МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет кораблебудування
імені адмірала Макарова

Н. М. Філіппова, М. К. Смуглякова

INFORMATION SECURITY

Методичні вказівки з вивчення англійської мови для студентів за напрямом "Захист інформації"

Рекомендовано Методичною радою НУК

Миколаїв 2007

УДК 811.111

Філіппова Н.М., Смуглякова М.К. Information Security: Методичні вказівки з вивчення англійської мови для студентів за напрямом "Захист інформації". – Миколаїв: НУК, 2007. – 64 с.

Кафедра сучасних мов

Дані методичні вказівки є першою частиною навчального комплексу з англійської мови за темою "Захист інформації".

Наведено системи завдань для вивчення лексики з даної теми і розвитку навичок користування цією лексикою (пошукове і поглиблене читання та розвиток мовлення).

Рецензенти:
Є.І. Трушляков, канд. техн. наук, доцент;
Т.І. Козимирська, канд. філол. наук, доцент

ВСТУП

Сьогодні розвинені країни світу переходять на новий історичний етап науково-технічної революції, пов'язаний зі зростанням ролі інформації в суспільному виробництві. Особливістю цього етапу є перетворення індустріального суспільства на інформаційне.

На жаль, інформація, яка накопичується, зберігається та обробляється в автоматизованих системах, є досить уразливою як з точки зору небезпеки її викривлення або знищення (порушення фізичної цілісності), так і з точки зору несанкціонованого доступу до неї осіб, що не мають на це повноважень. Тому методи захисту інформації динамічно розвиваються, ускладнюються і поступово оформлюються в окрему галузь інформаційно-комунікаційних технологій.

До основних аспектів захисту інформації належать сервісна служба, механізм та порушення захисту. Конфіденційність, аутентифікація, цілісність, неможливість відмови, управління доступом, доступність – основні функції, які повинні забезпечуватися відповідними засобами захисту.

Мета даних методичних вказівок полягає у тому, щоб подати студентам, які спеціалізуються у напрямі інформаційної безпеки, вступ до їх спеціальності англійською мовою, допомогти ознайомитися з лексикою і термінологією. Наведено типові тексти, які розвивають навички читання, усного та писемного мовлення.

Unit 1. THE SYSTEMS OF INFORMATION SECURITY

Communication without intelligence is noise; intelligence without communication is irrelevant.
Gen. A.M. Gray

I. Warm-up discussion.

1. What is security for you?

2. What is information security for you?

3. What are threats and disasters? What are information threats and disasters?

4. What do you know about the data protection systems?

5. Do you think whether information security is a state or a continuous process of perfecting?

II. Check if you know the following international words:

computer, system, hacker, information, server, communication, method, algorithm, detector, radiation;

confidential, physical, technical, dynamical, absolute.

III. Check if you know the derivatives.

V	N	Adj	Adv
process			
	protection		
		organizational	
		administrative	
	confidentiality		
	contamination		
implement			
		unauthorized	
	restriction		
	vulnerability		

IV. Translate the following words:

1) accessibility, property, entity, confidentiality, integrity, probability, vulnerability, security, responsibility;

2) distribution, intrusion, information, corruption, communication, classification, distribution, restriction;

3) accidental, confidential, organizational, technical, physical, dynamical;

4) disclose, unauthorised, unlimited, unintentional.

V. Study the following words and divide them into topic groups.

1. [D]DoS ([Distributed] Denial of Service)
2. access
3. access authorization
4. access control
5. access right (permission)
6. accidental disclosure
7. assessment (efficiency, risk or damage)
8. attack
9. audit
10. authentication
11. authorized person
12. availability of information
13. back[-]up
14. breach
15. bug
16. channel
17. cipher (decipher) key
18. classification level (security label)
19. classified information
20. communication interface
21. compromise
22. computer [system] security (COMSEC)
23. confidentiality of information
24. contingency planning
25. corruption of information
26. cost-risk analysis
27. cryptogram
28. cryptology (cryptography and cryptanalysis)
29. decryption
30. dedicated mode
31. denial
32. DES (Data Encryption Standard)
33. digital signature
34. disclosure
35. emission (emanations) security (EMSEC)
36. encryption method
37. environment
38. erasure of information
39. evaluation
40. file
41. firewall
42. fork bomb (logic bomb)
43. gateway
44. global area network
45. hacker (cracker)
46. hanging
47. hard disk [drive]
48. hardware
49. hub
50. information [systems] security (INFOSEC)
51. information carrier
52. integrity of information
53. interface
54. intrusion detection
55. leakage of information
56. leakage point
57. local area network (LAN)
58. log
59. log on, log in (log off, log out)
60. login name
61. malicious code
62. modem
63. need-to-know
64. network architecture
65. network node (host)
66. online
67. operating system
68. password protection (security)
69. PC (Personal Computer)
70. penetration
71. PGP (Pretty Good Privacy)
72. phreaking
73. piggy back
74. processing of information
75. protocol

