Министерство сельского хозяйства РФ

ФГОУ ВПО «Брянская государственная
сельскохозяйственная академия»

Кафедра иностранных языков

Катунина Л.В.

Internet.
Information Protection.

Учебно-методическое пособие
для студентов 2-го курса экономического факультета
(специальность «Прикладная информатика
в экономике»)

Брянск 2009

УДК 811:002:330 (075)
ББК 81.2:73:65
К 29

Катунина Л.В. Internet. Information protection. Учебно-методическое пособие для студентов 2-го курса экономического факультета. Брянск. Издательство Брянской ГСХА. 2009- 44 с.

Предназначено для студентов 2 – го курса экономического факультета обучающихся по специальности «Прикладная информатика в экономике». Имеет своей целью развить у студентов навыки чтения и перевода оригинальных текстов по специальности на английском языке. Данное пособие составлено из текстов по темам, представляющих особую актуальность в наше время в сфере IT технологий и рассчитано на 30 аудиторных часов и столько же часов самостоятельной работы.

Рецензенты: старший преподаватель кафедры иностранных языков БГСХА Т.И. Васькина, зав. кафедрой английского языка БГУ им. академика И.Г. Петровского к.п.н., доцент И.В. Барынкина.

Рекомендовано к изданию методической комиссией экономического факультета Брянской государственной сельскохозяйственной академии, протокол №5 от 13 мая 2009 года.

Введение

Пособие “Internet. Information protection.”, предназначенное для студентов 2-го курса экономического факультета обучающихся по специальности «Прикладная информатика в экономике», имеет своей целью развить у студентов навыки чтения и перевода оригинальных текстов по специальности на английском языке. Задачи пособия состоят в ознакомлении студентов со специальной терминологией, предоставлении информации, находящей практическое применение в повседневной работе с компьютером. Данное пособие составлено из текстов по темам, представляющих особую актуальность в наше время в сфере IT технологий и рассчитано на 30 аудиторных часов и столько же часов самостоятельной работы.

Пособие состоит из 7 уроков (Units) и Приложения (Supplement), охватывающие следующие проблемы: Интернет, электронная почта, преступления, связанные с использованием компьютеров, защита информации. Для более эффективного усвоения материала предлагается ряд лексико-грамматических упражнений.

Unit 1.
Internet

The Internet, a global computer network which embraces millions of users all over the world, began in the United States in 1969 as a military experiment. It was designed to survive a nuclear war. Information sent over the Internet takes the shortest path available from one computer to another. Because of this, any two computers on the Internet will be able to stay in touch with each other as long as there is a single route between them. This technology is called packet switching. Owing to this technology, if some computers on the network are knocked out (by a nuclear explosion, for example), information will just route around them. One such packet-switching network which has already survived a war is the Iraqi computer network which was not knocked out during the Gulf War.

Most of the Internet host computers (more than 50 %) are in the United States, while the rest are located in more than 100 other countries. Although the number of host computers can be counted fairly accurately, nobody knows exactly how many people use the Internet, there are millions worldwide, and their number is growing by thousands each month.

The most popular system currently in use is the World-Wide Web (WWW) which began in March 1989. The Web is an Internet-based computer network that allows users on one computer to access information stored on another through the world-wide network. The world-Wide Web is a product of the continuous search for innovative ways of sharing information resources. The WWW project is based on the principle of universal readership: "if information is available, then any person should be able to access it from anywhere in the world." The Web's implementation follows a standard client-server model. In this model, a user relies on a program (the client) to connect to a remote machine (the server), where the data are stored. The architecture of the WWW is the one of clients, such as Netscape, Mosaic, or Lynx, "which know how to present data but not what their origin is, and servers, which know how to extract data", but are

ignorant of how data will be presented to the user.

One of the main features of the WWW documents is their hypertext structure. On a graphic terminal, for instance, a particular reference can be represented by underlined text, or an icon. "The user clicks on it with the mouse, and the referenced document appears." This method makes copying of information unnecessary: data need only to be stored once, and all referenced to it can be linked to the original document. Because of the intuitive nature of hypertext, even inexperienced computer users are able to connect to the network. Further more, the simplicity of the Hyper Text Markup Language, used for creating interactive documents, allows users to contribute to the expanding database of documents on the Web. Also, the nature of the World-Wide Web provided a way to interconnect computers running different operating systems, and display information created in a variety of existing media formats. In short, the possibilities for hypertext in the world-wide environment are endless.

The most popular Internet service is e-mail. Most of the people, who have access to the Internet, use the network only for sending and receiving e-mail messages. However, other popular services are available on the Internet: reading USENET news, using the World-Wide Web, telnet, FTP and Gopher.

In many developing countries the Internet may provide businessmen with a reliable alternative to the expensive and unreliable telecommunications systems of these countries. Commercial users can communicate cheaply over the Internet with the rest of the world. When they send e-mail messages, they only have to pay for phone calls to their local service providers, not for calls across their countries or around the world. But who actually pays for sending e-mail messages over the Internet long distances, around the world? The answer is very simple: users pay their service provider a monthly or hourly fee. Part of this fee goes towards its costs to connect to a larger service provider, and part of the fee received by the larger provider goes to cover its cost of running a worldwide network of wires and wireless stations.

But saving money is only the first step. If people see that they

can make money from the Internet, commercial use of this network will drastically increase. For example, some western architecture companies and garment centers already transmit their basic designs and concepts over the Internet into China, where they are reworked and refined by skilled – but inexpensive – Chinese computer-aided-design specialists.

However, some problems remain. The most important is security. When you send an e-mail message to somebody, this message can travel through many different networks and computers. The data are constantly being directed towards their destination by special computers called routers. However, because of this, it is possible to get into any of the computers along the route, intercept and even change the data being sent over the Internet. In spite of the fact that there are many good encoding programs available, nearly all the information being sent over the Internet is transmitted without any form of encoding, i.e. "in the clear". But when it becomes necessary to send important information over the network, these encoding programs may be useful. Some American Banks and companies even conduct transactions over the Internet. But there are still both commercial and technical problems which will take time to be resolved.

Vocabulary

1. Encoding programs	программы кодирования
3. Owing to	благодаря чему-либо
4. Packet-switching	коммутация пакетов
5. To be knocked out	быть выведенным из действия
6. Implementation	выполнение, осуществление
7. To rely on smb	полагаться на кого-либо
8. To underline	подчеркивать
9. To expand	расширять
10. Fee	плата, вознаграждение
11. Destination	место назначения
12. To intercept	перехватить
13. Transaction	финансовая операция

Vocabulary exercises

1. Read, write down and memorize the following words and word combinations.
2. Give Russian equivalents of the following words and word combinations:
1) for instance; 2) a monthly fee; 3) to increase drastically; 4) garment center; 5) to resolve a problem; 6) military experiment; 7) to survive a nuclear war; 8) to stay in touch with smb; 9) fairly accurately; 10) to share information resources; 11) to follow a standard client-server model; 12) particular reference can be presented; 13) to contribute to the expanding database of documents; 14) to communicate with rest of the world.

