include securing data, limiting authorized access to that data and involve all personnel of an organization in matters of information security.

**Exercise 3.** *Answer the following questions.*

1. When did the history of Information Security begin? What were its aims?
2. What was one of the first documented security problem?
3. What were the origins of APRANET?
4. What were the fundamental problems with ARPANET security?
5. What did "Protection Analysis: Final Report" focus on?
6. What is Rand Report R-609? And how did it influence modern computer security?
7. What are the main issues that should be concerned in Information Security?

**Exercise 4.** *Comment on the statements:*

1. During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes.
2. During the Cold War it became necessary to find a way to enable mainframes to communicate with each other by means of a less cumbersome process than mailing magnetic tapes between computer centers.
3. In December of 1973, Robert M. “Bob” Metcalfe, who is credited with the development of the Ethernet, one of the most popular networking protocols, identified fundamental problems with ARPANET security.
4. The movement toward security that went beyond protecting physical locations began with a single paper, the Rand Report R-609.
5. This paper signaled a pivotal moment in computer security history – when the scope of computer security expanded significantly from the safety of physical locations and hardware.

**Exercise 5.** *Sum up the text highlighting the most significant events in the development of Information security.*

**TEXT 5      A brief look at the history of computer viruses**

Computer viruses are relatively new and started to emerge and upgrade soon after the Internet appeared. The history of computer viruses shows us that the founding blocks of computer viruses were laid in 1949, when scientist John von Neumann came up with the theory about self-replicating programs. In 1969, AT&T Bell Laboratories came up with the first multi-tasking operating system, UNIX, and, in the same year, ARPANET is developed by the Advanced Research Projects Agency. This was the precursor of the Internet. Let us look back in time at the interesting history of computer viruses.

In 1979, engineers at Xerox Palo Alto Research Center make a huge discovery: the computer worm. This rudimentary program is the ancestor of modern computer worms and is designed to search for idle processors in a network. In 1983, Fred Cohen of the University of Southern California

comes up with the term “computer virus” to describe a program that is created to "affect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself."

In 1986, the first PC virus, codename “The Brain” is released from Pakistan. In 1988 came the first devastating attack against ARPANET computers. Robert Morris, 23, created a small virus that infected almost 6,000 computers on the network and flooded them with copies of itself. In 1991, Symantec develops the Norton Anti-Virus software as a way of protecting computers from viruses.

In 1998, more than 500 military and government computer systems are hijacked. Although it was first believed that the masterminds were based in Iraq, investigators soon found out that two California teenagers were behind the incident. This hijack demonstrated what a coordinated attack could do, especially combined with a physical attack.

In 1999 came the “Melissa” virus. It managed to infect thousands of computers at an alarming speed, causing over \$80 million in damages. Antivirus software hit record sales. Melissa works by sending infected Word documents to the first 50 people in your Outlook list.

In 2000, the “I Love You” virus appears. It managed to infect millions of computers in just under a day. The virus sent usernames and passwords it found on the infected computer back to the author. In 2001, the “Anna Kournikova” frightens experts who believe that this virus was written using a toolkit. A toolkit would allow even inexperienced programmers to create computer viruses.

In 2001, the Code Red virus posed a serious threat to the White House website. It infected tens of thousands of computers, causing damages in excess of \$2 billion. It was programmed to unleash the power of all the infected computers against the White House website at a predetermined time. It was stopped before it could act. The same year, the Nimda virus hits the Internet. In the brief history of computer viruses this is one of the most sophisticated viruses ever to appear.

In 2003, the Slammer computer virus infects hundreds of thousands of computers in under three hours. This virus even delayed airline flights worldwide and in computer virus history this was the fastest spreading virus ever. Then in 2004, the MyDoom virus, an email virus, claims the top place as the fastest spreading email virus. However, this computer virus did very little damage.

This is the history of computer viruses up to 2004. After 2004, no more notable viruses appeared due to sophisticated antivirus and firewall systems.

## ***EXERCISES***

**Exercise 1.** *What do these figures refer to?*

1949, 1979, 1991, 23, 500, 50, 2 billion, 2004.

**Exercise 2.** *Agree/disagree with the following statements.*

1. Computer viruses appeared at the same time with the Internet.
2. The basis for creating any virus is a self-replicating program.
3. Computer virus can be described as a program created to delete any information on a computer.
4. Norton Anti-Virus software was developed after the appearance of the first computer virus.
5. The masterminds of a virus that hit over 500 million military and government computer systems in 1998 were 2 Californian teenagers.
6. “I love you” virus was written using a toolkit.
7. The Code Red virus caused the delay of airline flights.