76. proxy [-server]
77. recovery
78. remote access
79. risk management
80. risk assessment
81. safeguards (countermeasures)
82. secret
83. security (protection) system
84. security policy
85. sensitivity of information
86. server
87. shared access
88. shared resources
89. software
90. steganography
91. TEMPEST
92. threat
93. top secret
94. traffic
95. Trojan horse
96. unauthorized access (illegal access)
97. user account
98. virus (computer virus)
99. vulnerability of information
100. wide area network (WAN)
101. worm
102. WWW (World Wide Web), the Web

VI. Read the following text and find the answers to the questions.

1. What does the "The System of Information Security" include?

2. What is one of the primary concepts of information security?

The Systems of Information Security

The *Systems of Information Security* includes theory and technologies of information processing and storing protection: controlling access to confidential information, protection algorithms, technical devices, organizational and administrative countermeasures, legal basis, etc.

One of the primary concepts of information security is the *information access*. In reference to that, there are two kinds of information: the public one (the information of unlimited access) and, more important, the information of *limited access*. It may be *confidential* (*classified*) or *secret* one.

Usual requirements to processing of confidential information are integrity, accessibility and confidentiality. *Accessibility* is the property of being accessible and usable upon demand by an authorized entity. *Integrity* is the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. *Confidentiality* is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Every potential threat to confidential information can be finally brought to one of three cases: *corruption*, *erasure*, or *leakage* of data. Each of these accidents may affect the processing requirements.

Recently, the probability of the damage has increased concurrently with computer communications development. Facilities of computer local and wide-

area networks, such as shared resources, servers of multi-user access, enterprise environment, etc., cause more vulnerabilities and higher probability of damages.

The incidents with confidential information may be *deliberate* (due to *unauthorized access* to the system) and *unintentional* (e.g. natural disasters or hardware failures). Unauthorized access may be *external* or *internal* and may happen in consequence of computer *hackers attacks* or *cybervandals intrusion*, computer *viruses* contamination, *Trojan horses*, *worms*, etc.

The subject of information security can be divided into *organization*, *system and technical* methods and countermeasures. Another, more detailed classification provides *administrative*, *organization*, *management*, *personnel*, *system*, *communication*, *technical* and *physical* security. Of course, any classification in such a young and, more important, dynamically developing discipline is quite relative.

Administrative and organization measures mean creating information security legislation, *security policy*, security establishment, definition of rights and responsibilities of employees, customers or users, access distribution, risk management, etc.

Software products and algorithms protect computer information systems from external intrusion or internal unauthorized access by *authentication*, *cryptography*, *access control and distribution*, *logging and audit*, *backup and recovery*, *filtering*, *vulnerabilities detecting*, *patching and upgrading*, etc.

Engineering aspects of information protection include various electronic devices restricting, excluding and controlling the access to confidential information or private property, detecting intrusions and attacks, testing vulnerability, various alarm devices, anti-tapping detectors, radiation restriction devices, etc.

One of the main security principles sounds that it is not impossible to implement absolutely secure information system. Hackers' methods become more sophisticated. As cracking tools are appearing in the Internet to be downloaded for free, a user does not need special knowledge to crack a computer system. So the information security is not a state, but a continuous process of perfecting.

SIMPLE INFORMATION SYSTEM

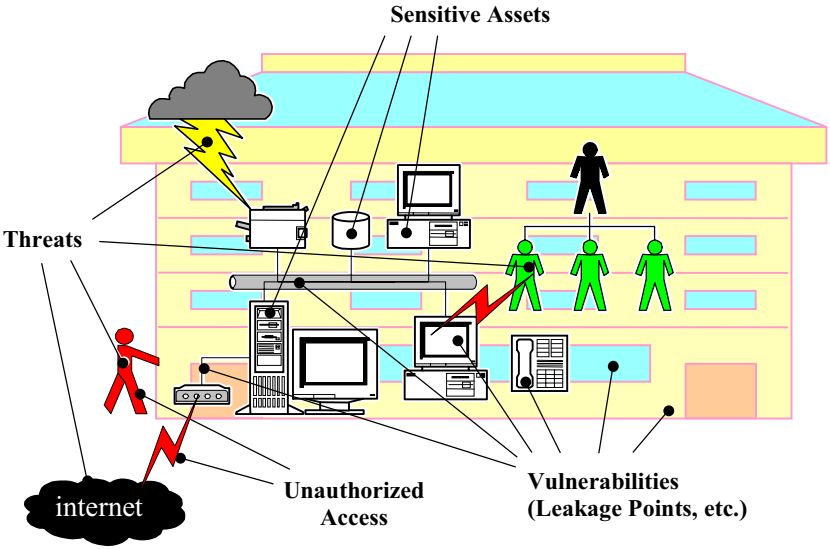


Fig. 1

Now answer the questions.