3. Give English equivalents of the following words and word combinations:
1) проходить через многие различные сети и компьютеры; 2) перехватывать данные, посылаемые через сеть Интернет; 3) осуществлять финансовые операции; 4) это займет время на решение проблемы; 5) это самый короткий путь от одного компьютера к другому; 6) если некоторые компьютеры выведены из строя; 7) создавать интерактивные документы; 8) многообразие существующих медиа форматов; 9) часть оплаты идет на покрытие расходов по присоединению к провайдеру.

4. True or false ?
1. The Internet, a global computer network began in 1969 as an industrial experiment.
2. Owing to the Internet two computers are able to stay in touch with each other.
3. The user clicks on an icon to retrieve the referenced document.
4. The use of Hyper Text Markup Language allows users to contribute to the expanding database documents.
5. Encoding programs may be useful for security.
6. There are no good encoding programs where all the information is transmitted without any form of encoding, i.e. “ in the clear”.

5. Answer the questions:
1. What is the Internet? 2. What technology is called packet switching? 3. Where are most of the Internet host computers located? 4. What does the WEB allow for? 5. What is the main feature of the WWW documents? 6. What is the most popular Internet service? 7. How can one characterize commercial use of the Internet? 8. What is an urgent problem the Internet is facing now?

6. Summarize the main points presented in the text.

Unit 2.
Surfing the Net

What is more impressive than the pyramids, more beautiful than Michelangelo's David and more important to mankind than the wondrous inventions of the Industrial Revolution? To the converted, there can be only one answer: the Internet that undisciplined radical electronic communications network that is shaping our universe. Multimedia, the electronic publishing revolution, is entering every area of our lives –college, work, and home. This new digital technology combines texts, video, sound and graphics to produce interactive language learning, football, music, movies, cookery and anything else you might be interested in.

The industrial age has matured into information age; wherein the means to access, manipulate, and use information has become crucial to success and power. The electronic superhighway provides an entry to libraries, research institutions, databases, art galleries, census bureaus, etc. For those of us interested in intercultural communications Cyberspace is a universal community, with instant access not only to information anywhere, but also to friends old and new around the globe.

The Internet is an amorphous global network of thousands of linked computers that pass information back and forth. While the Internet has no government, no owners, no time, no place, no country, it definitely has a culture, which frequently approaches anarchy; and

it has a language, which is more or less English. People who interact in an Internet environment know how addresses are formed, how to use e-mail, ftp, Usenet News, Telnet and other software tools.

Like all new words, Cyberspace has its own lingo, for example: e-bahn, i-way, online, freenet, web page, freeware, browser, gopher, archie, gateway. There are words to describe people who roam the net: netters, e-surfers, internet surfers, netizens, spiders, geeks…. The Internet has its own prerogatives: for example, the dismissive term lurker for the person who hangs around the net, reading what is there but not contributing anything. The term flaming refers to the public humiliation of another netter as punishment for a real or imagined transgression against net culture.

Information technology is a good vehicle for the argument. Some scientists remind us that voluminous information does not necessarily lead to sound thinking. There are many genuine dangers that computers bring to modern society: efficient invasion of privacy, overreliance on polling in politics, even abdication of control over military decision-making. Data glut obscures basic questions of justice and purpose and may even hinder rather than enhance our productivity. Edutainment software and computer games degrade the literacy of children. On the other hand, only a few use of PCs on network to share information and ideas. In most cases IT is used to speed routine tasks, to automate manual processes rather than to change work patterns and business practices. Most managers use their PCs to edit documents – not a good use of their time when they could be dreaming up creative applications. It is time to evaluate anew the role of science and technology in the affairs of the human species.

So, if you are riding on the information highway, you should take steps to cope with information overload. The gift of boundless information is causing a new kind of stress known alternatively as technostress, information overload or Information Fatigue Syndrome. According to some estimates, our mind is capable of processing and analyzing many gigabytes of data per second – a lot more data than any of today's supercomputers can process and act on in real time.

We feel overloaded by the quantity of information because we are getting it unfiltered. We should filter out the junk and turn data into shapes that make sense to us. Stress in moderation is good: it drives us to achieve, stimulates our creativity and is the force behind social and technological breakthroughs.

The cornerstone of an economy are land, labor, capital and entrepreneurial spirit. That traditional definition is now being challenged. Today you find a fifth key economic element: information dominant. As we evolve from an industrial to an information society, our jobs are changing from physical to mental labor. Just as people moved physically from farms to factories in the Industrial age, so today people are shifting muscle power to brain power in a new, computer-based, globally linked by the Internet society.

Vocabulary

1. Multimedia	мультимедийные средства
2. Means	средства
3. To roam	бродить
4. Lingo	слово
5. Transgression	нарушение
6. Invasion of privacy	вторжение в личную жизнь
7. Abdication of control	отказ от контроля
8. An estimate	оценка, суждение
9. Data glut	чрезмерное количество данных
10. To filter out the junk	отфильтровать ненужную информацию
11. Gateway	шлюз, межсетевой интерфейс
12. To challenge	бросать вызов, оспаривать
13. Eduitment	самообучение

Vocabulary exercises

1. Read, write down and memorize the following words and word combinations.

2. Give Russian equivalents of the following words and word combinations:
1) abdication of control; 2) data glut; 3) to enhance productivity; 4) to shape universe; 5) to exchange information; 6) to speed routine tasks; 7) to automate manual processes; 8) to change work patterns; 9) to transfer large amounts of data; 10) information overload; 11) according to some estimates; 12) to stimulate creativity; to lead to sound thinking.

3. Give English equivalents of the following words and word combinations:
1) виртуальные соединения; 2) войти в каждую сферу нашей жизни; 3) интерактивное обучение иностранным языкам; 4) принимать и отправлять информацию; 5) «бороздить» Интернет; 6) истинная опасность; 7) управлять передачей большого количества данных; 8) оптико-волоконный; 9) скорее помешать, а не повысить производительность; 10) редактировать документы; 11) справиться с информационной перегруженностью; 12) эффективные средства снятия стресса; 13) краеугольный камень.

4. Translate some computer terms:
Simple terms: anchor, wizard, versioning, relink, cipher, containment.
Compounds: clipboard, runtime, turnkey, bitmapping, bandwidth.
Term collocations: frame-based layout, active template library, hypertext markup language, object linking and embedding, remote procedure call, uniform data transfer, active server pages, hypertext transfer protocol, interface definition language.