**Exercise 3.** *Answer the following questions.*

1. When and how did the history of computer viruses begin?
2. What was a huge discovery made by engineers at Xerox Palo Alto Research Centre?
3. When did the term “a computer virus” appear?
4. What was this term used for?
5. Who created a virus that hit more than 500 military and government computer systems in 1998?
6. What was the mechanism of “Melissa” virus?
7. Why was “Anna Kournikova” virus so frightening?
8. What virus posed the most serious threat to the White House websites?
9. What was the fastest spreading e-mail virus?
10. Why haven’t any notable viruses appeared since 2004?

**Exercise 4.** *Comment on the statements:*

1. The history of computer viruses show us that the founding blocks of computer viruses were laid in 1949, when scientist John von Neumann came up with the theory about self-replicating programs.
2. The Red Code Virus was programmed to unleash the power of all the infected computers against the White House website at a predetermined time. It was stopped before it could act.
3. After 2004, no more notable viruses appeared due to sophisticated antivirus and firewall systems.

**Exercise 5.** *Make up a plan of the text and sum it up.*

**TEXT 6**                      **This is the story of Eugene Kaspersky**

“I was born many, many years ago in 1965”, Eugene laughs. His laugh is infectious, and it’s clear that he does not use it sparingly. Schooled in the Moscow region, Eugene’s talent for mathematics became glaringly obvious very quickly. “My mum recognized that I was interested in mathematics at a very young age, and I’d read special mathematics books and magazines”.

By the age of 12, Eugene Kaspersky was studying advanced mathematics at an evening school for children. Entering what they considered ‘The Olympic Games for kids mathematics’, Eugene took home second prize in his town. Attending a mathematical boarding school in Moscow in his teens, Eugene took a particular interest in the school’s computer. “Well, I suppose it was just a digital machine”, he smiles. He spent his last two years of secondary school taking physics and mathematics courses in a specialized programme for gifted students organised by and affiliated with Moscow State University.

Despite his obvious intelligence, Eugene remains modest about his potential. “I wasn’t clever enough to become a cryptologist. Cryptology is such a science that very few are able to do it successfully without losing their minds”. So, how did Eugene’s talent as a mathematician lead to him founding an incredibly successful information security company? “If you’re a mathematician you can easily be a computer engineer”, Eugene explains, “but if you’re computer engineer, you’ll never be a mathemati-

cian. I did it the right way around – it was very good training for my brain”.

In 1987, Eugene graduated from the Institute of Cryptography, Telecommunications and Computer Science, where he studied mathematics, cryptography and computer technology, majoring in mathematical engineering.

After graduating, Eugene worked at a multi-disciplinary research institute. It was there that Eugene first began studying computer viruses after detecting the Cascade virus on his computer in October 1989. Eugene analyzed the virus and developed a disinfection utility for it – the first such utility he developed.

In the early 1990s, Eugene embarked on the AVP anti-virus project. “The name of the first version of my software was called minus V, [written –V]. The reason for this? I wanted it to appear first in product lists”, laughs the Kaspersky CEO.

The story about the naming of the project gets better, Eugene explains. “We called the innovative anti-virus software the anti-viral toolkit pro – ATP. When a friend of mine from Bulgaria asked me to send the software for tests, I made the mistake of calling the product AVP when packing the file. Later, this man sent me a message saying that the AVP package is becoming popular because it’s good software. I told him that it was a mistake and that its actual name is ATP and he said “too late – it’s known as AV”.”

“By 1992 I had recruited more people to help with the software development, and we had a very innovative anti-virus for that time.” Two years later, tests in Hamburg University declared Eugene Kaspersky’s AVP product ‘best in list’.

The product grew through international distribution, and received much interest from German companies. “There was no money, but we were happy that our product was being promoted. At that point, we were probably a team of four or five, with no resources to control our distribution, finance or sales results”.

Eugene Kaspersky learnt the hard way about the dog-eat-dog world of business. An American man registered AVP as a trademark under his own name, and started to behave as a software vendor. “He owned the trademark, so he owned the software”, Kaspersky says regretfully. “In 1999 we started negotiation to take back the trademark and website, but

unfortunately, there were no results. So we had to change everything, and started again”.