1. What are the usual requirements to processing of confidential information?

2. What are the accidents that may affect the processing requirement?

3. What are the potential incidents with confidential information?

4. What can the subject of information security be divided into?

5. What are the administrative and organization measures to secure information?

6. What are the means of computer information security?

7. What are the engineering aspects of information protection?

8. Why is the information security not a state, but a continuous process of perfecting?

VII. Check if the statements are true (T) or false (F).

One of the primary concepts, of information security is the information access.

Integrity is the property that data may be changed, destroyed or lost in an authorized manner.

Confidentiality is the property that information may be made available to any individual.

The information security can be divided into administrative, organization, management, personnel, communication, technical and physical security.

One of the main security principles sounds that it is impossible to secure the perfect secure information system.

VIII. Find an odd-man out:

1) to control, to protect, to defend, to cause;
2) limited access, confidential, classified, secret, damage;
3) data corruption, data erasure, data leakage, data storage;
4) to destroy, to lose, to protect, to crack;
5) deliberate, intentional, administrative;
6) legislation, rights, law, hactivism.

IX. Match the requirements with the solutions.

Requirement	Possible Solution
1. **User IDs.** All users should be allocated an identifier (user ID)	a) Public-key infrastructure (PKI); application of cryptographic and authentication protocols for implementing Virtual Private Networks
2. **Access Control.** Access rights should be reviewed at regular intervals. Inactive accounts should be locked	b) Minimise the security vulnerabilities that can be introduced by user modifications. Encourage the use of certified Security Handbooks and Checklists
3. **Software Integrity Checks.** Breaches of software integrity should be detected and prevented	c) Design network and operating system administration procedures to minimise the need for a system administrator account
4. **Security of Network Services.** The service provider's contract should formally define the security issues for the Network Service	d) Standard contracts and terms of business relating to security issues can be standardised by relevant bodies and applied uniformly across all network service providers
5. **Mutual Authentication.** All communicating entities should be authenticated	e) Integrate firewall functionality and auditing facilities into router and gateway software
6. **Network Access.** The flow of traffic to and from external networks should be controlled	f) The operating system should ensure that access is only granted with the provision of an ID and a means of authentication (e.g. password, smart card)

7. **Operational Change Procedures.** Management responsibilities and associated procedures are necessary to ensure satisfactory control of all changes to equipment, software, and procedures	g) Automate the review of access rights based on checklists and procedures available in certified Security Handbooks
8. **Operating System Changes.** When such changes occur the security of the system should be reviewed to ensure that the changes have not introduced any adverse affects	h) Development of sector-specific Incident Reporting Schemes. Some types of incidents could be automatically reported and managed by the network service providers
9. **Access to Manager Accounts.** The system administrator account should not be used for day-to-day operations	i) Include security checks in the installation procedures of operating systems updates. Provide a certification framework for operating system upgrade procedures
10. **Incident Handling.** Security incidents should be detected and investigated thoroughly	j) Several security packages offer file integrity checking. These facilities could be integrated into the operating system

Compare your answers with the text.

Requirement	Possible Solution
User IDs. All users should be allocated an identifier (user ID)	The operating system should ensure that access is only granted with the provision of an ID and a means of authentication (e.g. password, smart card)
Password management. Passwords should be difficult to guess. They should be kept in a one way encryption form; they should change at least once every six months; they should be transmitted in an encrypted form; they are not to be stored in macros or function keys	Current practice in PC-based systems does not comply with the above requirements (e.g. passwords are often stored in macros to be used for ftp or telnet sessions). The problem could be addressed by means of using proactive password checkers, password generators and the provision of relevant services by the operating system. Smart cards provide an alternative authentication method, but appropriate infrastructure is needed (e.g. inexpensive and easy to use card readers, standardisation in smart card technology)