5. Define the following terms:
Buffer, e-mail, byte, browser, bug, cursor, gateway, drive, router, hypertext, protocol, graphics, modem, freenet, zoom.

6. Answer the questions:
1. How has technology changed in just the last 20 years? 2. What is communications Cyberspace? 3. What is the language of the Internet? 4. What new words from Cyberspace lingo do you know? 5. What is flaming? 6. What are the main dangers that computers bring to modern society? 7. How can technostress be characterized? What is a fifth key economic element?

7. Give a summary of the presented text based on your own plan.

Unit 3.
The Language of E-mail

E-mail is the simplest and most immediate function of the Internet for many people. Run through a list of questions that new e-mail users ask most and some snappy answers to them.

What is electronic mail? Electronic mail, or e-mail as it's normally shortened to, is just a message that is composed, sent and read electronically (hence the name). With regular mail you write out your message (letter, postcard, whatever) and drop it off at the post office. The postal office then delivers the message and the recipient reads it. E-mail operates basically the same-way except that everything happens electronically. You compose your message using e-mail software, send it over the lines than connect the Internet's networks and the recipient uses an e-mail program to read the message.

How does e-mail know how to get where it's going? Everybody who's connected to the Internet is assigned a unique e-mail address. In a way, this address is a lot like the address of your house or apartment because it tells everyone else your exact location on the Net. So anyone who wants to send you an e-mail message just tells the e-mail program the appropriate address and runs the Send command. The Internet takes over from there and makes sure the message arrives safely.

What's this netiquette stuff I keep hearing about? The net is a huge, unwieldy mass with no "powers-that-be" that can dictate con-

tent or standards. This is, for the most part, a good thing because it means there's no censorship and no one can wield authority arbitrarily. To prevent this organized chaos from descending into mere anarchy, however, a set of guidelines has been put together over the years. These guidelines are known collectively as netiquette (network etiquette) and they offer suggestions on the correct way to interact with the Internet's denizens. To give you a taste of netiquette, here are some highlights to consider.

Keep your message brief and to the point and make sure you clear up any spelling slips or grammatical gaffes before shipping it out.

Make sure the Subject lines of your message are detailed enough so that they explain what your message is about.

Don't shout by writing your missives entirely in upper-case letters.

Don't bother other people by sending them test messages. If you must test a program, send a message to yourself.

What's a flame? The vast majority of e-mail correspondence is civil and courteous, but with millions of participants all over the world, it's inevitable that some folk will rub each other the wrong way. When this happens, the combatants may exchange emotionally charged, caustic, often obscene messages called flames. When enough of these messages exchange hands, an out-and out flame war develops. These actually burn themselves out after a while, and then the participants can get back to more interesting things.

`Is e-mail secure ? In a word, no. The Net's open architecture allows programmers to write interesting and useful new Internet services, but it also allows unscrupulous snoops to lurk where they don't belong. In particular, the e-mail system has two problems: it's not that hard for someone else to read your e-mail, and it's fairly easy to forge an e-mail address. If a security is a must for you, then you will want to create an industrial strength password for your home directory, use encryption for your most sensitive messages, and use an anonymous remailer when you want to send something incognito.

Vocabulary

1. To compose a message	составить сообщение
2. To deliver a message	доставить сообщение
3. Recipient	получатель
4. To assign address	предоставлять адрес электр. почты
5. Missive	послание
6. Netiquette	сетевой этикет
7. Censorship	цензура
8. Guidelines	основные направления
9. Flame	сообщение оскорбительного характера
10. To lurk	несанкционированно искать информацию
11. To wield authority	обладать полномочиями
12. To forge	подделать

Vocabulary Exercises

1. Read, write down and memorize the following words and word combinations.
2. Give Russian equivalents of the following words and word combinations:
1) to run through a list of questions; 2) normally shortened; 3) exact location on the Net; 4) postal service; 5) to run the Send command; 6) to make sure missive arrives safely; 7) from descending into mere anarchy; 8) to put forward a set of guidelines; 9) to offer suggestions; 10) to consider highlights; 11) to keep message brief and to the point; 12) the vast majority of e-mail correspondence.

3. Give English equivalents of the following words and word combinations:
1) этикет в Интернете; 2) отправить по почте; 3) исправить ошибки правописания; 4) с эмоциональной окраской;

5) отправить тестовое сообщение; 6) если безопасность является крайней необходимостью; 7) подделывать электронный адрес; 8) «подглядывать» то, что не предназначено для показа; 9) создавать безопасный пароль; 10) выполнить команду «послать»; 11) переписка обычного характера.

4. Study the following:
E-mail messages usually have the following format:
To: (Name and e-mail address of recipient)
From: (Name and e-mail address of sender)
Subject: (Identification of main point of message)
Here is an example of an e-mail address:
smith@cup.ac.uk
Note that symbol @ in e-mail address is read *at* and that the full stops are read as *dot*. Thus the example address would be read as Smith at C-U-P dot A-C dot U-K.
The ac.uk in the example address tells you that the address is based at a university in the United Kingdom.

5. Write an e-mail message to your friend.

6. Answer the questions:
1. What major problems are there with the e-mail? 2. What do you think is the reason for the various bits of netiquette which are mentioned? 3. Is e-mail secure? 4. For which types of writing it is necessary to be brief? 5. Do faxes, electronic mail and papers offer an escape from human interaction?

7. Make up a plan for retelling the text.

8. Give a summary of main ideas outlined in the text.

Unit 4
Text 1. Hackers

The first “hackers” were students at the Massachusetts Institute of Technology (MIT) who belonged to the TMRC (Tech Model Railroad Club). Some of the members really built model trains. But many were more interested in the wires and circuits underneath the track platform. Spending hours at TMRC creating better circuitry was called “ a mere hack”. Those members who were interested in creating innovative, stylistic, and technically clever circuits called themselves (with pride) hackers.

During the spring of 1959, a new course was offered at MIT, a freshman programming class. Soon the hackers of the railroad club were spending days, hours, and nights hacking away at their computer, an IBM 704. Instead of creating a better circuit, their hack became creating faster, more efficient program –with the least number of lines of code. Eventually they formed a group and created the first set of hacker’s rules, called the Hacker’s Ethic. Steven Levy, in his book “Hackers”, presented the rules:

Rule 1: Access to computers – and anything, which might teach you, something about the way the world works – should be unlimited and total.

Rule 2: All information should be free.

Rule 3: Mistrust authority – promote decentralization.

Rule 4: Hackers should be judged by their hacking, not bogus criteria such as degrees, race or position.

Rule 5: You can create art and beauty on a computer.

Rule 6: Computers can change your life for the better.

These rules made programming at MIT’s Artificial Intelligence Laboratory a challenging, all encompassing endeavor. Just for the exhilaration of programming, students in the AL Lab would write a new program to perform even the smallest tasks. The program would be made available to others who would try to perform the same task with fewer instructions. The act of making the computer work more elegantly was, to bona fide hacker, awe-inspiring.