Eugene Kaspersky registered ‘Kaspersky’ as a global trademark, designed the new logo, and “the new everything. I like to say I’m working on my second million dollars, because I gave up the first one”, he laughs.

“At the time, the software market was very small, and we had almost zero sales, but we used every opportunity for income. I recognised that it was possible to earn money from anti-virus software when I first saw companies starting to suffer from virus.”

Virus research was always a passion of Eugene Kaspersky, who admits that “I was working not for money, but for fun”.

Survival was assured by signed technology contracts. “The Russian anti-virus market was not big enough to survive. In the industry we were known to have one of the best engines. We had a lot of innovations and the quality of detections was respected”.

The Russian financial crisis in 1998 taught Eugene to depend on different currencies. “We used the crisis to improve the company – we started to recruit more people because it was cheap.

Successful Russian information security companies are few and far between. Is it therefore more of a challenge to set up an information security company in Russia? “Yes and no”, answers Eugene. “Yes because the Silicon Valley is a better environment with a lot of investors. No because there is a very good pool of talented engineers in Russia”.

In fact, most of Kaspersky’s engineers are based in Russia. “When it comes to marketing and sales, however, it is harder to find the right people here in Russia, because technical education has a stronger history in Russia. In soviet times there was no marketing or business education, which is why we are the first generation. Even today, education is focussed on technology”.

Unlike many entrepreneurs, Eugene confirms that he never had an exit plan. “I was interested in researching viruses and researching malicious codes. It was my hobby, and when you have a hobby, it is not up for sale”. Interestingly, Eugene was asked many times over the years to join other companies or sell his company, but now the tables have turned. “There was one company that once wanted to acquire us. Now they have asked us to acquire them”, he says with a sense of pride.

Eugene, however, is intent on keeping the Kaspersky corporate culture, which seems to be respected so much by his employees. “That’s why we are so conservative with acquisitions. We want to keep the special spirit of the team of the company, and acquisitions are the wrong way to do this”.

In hindsight, Eugene Kaspersky looks fondly upon his journey to where he is now. And so he should.

My time with Eugene is up, but not before I get to ask him one last question. The biggest mistake of his career? “A technical mistake”, he says without hesitation. “The AV engine in 1996 wasn’t able to process two files at the same time. This was the most serious, critical mistake of my career. We had to develop special envelopes for the engine to run in a multi-threat landscape. If I could live my life again, that is the one thing I would change, but not the rest.” And why should he?

## ***EXERCISES***

**Exercise 1.** *What do these figures refer to?*

1998, 12, 1 million, 1992, 1996, 1999, 4 or 5.

**Exercise 2.** *Agree/disagree with the following statements.*

1. Kaspersky has been interested in mathematics since his childhood.
2. He took the second prize in the “Olympic Games for kids mathematics” at the age of 12.
3. He was taking computing course during his last 2 years of secondary school.
4. He considers Cryptology to be a science that everyone is able to do successfully.
5. He believes that a mathematician can easily be a computer engineer.
6. He began studying computer viruses after detecting one of them in his computer.
7. His first anti-virus project appeared in 1990.
8. His first anti-virus software package was named “AV”.
9. His AVP product was declared “best in list” in 1992 in Germany.
10. He had to register “Kaspersky” trademark as AVP was not successful.

11. Virus search has always been a passion of Eugene Kaspersky.
12. He thinks that today education is focused on technology.
13. The biggest mistake in his career was to start business in Russia.

**Exercise 3.** *Answer the following questions.*

1. Where did he study mathematics?
2. What can you say about his character?
3. How does he explain his choice of occupation?
4. When and why did he begin studying computer viruses?
5. Why was his first produce named AV?
6. Were his first attempts in doing business successful?
7. How did the Russian financial crisis in 1998 influence Kaspersky's company?
8. What has he always been interested in?
9. What was the biggest mistake in his career?

**Exercise 4.** *Arrange the following headings in the logical order and match them with the paragraphs of the text.*

- 1) The Russian market;
- 2) The first product;
- 3) No regrets;
- 4) Stabbed in the back;
- 5) First steps in mathematics.

**Exercise 5.** *Make up a plan of the text and sum it up.*

### **TEXT 7      Information security: is it an art or a science?**

Given the level of complexity in today's information systems, the implementation of information security has often been described as a combination of art and science. System technologists, especially those with a gift for managing and operating computers and computer-based systems, have long been suspected of using more than a little magic to keep the systems running and functioning as expected. In information security such technologists are sometimes called *security artisans*. Everyone who has studied computer systems can appreciate the anxiety most people feel

when faced with complex technology. Consider the inner workings of the computer: with the mind-boggling functions of the transistors in a CPU, the interaction of the various digital devices, and the memory storage units on the circuit boards, it's a miracle these things work at all.