Logical Access Control. The owner of a file or a program should be provided with the facility to specify who is allowed to access the file or program (Discretionary Access Control). All files and directories should have an owner	Incorporate Discretionary Access Control in PC-based operating systems and networking software
Access Control. Access rights should be reviewed at regular intervals. Inactive accounts should be locked	Automate the review of access rights based on checklists and procedures available in certified Security Handbooks
Auditing Tools. A range of facilities for keeping and analysing Audit Logs should be provided. Audit logs should be available in database format and reports should be provided in word-processing format	Provision of easy to use audit tools, with predefined auditing profiles and customisation options. Quite often the difficulties of managing huge audit logs force users not to activate auditing
Investigation of Incidents. When incidents are detected or suspected they must be investigated in a thorough manner	Development of Incident Reporting Schemes (IRS). General purpose CERTs will not be able to address the increasing needs for incident response in the future. The development of sector-specific IRS appears as a more promising solution
System Security Acceptance Criteria. Acceptance criteria should be established against which suitable test should be carried out prior to acceptance of a system as providing the required level of security	Certification of software by accredited certifiers
Software Integrity Checks. Breaches of software integrity should be detected and prevented	Several security packages offer file integrity checking. These facilities could be integrated into the operating system
Detection of Malicious Software. Any malicious software should be detected, identified, isolated, and removed. Users have to deal with attacks from malicious network applets which can cause many problems, such as denial of service, invasion of privacy, and annoyance	Anti-virus tools and good practice rules. All anti-virus tools must be kept up-to-date. Digital signature techniques can be used for the verification of signed applets (e.g. Microsoft's Authenticode technology)

Security of Network Services. The service provider's contract should formally define the security issues for the Network Service	Standard contracts and terms of business relating to security issues can be standardised by relevant bodies and applied uniformly across all network service providers
Mutual Authentication. All communicating entities should be authenticated	Public-key infrastructure (PKI); application of cryptographic and authentication protocols for implementing Virtual Private Networks
Network Access. The flow of traffic to and from external networks should be controlled	Integrate firewall functionality and auditing facilities into router and gateway software
Message Origin Authentication. The origin of a message should be authenticated	Research has provided several non-repudiation techniques that need to be standardised and employed. Digital signatures, based on public-key cryptography, are widely considered as crucial. Legal and regulatory issues have to be addressed by governments leading towards an integrated framework for secure network transactions
Operational Change Procedures. Management responsibilities and associated procedures are necessary to ensure satisfactory control of all changes to equipment, software, and procedures	Minimise the security vulnerabilities that can be introduced by user modifications. Encourage the use of certified Security Handbooks and Checklists
Operating System Changes. When such changes occur the security of the system should be reviewed to ensure that the changes have not introduced any adverse affects	Include security checks in the installation procedures of operating systems updates. Provide a certification framework for operating system upgrade procedures
Access to Manager Accounts. The system administrator account should not be used for day-to-day operations	Design network and operating system administration procedures to minimise the need for a system administrator account
Data Backups. Backups should be taken of all essential business data; backup should be stored in a separate location; it should be possible to re-create data lost since the last backup	Provision of backup services by network service providers; for example, user data backup can be performed over a high-speed network

Security Awareness. Staff should be aware of IT security issues	Small enterprises cannot afford seminars and training programs on security, but at least users should be aware of the threats and of the basic security requirements
Security policies. An IT Security Policy should be documented	Use of baseline or standard security policies developed by associations, standardisation bodies and other trusted organisations
Incident Handling. Security incidents should be detected and investigated thoroughly	Development of sector-specific Incident Reporting Schemes. Some types of incidents could be automatically reported and managed by the network service providers

X. Read the following text and select a suitable headline.

a) Threats analysis;
b) Risk analysis;
c) Damage analysis;
d) Selection analysis;
e) Identification analysis.

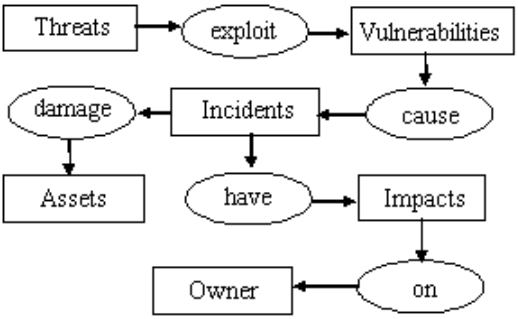


Fig. 2

The CRAMM software tool provides automated selection of countermeasures. CRAMM countermeasures are also ascribed to policy statements that constitute the security requirements of the system and form the basis for the development of a security policy.