Hackers were given free reign on the computer by two AL Lab professors, "Uncle" John McCarthy and Marvin Minsky, who realized that hacking created new insights. Over the years, the AL Lab created many innovations: LIFE, a game about survival; LISP, a new kind of programming language; the first computer chess game; The Cave, the first computer adventure; and SPACEWAR, the first video game.

Vocabulary

1. Hacker	«взломщик»
2. Freshman	первокурсник
3. Bogus	поддельный, мнимый
4. Artificial intelligence	искусственный интеллект
5. Endeavor	попытка
6. Bona fide	честный
7. Insight	понимание, взгляд
8. To give free reign	зд. дать свободу действий
9. Mistrust	недоверие

Text 2. Hackers of Today

Hackers, having started as toy railroad circuitry designers in the late fifties, are completely new people now. Once turned to computers, they became gods and devils. Nowadays holders and users of the World Wide Web hide their PCs under passwords when the keyword "hacker" is heard. When and how did this change take place? Why are we so frightened of Hacker The Mighty and The Elusive?

One of the legends says that hackers have changed under the influence of "crackers" – the people who loved to talk on the phone at somebody else's expense. Those people hooked up to any number and enjoyed the pleasure of telephone conversation, leaving the most fun – bills –for the victim. Another legend tells us that modern hackers were born when a new computer game concept was invented. Rules were very simple: two computer programs were fighting for

the reign on the computer. Memory, disk-space and CPU time were the battlefield. The results of that game are two in number and are well known: hackers and computer viruses. One more story tells that the "new" hackers came to existence when two MIT students that attended the AL Lab found an error in a network program. They let people, responsible for the network, know but with no result. The offended wrote a code that completely paralyzed the network and only after that the error was fixed. By the way, those students founded The Motorola Company later.

Today, when the Internet has entered everyone's house there's no shield between a hacker and your PC. You can password yourself up, but then either hackers will crack your PC anyway or nobody will enter your site, because passwords kill accessibility. If your PC is easy to access no one can guarantee what'll happen to your computer – hackers, you know them.

Monsters? Chimeras? Not at all! Every hacker is a human being and has soft spots: good food, pretty girls or boys (it happens both ways), classical music, hot chocolate at the fireplace, apple pie on Sunday. Hacker is first of all a connoisseur, a professional with no computer secret out of his experience. And what is the application for skills depends on him, God and Holy Spirit.

Vocabulary

1. To hide	прятать
2. To be frightened	быть напуганным
3. At smb's expense	за чей-либо счет
4. To hook up	подключиться к линии
5. Bill	счет к оплате
6. To found a company	основать компанию
7. Shield	защита
8. To crack PC	«взломать» компьютер
9. Accessibility	доступность
10. Soft spot	уязвимое место
11. Connoisseur	знаток

Vocabulary Exercises

1. Read, write down and memorize the words and word combinations from Text 1 and Text 2.
2. Give Russian equivalents of the following words and word combinations:
1) to be interested in wires and circuits; 2) to create better circuitry; 3) "a mere hack"; 4) to offer a new course; 5) to hack away time at their computers; 6) eventually; 7) mistrust authority; 8) bogus criteria; 9) ethic code; 10) exhilaration of programming; 11) awe-inspiring; 12) once turned to computers; 13) Hacker The Mighty and The Elusive; 14) "cracker"; 15) to fight for the reign on the computer; 16) to be battlefield; 17) to let know the results; 18) to fix an error; 19) out of experience; 20) application of skills.

3. Give English equivalents of the following words and word combinations:
1) с наименьшим количеством строчек в коде; 2) создать свод правил; 3) должно быть неограниченным и всеобъемлющим; 4) способствовать децентрализации; 5) судить по критериям; 6) сделать программу доступной для других; 7) осуществлять подобную задачу заданием меньшего количества команд; 8) измениться под влиянием; 9) компьютерные вирусы; 10) обнаружить ошибку в программе; 11) основать компанию; 12) начать существовать; 13) «взломать» компьютер.

4. True or false?
1. Those who can, do. Those who cannot, teach. Those who cannot teach, HACK.
2. The first hackers were interested in railroad circuitry.
3. The first hackers studied at MIT.
4. The point of a hacker's work was to create a faster and smaller code.
5. Hackers have their own Ethic Code.
6. TMRC stands for Toy Machinery Railroad Car.

7. Hackers sabotaged the work of the AI Lab.
8. An elegant computer was, to a real hacker, awe-inspiring.
9. At AI Lab hackers wrote a computer program for every other task.
10. Hackers were quite prolific in innovations.
11. Hackers were given free reign on the two AI Lab professors.

5. Put the proper words into sentences:
programming, insights, innovations, ethic, instructions, exhilaration, endeavor, awe-inspiring, encompass, freshmen, authority, bogus, mistrust.
1. Decentralization results in …….to the chief.
2. Holding the door for a lady is the question of…….
3. This still life isn't Picasso's, it's a ……
4. The report you've presented doesn't …….. some of the problems.
5. If you can survive both in the jungle and the desert, a ……Indian you are.
6. The…..in how hardware works is obligatory for a good programmer.
7. Each……. is another step to a new technological revolution.
8. In 1961 the Soviet Scientists'……to conquer the space was a success.
9. ……without any reason proves one's carelessness.
10. Iron grip boss expects you to carry out all his……
11. Annually MIT gains over 5000 …….
12. …..should cause ……terror in your heart.

6. Read the following recommendations and try to keep to them .
How to check your own security (the computer is presumed to be in the home).
A personal checklist for hardware.
1. No eating, drinking, or smoking near the computer.
2. Do not place the computer near open windows or doors.
3. Do not subject the computer to extreme temperatures.
4. Clean equipment regularly.
5. Place a cable lock on the computer.

6. Use a surge protector.
7. Store diskettes properly in a locked container.
8. Maintain backup copies of all files.
9. Store copies of critical files off site.
A personal checklist for software.
A word of prevention is in order. Although there are programs that can prevent virus activity, protecting yourself from viruses depends more on common sense than on building a "fortress" around the computer. Here are a few common-sense tips:
1. If your software allows it, follow write-protect measures for a floppy disks before installing any new software. If it does not allow it, write –protect the disks immediately after installation.
2. Do not install software unless you know it is safe. Viruses tend to show up on free software acquired from sales representatives, re-sellers, computer repair people, power users and consultants.
3. Make your applications (and other executable files) read-only. This will not prevent infection, but it can help contain those viruses that attack applications.
4. Stop the so-called sneakernet crowd. This is the group that moves around the office (in sneakers, of course) and prefers to transfer files quickly via floppy disk.
5. Make backups. This is a give motto: Always back up your hard disk and floppies.