### *Security as art*

The security administrators and technicians who implement security can be compared with a painter applying oils to canvas. A touch of color here, a brush stroke there, just enough to represent the image the artist wants to convey without overwhelming the viewer, or in security terms, without overly restricting user access. There are no hard and fast rules regulating the installation of various security mechanisms, nor are there many universally accepted complete solutions. While there are many manuals to support individual systems, there is no manual for implementing security throughout an entire interconnected system. This is especially true given the complex levels of interaction between users, policy, and technology controls.

### *Security as science*

Technology developed by computer scientists and engineers – technology designed to perform at rigorous levels of performance – makes information security a science as well as an art. Most scientists agree that specific conditions cause virtually all actions in computer systems. Almost every fault, security hole, and systems malfunction is a result of the interaction of specific hardware and software. If the developers had sufficient time, they could resolve and eliminate these faults.

The faults that remain are usually the result of technology malfunctioning for any one of a thousand possible reasons. There are many sources of recognized and approved security methods and techniques that provide sound technical security advice. Best practices, standards of due care, and other tried-and-true methods can minimize the level of guesswork necessary to secure an organization's information and systems.

### *Security as a social science*

A third view to consider when examining information security is security as social science, which integrates some of the components of art and science, and adds another dimension to the discussion. Social science examines the behavior of individuals as they interact with systems, whether these are societal systems or, as in this context, information systems.

Information security begins and ends with the people inside the organization and the people that interact with the system, intentionally or otherwise. End users who need the very information the security personnel are trying to protect may be the weakest link in the security chain. By understanding some of the behavioral aspects of organizational science and change management, security administrators can greatly reduce the levels of risk caused by end users, and create more acceptable and supportable security profiles. These measures, coupled with appropriate policy and training issues, can substantially improve the performance of end users and result in a more secure information system.

## ***EXERCISES***

**Exercise 1.** *a) Give at least 2 arguments supporting the ideas of Information security as:*

- an art;
- a science.

*b) Why is Information Security considered to be a social science?*

*d) What is your own opinion?*

*c) What can contribute much to creating secure information system?*

**Exercise 2.** *Agree/disagree with the following statements.*

1. Implementation of information security can be described as a combination of art and science.
2. There are strict rules regulating the installation of various security mechanisms and many universally accepted complete solutions.
3. Almost every fault, security hole, and system malfunction is a result of the interaction of specific hardware and software.
4. Information security deals with the people inside organization and the people who interact with the system.
5. Only by understanding software and hardware security administrators can reduce the levels of risks.

**Exercise 4.** *Comment on the statements:*

1. Given the level of complexity in today's information systems, the implementation of information security has often been described as a combination of art and science.

2. There are no hard and fast rules regulating the installation of various security mechanisms, nor are there many universally accepted complete solutions.
3. There are many sources of recognized and approved security methods and techniques that provide sound technical security advice.
4. By understanding some of the behavioral aspects of organizational science and change management, security administrators can greatly reduce the levels of risk caused by end users, and create more acceptable and supportable security profiles.

**Exercise 5.** *Make up a plan of the text and sum it up.*

## ЗАКЛЮЧЕНИЕ

В учебном пособии был представлен материал профессиональной направленности, позволяющий развить навыки чтения и анализа научно-технической литературы и реферирования английских текстов, с этой целью использовались различные задания, направленные на проверку понимания прочитанного материала.

В пособии приводятся аутентичные, неадаптированные тексты для изучения и самостоятельной работы студентов, которые сопровождаются отдельно вынесенной специализированной лексикой. Материал изложен в доступной форме и расширяет словарный запас за счет овладения современной терминологией.

Авторы надеются, что при изучении пособия студенты смогут активизировать знания, умения и навыки, полученные на более ранних этапах изучения английского языка, и усовершенствовать навыки, направленные на понимание и анализ прочитанного текста, а также навыки реферирования и аннотирования текстов.

Авторы выражают надежду, что издание будет полезно студентам, изучающим английский язык в сфере профессиональной коммуникации.