The CRAMM methodology (UKCCTA 1996) involves three stages:

Asset Identification and Assessment. This requires the development of a complete model of the IS and considers both tangible assets (e.g. IT equipment) and intangible assets (e.g. information). The asset assessment follows a quantitative approach based on a numeric scale ranging from 1 to 10. The value of an asset is analogous to the impact of the destruction, unavailability, disclosure, or modification of the asset.

Threats and Vulnerabilities Identification and Assessment. This is

achieved by means of using predefined questionnaires. The overall risk is estimated as a combination of the triple threats/vulnerabilities, impacts and asset values.

Countermeasure Selection. This task is performed automatically by the software tool. The CRAMM tool however allows for expert intervention and refinement. CRAMM also facilitates the development of a security policy, the identification of roles and assignment of responsibilities to roles, and the monitoring of countermeasure implementation.

Managing risks may follow three strategies: risk reduction, risk transfer, and risk acceptance. Accepting risk means that although one is aware of it he or she prefers to accept the consequences instead of applying countermeasures. This applies in the case where the cost of countermeasures is significantly higher than the impact of a potential security breach. An example of risk transfer is insurance and applies in particular to physical assets (e.g. computers). Note that in most cases the insurance contract covers the replacement value of equipment and not the value of the data contained or processed by it. Finally, reducing risk could be achieved by means of reducing threat, reducing vulnerability, reducing impact, or recovering from threat occurrences.

CRAMM provides a list of recommended countermeasures that reduce risk in any of the ways mentioned above. A security expert may select those that provide the highest effectiveness with the lowest cost. As a result of the high risk values that we identified in the previous section, we compiled a lengthy list (a few hundred items) of requirements (Dubois and Wu 1996, Rohm et al 1998) and countermeasures to be applied. The most important requirements are abstracted in Table 3. The cost of implementing the countermeasures is obviously beyond the abilities not only of a home-office environment, but of a small enterprise, as well.

XI. Now read the text on risk management software tool and explain how risks can be managed.

XII. Make up the diagram to illustrate what information security is.

XIII. Check if the following proverbs may be used for the above ideas.

1. Everything is good in its season.
2. God helps those who helps themselves.
3. It is never too late to learn.
4. A little learning is a dangerous thing.
5. Live and learn.
6. The more you have the more you want.
7. One cannot be too careful.
8. A rolling stone gathers no moss.
9. You never know what you can do till you try.

10. A wonder lasts but nine days.
11. You will go most safely in the middle.

XIV. Put down 10 sentences to explain what information security is.

XV. Translate the following text (time – 20 min).

Klez Worm Goes after Myriad Files
January 19, 2002
Source: eWeek.com

Yet another e-mail-borne worm is making the rounds on the Internet using an infection and pattern that should be quite familiar to administrators and users. The worm is capable of deleting anti-virus and a lengthy list of other files. On the sixth day of every month save January and July, the worm tries to overwrite all files with the following extensions: .txt, .htm, .html, .wab, .doc, .xls, .jpg, .cpp, .c, .pas, .mpg, .mpeg, .bak and .mp3.

Klez.E showed up on anti-virus companies' radar screens Thursday and hasn't spread very widely, although, as a mass-mailing worm, it certainly has that potential. The e-mail message carrying the worm arrives in the user's inbox with a random subject line and bears an attachment that also has a randomised name. The attachment can be a file with either a .bat, .exe, .pif or .scr extension, according to an advisory published by Symantec Corp., which rates the worm's severity as low.

The attachment carrying the worm can execute either when the user opens it or views the message in Microsoft Outlook's preview pane. Once it is unleashed, Klez copies itself to the Windows System folder and either modifies a certain registry key or creates one of its own. It then creates a value in that key so that the worm will execute once the machine starts up again.

The worm then attempts to disable some virus scanners and, oddly enough, delete other worms such as Code Red and Nimda that may have infected the machine. Klez then drops a virus known as W32.Elkern.3587 on the infected machine and executes it. It also copies itself to local, mapped and network drives using a random file name and double extension, such as filename.txt.exe.

Klez then mails itself to any e-mail address it finds in the user's Windows address book, ICQ database or local files. It can also infect executable files by making a hidden copy of the original host file and then overwriting the original file with the virus.

Fig. 3

XVI. Surf the Internet to find the up-to-date information on the problem discussed in Unit 1.

Unit 2. THREATS TO INFORMATION

The Internet like any other society, is plagued with the kind of jerks who enjoy the electronic equivalent of writing on other people's walls with sprayprint, tearing their mailboxes off, or just sitting in the street blowing their car horns.