7. Answer the questions:
1. Who were the first hackers? 2. What does a set of hacker's rules look like? 3. Does there exist any relationship between crackers and hackers? 4. Is there a proven shield between a hacker and your PC? 5. Is hacker a connoisseur and a professional ?

8. Summarized the main points presented in the above two texts.

Unit 5.
Computer Crimes

More and more, the operations of our businesses, governments, and financial institutions are controlled by information that exists only inside computer memories. Anyone clever enough to modify this information for his own purposes can reap substantial rewards. Even worse, a number of people who have done this and been caught at it have managed to get away without punishment.

These facts have not been lost on criminals or would-be criminals. A recent Stanford Research Institute study of computer abuse was based on 160 case histories, which probably are just the proverbial tip of the iceberg. After all, we only know about the unsuccessful crimes. How many successful ones have gone undetected is anybody's guess.

Here are a few areas in which computer criminals have found the pickings all too easy.

Banking. All but the smallest banks now keep their accounts on computer files. Someone who knows how to change the numbers in the files can transfer funds at will. For instance, one programmer was caught having the computer transfer funds from other people's accounts to his wife's checking account. Often, traditionally trained auditors don't know enough about the workings of computers to catch what is taking place right under their noses.

Business. A company that uses computers extensively offers many opportunities to both dishonest employees and clever outsiders. For instance, a thief can have the computer ship the company's products to addresses of his own choosing. Or he can have it issue checks to him or his confederates for imaginary supplies or services. People have been caught doing both.

Credit cards. There is a trend toward using cards similar to credit cards to gain access to funds through cash-dispensing terminals. Yet in the past, organized crime has used stolen or counterfeit credit cards to finance its operations. Banks that offer after-hours or remote banking through cash-dispensing terminals may find them-

selves unwillingly subsidizing organized crime.

Theft of information. Much personal information about individuals is now stored in computer files. An unauthorized person with access to this information could use it for blackmail. Also, confidential information about a company's products or operations can be stolen and sold to unscrupulous competitors. (One attempt at the latter came to light when the competitor turned out to be scrupulous and turned in the people who were trying to sell him stolen information.)

Software theft. The software for a computer system is often more expensive than hardware. Yet this expensive software is all too easy to copy. Crooked computer experts have devised a variety of tricks for getting these expensive programs printed out, punched on cards, recorded on tape, or otherwise delivered into their hands. This crime has even been perpetrated from remote terminals that access the computer over the telephone.

Theft of Time-Sharing Services. When the public is given access to a system, some members of the public often discover how to use the system in unauthorized ways. For example, there are the "phone freakers" who avoid long distance telephone charges by sending over their phones control signals that are identical to those used by the telephone company.

Since time-sharing systems are often accessible to anyone who dials the right telephone number, they are subject to the same kinds of manipulation.

Of course, most systems use account numbers and passwords to restrict access to authorized users. But unauthorized persons have proved to be adept at obtaining this information and using it for their own benefit. For instance, when a police computer system was demonstrated to a school class, a precocious student noted the access codes being used; later, all the student's teachers turned up on a list of wanted criminals.

Perfect crimes. It's easy for computer crimes to go undetected if no one checks up on what the computer is doing. But even if the crime is detected, the criminal may walk away not only unpunished but with a glowing recommendation from his former employers. Of

course, we have no statistics on crimes that go undetected. But it's unsettling to note how many of the crimes we do know about were detected by accident, not by systematic audits or other security procedures. The computer criminals who have been caught may have been the victims of uncommonly bad luck.

Vocabulary

1. Computer abuse	злоупотребление компьютером
2. Phone freaker	телефонный мошенник
3. To go undetected	оставаться необнаруженным
4. Picking	воровство
5. To transfer funds	переводить денежные средства
6. Checking account	расчетный счет
7. To issue checks	выписывать чеки
8. Supply	поставка
9. Cash-dispensing terminals	аппараты обналичивания денеж. средств
10. Counterfeit	подделка
11. Competitor	конкурент
12. Attempt	попытка
13. To punch	пробивать
14. Unauthorized	несанкционированный, без права доступа
15. To restrict access	ограничить доступ
16. Benefit	польза, выгода
17. Audit	аудит

Vocabulary exercises

1. Read, write down and memorize the following words and word combinations.
2. Give Russian equivalents of the following words and word combinations:
1) to reap substantial reward: 2) would-be criminals: 3) 160 case his-

tories; 4) to be caught doing smth; 5) trained auditors; 6) to ship company's products; 7) to gain access to funds; 8) organized crime; 9) to finance operations; 10) to use for blackmail; 11) to come to light; 12) crooked computer experts; 13) to devise a variety of tricks; 14) to avoid telephone charges; 15) to dial telephone number; 16) to be subject to smth; 17) wanted criminals; 18) security procedures.

3. Give English equivalents of the following words and word combinations:
1) избежать наказания; 2) не остаться незамеченным; 3) пресловутая верхушка айсберга; 4) хранить счета; 5) предлагать много возможностей; 6) воображаемые поставки и услуги; 7) переводить по желанию; 8) поддельные электронные карточки; 9) субсидировать организованную преступность; 10) нещепетильные конкуренты; 11) лица без права доступа; 12) телефонные мошенники; 13) появиться в списке; 14) обнаружить случайно.

4. True or false?
1. A person is innocent until proven guilty.
2. Computer-related crime has diminished.
3. A thief can transfer funds from other people's accounts.
4. Dishonest employees can't ship the company's products to addresses of their choosing.
5. It is impossible to counterfeit credit cards.
6.Phone freaks can be found out.
7. Personal information should not be stored in computer files.
8. A real bank checks very carefully before handling out any money.
9. Unauthorized persons have proved to be inefficient laymen.
10. Hardware is less expensive than software.
11. Computer criminals will never be caught.
12. Companies don't punish some criminals because they don't want bad publicity.

5. Answer the questions.

1. What spheres of life is computer abuse registered? 2. What is the danger of electronic counterfeiting in banking? 3. Can cash-dispensing terminals pose a threat to credit cards transactions? 4. Can stolen information be used for blackmail? 5. What variety of tricks have crooked computer experts devised to benefit from unauthorized access to confidential information? 6. Is it possible that some computer crimes can go undetected?

6. Give a summary of the presented material.

Unit 6 .
Text 1.
The Information Protection in the Global Network Internet.

The global network Internet takes a significant place in a modern society. The access of organization to the global network Internet essentially increases its functioning effectiveness and opens a set of new opportunities. On the other hand, the organization should provide the creation of information resources protecting system to prevent an access of unauthorized users, who may use, modify or destroy important information. Regardless of its specifics, the information protecting system for global networks is part of general security complex that directed on information safety assurance. The information protection is the complex of means directed on information safety assuring. In practice it should include maintenance of integrity, availability, confidentiality of the information and resources that are used for data input, saving, processing and transfer. The complex character of this problem emphasizes that for its solution the combination of legislative, organizational and software-hardware measures should be realized.