## WORKS SITED\*

1. Mary Branscombe, Dan Grabham. Major Update to Windows 8. – URL: <http://www.techradar.com/reviews/pc-mac/software/2014> (дата обращения: 25.04.2014).
2. Michael Miller. Switching to Window 8: A quick Guide for Current Windows Users. – URL: <http://www.informit.com/articles/2012> (дата обращения: 26.04.2014).
3. Jeremy Reimer. A History of the GUI. – URL: <http://arstechnica.com/features/2013> (дата обращения: 28.04.2014).
4. GUI Gallery. – URL: <http://toastytech.com/guis/index.html> (дата обращения: 17.04.2014).
5. Gary Marchall. The iOS 7.1 update addresses. – URL: <http://www.techradar.com/reviews/pc-mac/ios-7> (дата обращения: 17.04.2014).
6. Matthew Baxter-Rynolds. iOS, Android, Windows Phone, Windows 8. – URL: <http://www.theguardian.com/technology/2011> (дата обращения: 19.04.2014).
7. Charles Arthur. Battle of the Smartphones // The Guardian. – 24 January. – 2012.
8. Alexander Moschina Apple vs. Google: Who Will Win the Battle of the Smartphones? – URL: <http://www.investmentu.com/article/detail/2010> (дата обращения: 19.04.2014).
9. Information security glossary of terms // The consultative Committee for Space Data Systems. – 2012. – November.
10. Information Security Glossary / University of Birmingham.
11. Dictionary of Information Security by Rob Slade, 2006.
12. Peter Norton “Introduction to computers”. – McGraw-Hill Publishing company, 2006.
13. Peter Salus “Net security: Then and Now (1969 – 1998)”.
14. [www.nluug.nl](http://www.nluug.nl)
15. [www.ischool.utexas.edu](http://www.ischool.utexas.edu)
16. Mike Gentile, Ron Collete. The CISO Handbook “A practical guide to securing your company”. – Auerbach, CRC Press. – 2005. – Aug. 24.
17. <http://www.computervirusremovalguide.com/>
18. <http://www.infosecurity-magazine.com>

---

\*Список источников приводится в авторской редакции.

## ОГЛАВЛЕНИЕ

<b>Предисловие</b> .....	3
--------------------------	---

### PART I

#### *Chapter I. THE LATEST DEVELOPMENTS IN COMPUTER SCIENCE*

<i>Unit 1. Graphical user interface (part one)</i> .....	4
<i>Unit 2. Graphical user interface (part two)</i> .....	10
<i>Unit 3. Smartphones and mobile operating systems</i> .....	17
<i>Unit 4. Cloud computing</i> .....	26
<i>Unit 5. What is “hybrid” cloud computing?</i> .....	31
<i>Unit 6. Search engine</i> .....	39

#### *Chapter II. INFORMATION TECHNOLOGY SECURITY*

<i>Unit 7. What is information technology security?</i> .....	45
<i>Unit 8. Data classification</i> .....	51
<i>Unit 9. How does a computer virus work?</i> .....	57
<i>Unit 10. How does antivirus software work?</i> .....	62
<i>Unit 11. Types of computer crimes and their impact</i> .....	68

### PART II

<i>Text 1. Father of information theory</i> .....	76
<i>Text 2. Google</i> .....	80
<i>Text 3. Steve Jobs</i> .....	83
<i>Text 4. The history of information security</i> .....	87
<i>Text 5. A brief look at the history of computer viruses</i> .....	90
<i>Text 6. This is the story of Eugene Kaspersky</i> .....	93
<i>Text 7. Information security: is it an art or a science?</i> .....	97

<b>Заключение</b> .....	101
-------------------------	-----

<b>Works sited</b> .....	102
--------------------------	-----

*Учебное издание*

КОЙКОВА Татьяна Ивановна  
БОРИСОВА Алёна Юрьевна

ENGLISH FOR IT

АНГЛИЙСКИЙ ДЛЯ СТУДЕНТОВ, ИЗУЧАЮЩИХ  
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

*Учебное пособие*

Редактор С. Ш. Абдуллаева  
Технический редактор Н. В. Тупицына  
Корректор иностранного языка О. В. Попкова  
Корректор В. С. Теверовский  
Компьютерная верстка Е. А. Кузьминой

Подписано в печать 21.10.15.  
Формат 60x84/16. Усл. печ. л. 6,05. Тираж 180 экз.

Заказ

Издательство

Владимирского государственного университета  
имени Александра Григорьевича и Николая Григорьевича Столетовых.  
600000, Владимир, ул. Горького, 87.