I. Warm-up discussion.

1. What threats to information security do you know?

2. How can some software cause damage to information system?

3. Who are people attacking computer system?

4. What factors can attract their attention?

5. Can you rely on a former hacker at your work?

6. What are the differences in the targets of a professional and an amateur hackers?

7. Do you know any methods of getting unauthorized access to computer system?

8. Can your password be a real threat to your computer system?

9. Do you know any techniques how to steal somebody's password?

10. Do you need to be a genius to break into computer system?

II. Look through the text (Task VI) and find the words with the prefixes as in the example. Translate them.

un – unsecure, unreliable, …; in – incredible, independent, …;
dis – dissatisfied, disabled, …; il – illegible, … .

III. Complete the table.

	Verb	Noun	Adjective
1	to attract		
2			responsible
3	to precise		
4		activation	
5	to connect		
6			penetrating
7		representation	
8			secure
9		script	
10			available

IV. Make up a list of adjectives to describe a criminal hacker. Look through the text and add some more words to your list.

V. Read the text and answer the question below.

What do most damages to information system come from?

VI. Divide the text into three parts and give them names.

Threats to Information Security

It is very difficult to estimate precisely what causes damage to information systems. Managers should be skeptical of any statistics about information security if they show very precise numbers. The problem is twofold: people don't recognize crimes or damage, and when they do they usually don't report them anywhere that collects statistics. Surveys that report on computer crime and other breaches of security are useful, but all of them suffer from the problems of voluntary compliance – the fundamental question of whether people who respond to questionnaires are representative of everyone in the field even though many people refuse to participate in the studies. Despite these problems, information security experts generally agree on some rough guesses about how damage occurs.

Perhaps half of all the damage caused to information systems comes from authorized personnel who are either untrained or incompetent. Another quarter or so of the damage seems to come from physical factors such as fire, water, and bad power. Maybe a fifth of the damage comes from dishonest and disgruntled employees. Computer viruses cause another few percent, and maybe about 5 or 10 % of the damage is caused by external attack.

The growth of Internet connectivity is altering these statistics. Many systems were once restricted to internal access, with maybe a slow modem or two for remote access by employees. Today we see production systems (those on which organizations depend day by day for continued operations) nonetheless being opened to access via TCP/IP connections from the wider Internet. Many organizations are also linking their systems tightly with those of trading partners using virtual private networks (VPNs) that increase the number of people allowed to access the systems.

Who are the people attacking computer systems? There seem to the two major classes: amateurs and professionals. Amateurs include poorly supervised children, rebellious and badly socialized adolescents, and psychologically disturbed or ideologically warped adults. Some amateurs cloak their destructive badly-protected computer systems in the language of social responsibility; they claim to have the best interests of their victims of heart. Their actions belie

their words, however: Well-meaning people do not place obscenities and insults on other people's property as these cybervandals do on many a Website.

Hobbyist attacks have recently become a major problem with the widespread availability of tools for distributed denial-of-service attacks (DDoS). Using these tools, even children can locate vulnerable sites on the Internet, implant special "zombie" software, and then later activate the zombie programs to send streams of spurious requests to one or more selected victims. Under siege from dozens or even hundreds of zombie programs, many such victims are swamped by the volume of traffic and see their response time for real customers and visitors increasing unacceptably.

Professionals are harder to characterize, since there are probably fewer of them and they may be harder to catch; however, some criminal hackers are earning a living with their skills. Some professionals use public and illegal sources of information to help unscrupulous private investigators. Some computer criminals steal credit card numbers and sell them to the criminal underground or participate in theft of services from telephone and mobile-phone companies. An unknown number may be involved in industrial espionage.

The use of Microsoft Office products has greatly increased the vulnerability of users because of Microsoft's decision to include a powerful scripting language at the heart of its word-processing, spreadsheet, presentation, database and email products. Email can therefore carry documents that include the equivalent of programs' macro viruses, which can not only harm documents but also call system routines and therefore wreak havoc with the operating system, memory and files. Other contributors to trouble include scripting languages used on Websites (e.g., ActiveX, Java, JavaScript) and even the fundamental formatting language of the Web, the HyperText Markup Language (HTML). All of these tools have been misused to harm users.