The main threats to the information safety in Internet.

The unauthorized access (UAA) in the Internet can be performed, in particular, using the following actions:

- penetration into network with the purpose of reading the

confidential information;

- penetration into network with the purpose of updating or destroying the existing information;
- embedding of the programs – viruses, which will disorganize the network functions or perform all the above mentioned actions;
- destroying of the Internet-servers functioning or local computers connected to the Internet.

All these actions can be realized separately or in any combination.

Let's list some examples of the unauthorized intrusions in the Internet: smart attacks, the Internet-viruses, the Troyan programs that assemble the secured information from WEB-pages, destroy the servers functioning, etc.

The protection from unauthorized access in the Internet.

Every information protecting means is directed to the certain type of safety threats, and realizes the protection against specific types of the unauthorized access. There are program and hardware protecting tools.

The software protecting tools are program complexes intended to reveal and to prevent the possible UAA threats. The examples of software protection tools are: firewalls, cryptographic program means, authenticating means, means for the vulnerable network components definition and protection.

The hardware tools are the set of hardware means intended to the data enciphering and to the protection from viruses. The examples of hardware tools are: cryptographic electronic boards and Hardware complexes – anti-viruses.

Nowadays the simple approaches to the protection system organization are the most widespread, such as the systems for protection from the unauthorized users access. These systems are rather reliable, however, they do not offer the required flexibility. They are based on the various tools for protection assurance, for example, the tools that permit the data transfer only to those users who possess the certain addresses of network protocol IP, tools that deny the direct

users access to the Internet resources and local networks. The shortcomings of this approach consist in narrowness of the solved problem: to prevent access of the unauthorized users to the various local networks. The Similar protection is used for access prevention of the certain users of the local network (for example, corporate network of the enterprise) to all the Internet resources, except for electronic mail. The principle of this protection method is the next: the protection of the local information and decreasing of external channels traffic. However users and providers of the Internet services are more concerned in maintaining of general safety of network, in particular, the confidentiality of the information of the sender and receiver, and the absolute reliance is necessary for the providers and users that on the other end of the communication channel is the legal user.

Vocabulary

1. Information security assurance	гарантия информац. безопасности
2. Integrity	целостность
3. Availability	доступность
4. Penetration	проникновение
5. Embedding of a program	установка программы
6. Intrusion	вторжение
7. Smart attack	управляемая атака
8. Interchange	взаимообмен
9. Authenticating means	средства придания аутентичности
10. To encipher	кодировать

Vocabulary exercises

1. Read, write down and memorize the following words and word combinations:
2. Give Russian equivalents of the following words and word combinations:

1) branches of information; 2) functioning effectiveness; 3) to modify information; 4) regardless of its specifics; 5) maintenance of integrity; 6) safety threats; 7) a complex intended to reveal; 8) vulnerable network components; 9) cryptographic electronic boards; 10) to be most widespread; 11) to consist in narrowness of the solved problem; 12) external channels traffic; 13) to be concerned in.

3. Give English equivalents of the following words and word combinations:
1) ресурсы, которые используются для ввода данных, сохранения их, обработки и передачи; 2) комплексный характер проблемы; 3) проникновение в сеть с целью; 4) вирусы, которые дезорганизуют работу сети; 5) вышеупомянутые действия; 6) надежные системы; 7) недостатки подхода; 8) законный пользователь; 9) быть направленным на обеспечение гарантии информационной безопасности.

Text 2.
The Protocol SSL and its Extension PCT

Today the various mechanisms for the solution of the wide spectrum of problems of information safety maintenance in the Internet are developed. The most known and the most advanced information protection means is protocol Secure Socket Layer (SSL) offered by Netscape. The wide distribution of it caused the SSL realization by the other large corporations such as the IBM, Microsoft and Spyglass. They have embedded this protocol in the applications using for systems based on architecture the client-server.

The version SSL 2.0 takes into account the most important aspects of information protection in the network: authentication and enciphering. Authentication is necessary for confirmation of the fact that the user is legal. Usually the user only needs to input the identifier (network “name”) and password. However during authenticating process the intruder can “overhear” on the communication channel and intercept the user password and identifier. The mechanism SSL

and the Authenticating methods of types PAP or CHAP that used in many remote access systems, are mainly similar.

The protection from UAA is necessary not only for user identificating data, but also for electronic mail or for confidential files loaded from FTP-server. In the SSL for these purposes the enciphering is realized that allows to ensure the safety practically to all the information, transferred between user and server.

Protocol SSL is not absolutely perfect. Some doubts concerning reliability of used enciphering mechanism are expressed. In order to correct this situation, the Microsoft has offered the extension of the protocol SSL that named PCT (Private Communications Technology). It is expected, that this new protocol will be embedded into the structure of the universal system "Information Server" for access in the Internet, created by Microsoft. The additional key specially intended for authentication is proposed in the PCT. Besides that the Microsoft is going to develop more proof algorithm for random numbers generation. This generator, intended for creating of enciphering key, is considered as one weaker item in the protocol SSL safety. It is mentioned, that protocol SSL even supplied with PCT options, is not capable to solve a problem of absolute safety of the information. The systems of general protection, the similar to the combination SSL and PCT only prevent an opportunity of viewing transferring messages and data contents that may have happened on communication lines. At the same time they are not quite suitable for restriction or protection from access to the information sources.

There are several groups of the Internet users, whose requirements are out from frameworks of standard confidentiality. For example, one of such large and influential groups is governmental structures. The absolutely reliable authentication is especially important for these structures. The critical importance for them has the guarantee that the users and information services are really legal. The system Fortezza is a mechanism guaranteeing the increased information security level and more preferable to these users of the Internet.

Vocabulary

1. To embed	включить, внедрить
2. Authentification	подтверждение подлинности
3. Enciphering	кодирование, шифрование
4. Intruder	человек незаконно нарушающий права другого человека
5. SSL	протокол защищенных сокетов
6. PCT	технология конфиденциальной связи
7. Legal	законный, имеющий права
8. Framework	структура, каркас
9. Influential	влиятельный
10. Preferable	предпочтительный

Vocabulary exercises

1. Read, write down and memorize the following words and word combinations.
2. Give Russian equivalents for the following words and word combinations:
1) advanced information protecting means; 2) to input the identifier; 3) the intruder can “overhear”; 4) remote access systems; 5) enciphering key; 6) to view transferring messages; 7) to be suitable for; 8) client-server architecture; 9) concerning reliability; 10) to offer the extension of the protocol.

3. Give English equivalents for the following words and word combinations:
1) обеспечить безопасность; 2) реализовать кодирование; 3) выражать сомнения по поводу; 4) главным образом простые; 5)будет включен в структуру; 6) за пределами рамок; 7) правительственные структуры; 8) особая важность; 9) повышенный уровень безопасности информации; 10) влиятельные группы.

4. True or false?

1. The access of organization to the global network essentially increases its functioning effectiveness and opens a set of new opportunities.
2. In practice information safety assurance should include maintenance of integrity, availability and confidentiality of the information and resources used only for data transfer.
3. Penetration into network with purpose of reading the confidential information is not the authorized access case.
4. Every information protecting means is directed to the certain type of safety.
5. Information safety assurance is part of general security complex.
6. Firewalls, authenticating means and cryptographic program means are program protecting tools.
7. Information protecting means include only software protecting tools.
8. Users and providers of the Internet services are less concerned in maintaining general safety of network.
9. Nowadays the simple approaches to the system organization are most widespread.
10. The narrowness of the solved problem is the advantage of such approach as protection from unauthorized users access.

5. Answer the questions.

1. Why should one provide the creation of information resources protecting system? 2. What types of information threats in Internet do you know? 3. What does UAA mean? 4. How can the unauthorized access be performed? 5. What are the most widespread means for information protection? 6. What are the shortcomings of systems for protection from unauthorized users access? 7. What is the most known information protecting means? 8. Why is SSL not absolutely perfect?

6. Summarize the main points presented in the text.

Unit 7.
Text 1.
Intranet Security

Intranets: An Emerging Business Resource. Intranets are revolutionizing the way organizations function. Internal Web servers have moved from being a repository for simple shared content to encompassing applications that interact with legacy systems. Unfortunately, these advantages also bring critical risks if the intranet is not properly secured. CTR's new report, Intranet Security, is designed to help information systems (IS) managers and other information security personnel work together to build secure corporate intranets. The report discusses the misconception that intranets are intrinsically more secure than Internet applications and explains why businesses must evaluate their risk level before implementing a security policy. Specific security tools and the future of intranets are also examined in detail.

Intranet Security: Internal and External Risks. CTR's Intranet Security report evaluates the internal and external risks related to intranets, including: data theft, viruses. Web server vandalism, client security, and reusable passwords. Reusable passwords act as the doorway for intruders in 72% of attacks. The report addresses the need for strong authentication methods, such as one-time passwords (OTP) and digital certificates. The report also explores the risks associated with providing remote intranet access. Virtual private networks (VPN's) provide a means to securely connect remote offices to the intranet. The technology behind VPN's is examined, as well as the cost of providing access using VPN's versus leased lines. Because intranets are typically open to the entire company, the majority of security breaches are committed internally. The report discusses this issue and offers valuable information on how to protect your organization against internal security breaches.

Intranet Security Solutions. Intranet Security offers an in-depth discussion of available intranet security products and technol-

ogies. Perhaps the most well-known measure for securing intranets is the use of firewalls. The report compares the different types of firewall products, describes the capabilities and limitations of firewalls, and offers a set of guidelines for successfully operating firewalls. Another key technology for securing intranets is encryption and offers an overview of important encryption concepts and technologies such as public key encryption, digital signatures, and the Secure Sockets Layer (SSL).

Developing an Intranet Security Policy. Developing an intranet security policy is the most important measure that organizations can take to improve their security. While existing security policies may address computing and network issues, intranet policies must cover such areas as intranet publishing guidelines and employee use of the Internet. CTR's new report provides specific steps for putting together an effective intranet security policy, including conducting a corporate audit, monitoring computer and Internet use, and educating intranet users. Information on how to respond to security incidents and advice on hiring security staff is also included.

Future Trends in Intranet Security. Intranet Security includes a discussion of trends in the intranet security market, including all-in-one solutions, increased use of security outsourcing, and predictions that intranet security breaches will increase in the short term as many organizations are reactive rather than proactive in implementing intranet security. One important, and very popular, trend in corporate intranets involves making intranets available to third parties. Extended intranets, called extranets, allow customers and business partners access to the intranet. This connection enables the use of technologies such as E-commerce. Intranets offer strategic advantages to businesses by creating a centralized knowledge base, enabling collaboration, and providing a standard interface to information across all hardware platforms. As intranets grow into trusted resources, relied on by employees and customers alike, the need to protect them becomes paramount. This new report from CTR includes the tools and information necessary to help ensure the protection and success of your corporate intranet.

Vocabulary

1. Repository	хранилище
2. Misconception	неправильное представление
3. To implement a security policy	проводить политику безопасности
4. Reusable password	многоразовый пароль
5. One-time password	одноразовый пароль
6. Remote intranet access	удаленный доступ к сети
7. Security breach	брешь в защите
8. Firewall	брандмауер (ср-ва межсетевой защиты)
9. Security outsourcing	аутсорсинг безопасности (передача стороннему подрядчику функций по организации и проведению мер обеспечения безопасности.

Vocabulary Exercises

1. Read, write down and memorize the following words and word combinations.
2. Give Russian equivalents of the following words and word combinations:
1) to interact with legacy systems; 2) to build secure corporate internets; 3) the internal and external risks related to intranets; 4) to act as a doorway for intruders; 5) to explore the risks associated with; 6) using VPN's versus leased lines; 7) capabilities and limitations of firewalls; 8) the report assesses the need for encryption; 9) simple shared content; information security personnel; 10) to put together security policy; 11) to enable the use of technology.

3. Give English equivalents of the following words and word combinations:
1) оценить уровень риска; 2) специальные средства безопасности; 3) воровство данных; 4) предлагать обзор важных концеп-

ций; 5) охватывать такие области как; 6) принимать меры по улучшению безопасности; 7) обучать пользователей сети; 8) реагировать на инциденты; 9) включая решения « все в одном»; 10) в краткосрочной перспективе; 11) обеспечивать сотрудничество; 12) централизованная база знаний.

Text 2.
Hash Function

A hash function H is a transformation that takes a variable-size input m and returns a fixed-size string, which is called the hash value (that is, h=H(m)). Hash functions with just this property have a variety of general computational uses, but when employed in cryptography the hash functions are usually chosen to have some additional properties.

The basic requirements for a cryptographic hash function are:

- the input can be of any length,
- the output has a fixed length,
- H(x) is relatively easy to compute for any given x,
- H(x) is one-way,
- H(x) is collision-free.

A hash function H is said to be one-way if it is hard to invert, where “hard to invert” means that given a hash value h it is computationally infeasible to find some input x such that H(x)=h.

If, given a message x, it is computationally infeasible to find a message y i x such that H(x)=H(y) then H is said to be a weakly collision –free hash function.

A strongly collision-free hash function H is one for which it is computationally infeasible to find any two messages x and y such that H(x) =H(y).