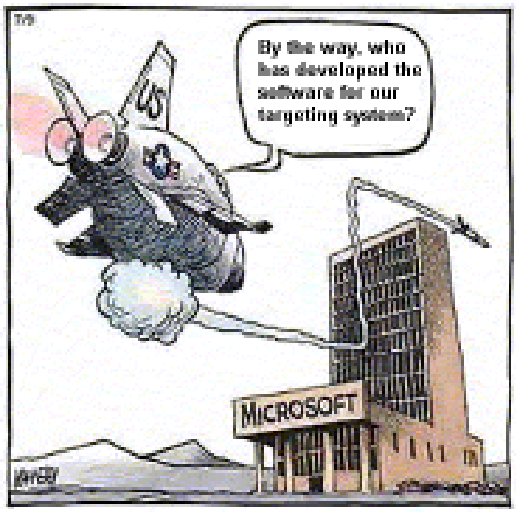


Fig. 4

Some criminal hackers have set up shop as security consultants and offer penetration analysis and consulting services for their clients. There is a serious question about the trustworthiness of people who used to break or skirt the law and now claim that they no longer do so; some security experts argue that leopards have indelible spots, whereas others are willing to believe that there is such a thing as an ex-hacker. I strongly urge managers considering hiring such people to ensure that their contracts include severe penalty clauses if any of their employees are found to be breaching client confidentiality in the course of their duties.

Several factors influence the likelihood of attack. For example, a small, obscure tool-and-die company with eight employees is unlikely to be as attractive to any external attacker as a major corporation with thousands of employees and a significant share of its market. It is possible that having a public Website makes an organization an attractive target for cybervandals. Any site proclaiming its tight security is likely to attract the attention of the amateurs who were trying to prove their prowess; for example, security firms are under constant daily attack. Some amateurs deliberately attack financial institutions and military systems to demonstrate their weakness and ostensibly to force improvements. Finally, some hackers attack sites for political purposes; recent attacks on such victims as Indian nuclear power company Websites are said to be examples of "hactivism."

VII. Match the words below with their explanations:

1) a breach of security	a) to pass along the edge of a law;
2) to cause	b) harm or injury that makes something less useful or less valuable;
3) available	c) capable of being used or obtained;
4) severe penalty	d) a weak point, a fault or defect;
5) remote	e) the action of breaking safety;
6) to skirt a law	f) open to injure or attack, not adequately protected;
7) vulnerable	g) to enter into, to thrust through;
8) damage	h) strict punishment for breaking a law;
9) weakness	i) to produce an effect that makes a thing happen;
10) to penetrate	j) distant, far off in place.

VIII. Find an odd-man out:

1) clause, law, legal, criminal, virtual;

2) to alter, to break, to steal, to prove, reality;

3) unscrupulous lawyer, authorized dealer, powerful computer;
4) hackers, dealers, employers, employees, cybervandals, power;
5) access, network, linking, connection.

IX. Complete the diagram with the information from the text.

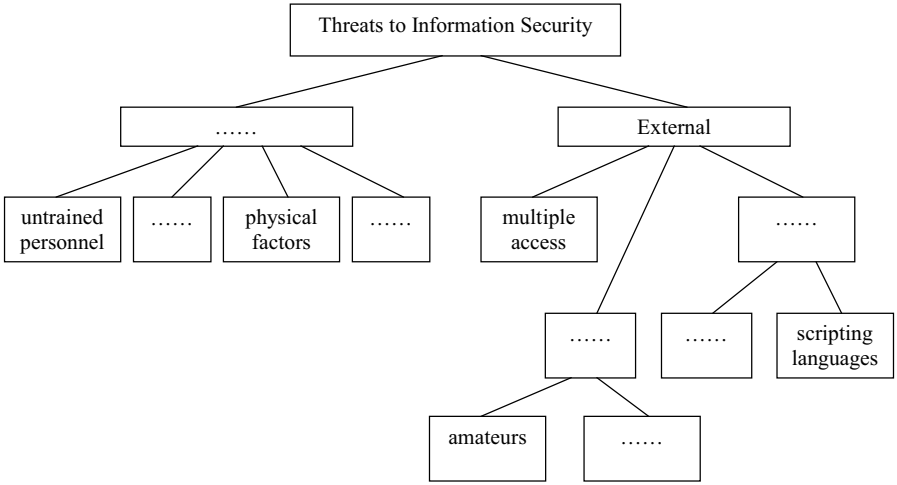


Fig. 5

X. Read the text and find the answers to the questions.

1. What are three common methods to obtain unauthorized access to computer system?

2. What are three main types of computer attackers?

A variety of weaknesses can leave computer systems vulnerable to attack. For example, they are vulnerable when inexperienced or untrained users accidentally violate good security practices by inadvertently publicizing their passwords, weak passwords are chosen which can be easily guessed, or identified security weaknesses go uncorrected. Malicious threats can be intentionally designed to unleash computer viruses, trigger future attacks, or install software programs that compromise or damage information and systems.

Attackers use a variety of methods to exploit numerous computer system vulnerabilities.