The hash value represents concisely the longer message or document from which it was computed; one can think of a message digest as a “digital fingerprint” of the larger document. Examples of well-known hash functions are MD2, MD5 and SHA.

Perhaps the main role of a cryptographic hash function is in the provision of digital signatures. Since hash functions are generally faster than digital signature algorithms, it is typical to compute the digital signature to some document by computing the signature on the document's hash value, which is small compared to the document itself. Additionally, a digest can be made public without revealing the contents of the document from which it is derived. This is important in digital timestamping where, using hash functions, one can get a document time stamped without revealing its contents to the timestamping service.

Vocabulary

1. Hash	ненужная информация
2. Property	характеристика, свойство
3. Variable	переменная
4. To compute	производить расчеты
5. Infeasible	невыполнимый, неосуществимый
6. Collision-free	без вступления в противоречие
7. Fixed size string	строка постоянного размера
8. Timestamping	с регистрацией времени
9. Digest	зд. вставка

Vocabulary Exercises

1. True or false?

1. CTR's new report is designed to help in building secure corporate intranets.
2. Internal web-servers are simple repositories for shared content.
3. Intranets higher level of security as compared with internet applications is a misconception.
4. OTP and digital certificates are included into the list of risks related to intranets.
5. Intranets are intrinsically more secure than internet applications.

6. Reusable password acts as the doorway for intruders.
7. The majority of security breaches are committed internally.
8. VPN is a less secure technology than a leased line.
9. Firewalls is one of the newest and unfamiliar to users technologies.
10. Developing an intranet security policy is the most important measure that can be taken to improve security status.

2. Answer the questions.
1. Why is it said that intranets are revolutionizing the way organizations function? 2. What is the role of intranets as business resource? 3. What is the risk of intranet security? 4. What is the shortcoming of using a reusable password? 5. What are the ways and perspectives of developing an intranet security policy? 6. What is the most well-known measure for securing intranets? 7. How does an extended intranet function?

Supplement

1. Please study the correspondence of Russian and English terms used in screen menu.

File	Edit	View	Favorites	Tools
	Undo			
	Cut			
	Copy			
	Paste			
	Paste Shortcut			
	Copy to folder			
	Move to folder			
	Select all			
	Invert Selection			

Локальный диск (C:)

Файл	Правка	Вид	Избранное	Сервис
	Отменить			
	Вырезать			
	Копировать			
	Вставить			
	Вставить ярлык			
	Копировать в папку			
	Переместить в папку			
	Выделить все			
	Обратить выделение			

2. Memorize some more expressions which you can find on the computer screen:

1. To map network drive	подключить сетевой диск
2. To disconnect network drive	отключить сетевой диск
3. To create shortcut	создать ярлык
4. Shared documents	общие документы
5. To rename	переименовать
6. To log off	выйти из системы
7. View system information	просмотр сведений о системе
8. Set program access and defaults	выбор программ по умолчанию
9. Files and settings transfer wizard	мастер переноса файлов и параметров
10. Sharing and security	общий доступ и безопасность
11. Add or remove programs	установка и удаление программ
12. My native places	системное окружение
13. Devices with removable storage	устройства с съемными носителями
14. Stacker	накопитель
15. To refresh	обновить
16. Recycle bin	корзина
17. Briefcase	портфель
18. To empty	очистить
19. Clipboard	буфер обмена
20. Dial-up networking	программа удаленного доступа к сети
21. Net watcher	программа инспектирования сети

22. Screen savers	программа заставки
23. To defrag	дефрагментировать
24. Wizard	мастер
25. To restore files that are changed or corrupt	восстановить измененные или поврежденные файлы
26. To arrange icons	упорядочить отображения
27. To line-up	выстроить
28. Clip art	вставка
29. Attribute	вывод на экран из архива
30. Bulletin board	информационная панель
31. Linking	компоновка
32. Swapping	страничный обмен
33. Roll-in, roll out	свертка-развертка
34. Append	установление дополнительного пути поиска файлов
35. Assign	присвоение новой буквы дисководу
37. Break	прерывание работы программы
39. Bug	ошибка, дефект
40. Debug	отладка программы
41. Electronic counterfeiting	электронная подделка
42. Electronic trespass	электронный взломщик
43. Replace	замена файлов в текущей директории с тем же именем из другой директории
44. Substitute	замена полного имени файла на имя дисковода
45. Gadget	техническое новшество
46. Glitch	ошибка, сбой

3. Words and expressions used while typing and editing the text.

1. Backslash	обратная косая черта
2. Boldface	полужирное начертание
3. Brackets	скобки
4. Boundary alignment	выравнивание границ
5. Blank character	знак пробела
6. Colon	двоеточие
3. Comma	запятая
4. Drop cap	большая первая буква в начале статьи
5. Dot	точка
7. Embedded	встроенный, включенный
8. Facing page	титульный лист
9. Flush right	выровненное правое поле
10. Footer	нижний колонтитул
11. Header	верхний колонтитул, заголовок
12. Home	возврат курсора в начало строки
13. Indent	абзац, красная строка
14. Interparagraph spacing	межпараграфный интервал
15. Inverted commas	кавычки
16. Italics	курсив
17. Justification	выравнивание текста
18. Kerning	установка межзнакового интервала
19. Leftmost	крайний левый
20. Left justify	выравнивать левое поле
21. Line, string	строка
22. Line skip	пропуск строки
23. Line feed character	знак смещения строки
24. Lowercase	нижний регистр
25. Margin	поле печатной страницы
26. To mark	ставить знак, помечать

27. Nondestructive backspace	возврат без удаления
28. Page layout	макет страницы
29. Print control character	символ управления печатью
30. Question mark	знак вопроса
31. Reverse type	обратная печать
32. Rotated text	циклически сдвигать текст
33. Scrolling	прокрутка
34. Slash	косая черта
35. Soft carriage return	возврат каретки (с плавающем концом строки)
36. Soft page break	«мягкая» граница страницы
37. Spelling checker	блок орфографического контроля
38. Substring	подстрока
39. Text wrap	свертывание текста
40. Typeover mode	режим верхнего шрифта
41. Upper case	верхний регистр
42. Utmost	самый отдаленный
43. White space	пробельный символ (не выводимый на печать)

Contents

Учебное издание

Катунина Лариса Викторовна

Internet.
Information Protection.

Учебно-методическое пособие
для студентов 2-го курса экономического факультета
(специальность «Прикладная информатика
в экономике»)

Редактор Осипова Е.Н.

Подписано к печати 22.09.2009 г. Формат 60x84 $^{1}/_{16}$.
Бумага офсетная. Усл. п. л. 2,55. Тираж 100 экз. Изд. №1477.

Издательство Брянской государственной
сельскохозяйственной академии
243365 Брянская обл., Выгоничский район, с. Кокино.