Sendmail is a common type of electronic mail used over the Internet. An attacker can install malicious code in an electronic mail message and mail it to a networked machine. Sendmail will scan the message and look for its address, but also execute the attacker's code. Since sendmail is executing at the system's

root level, it has all systems privileges and can, for example, enter a new password into the system's password file which gives the attacker total system privileges.

Password cracking and theft is a technique in which attackers try to guess or steal passwords to obtain access to computer systems. This technique has been automated by attackers; rather than attackers trying to guess legitimate users' passwords, computers can very efficiently and systematically do the guessing. For example, if the password is a dictionary word, a computer can quickly look up all possibilities to find a match. Complex passwords comprised of alphanumeric characters are more difficult to crack. However, even with complex passwords, powerful computers can use brute force to compare all possible combinations of characters until a match is found. Of course, if attackers can create their own passwords in a system, as in the sendmail example above, they do not need to guess a legitimate one.

Packet sniffing is a technique in which attackers surreptitiously insert a software program at remote network switches or host computers. The program monitors information packets as they are sent through networks and sends a copy of the information retrieved to the hacker. By picking up the first 125 keystrokes of a connection, attackers can learn passwords and user identifications, which, in turn, they can use to break into systems.

Once they have gained access, attackers use the computer systems as though they were legitimate users. They steal information, both from the systems compromised as well as systems connected to them. Attackers also deny service to authorized users, often by flooding the computer system with messages or processes generated to absorb system resources, leaving little available for authorized use.

Attackers have varied motives in penetrating systems. Some are merely looking for amusement; they break in to obtain interesting data, for the challenge of using someone else's computers, or to compete with other attackers. They are curious, but not actively malicious, though at times they inadvertently cause damage. Others – known as computer vandals – are out to cause harm to particular organizations, and in doing so, attempt to ensure that their adversary knows about the attack. Finally, some attackers are professional thieves and spies who aim to break in, copy data, and leave without damage. Often, their attacks, because of the sophistication of the tools they use, go undetected.

Also, informal hacker groups, such as the 2600 club, the Legions of Doom, and Phrackers Inc., openly share information on the Internet about how to break into computer systems. This open sharing of information combined with the availability of user-friendly and powerful attack tools makes it relatively easy for anyone to learn how to attack systems or to refine their attack techniques.

XI. Translate the expressions from the text into Ukrainian.

To publicize your password inadvertently; to use a complex password; to refine attack techniques; to unleash computer viruses; to flood the computer system with messages; to obtain user-friendly tools.

XII. Read the text again and find the words which mean the same as the following:

1. unintentional;
2. to use for smb.'s own advantage;
3. wishing or intending to hurt others;
4. to break;
5. authorized;
6. to penetrate.

XIII. Read the text and say who the proverb "The leopard cannot change his spots" refers to.

Do you agree with the author's opinion?

XIV. Read the text below and choose a name for each part.

a) Passive Subversion;
b) Deliberate Penetration;
c) Accidental Disclosure;
d) Active Infiltration.

1. Technological development, technical problems, extreme environmental events and adverse physical plant conditions all present challenges to the smooth functioning of information systems. Large and small events may be equally disruptive to system functioning and use and equally debilitating to the organisation's effective operation. Technical factors leading to failures of information systems are numerous, sometimes not well understood, and constantly changing. They may be computer and communications hardware or software faults and malfunctions, caused by bugs, overloads or other operational or quality problems. The difficulty may arise in an internal system component (system hardware and peripherals, application and operating system software, LANs), an external system component (telecommunication circuits, satellites) or from the interaction of different parts of the system.

Physical threats to information systems fall into two broad categories: extreme environmental events and adverse physical plant conditions. Extreme environmental events include earthquake, fire, flood, electrical storms, and excessive heat and humidity. Accidental disclosures may also occur by improper actions of machine operating or maintenance personnel without deliberate intent.

2. Technical problems may be caused by intentional attacks on the system. Viruses, often introduced into the system via infected software, parasites, trap doors, Trojan horses, worms, and logic bombs are some of the technical means used to disrupt, distort or destroy normal system functions. Deliberate efforts to penetrate secure systems can either be active or passive.

3. One method of accomplishing active infiltration is for a legitimate user to penetrate portions of the system for which he has no authorization. The design problem is one of preventing access to files by someone who is aware of the access control mechanisms and who has the knowledge and desire to manipulate them to his own advantage. For example, if the access control codes are all four-digit numbers, a user can pick any four-digit number, and then, having gained access to some file, begin interacting with it in order to learn its contents.

Another class of active infiltration techniques involves the exploitation of trap-door entry points in the system that by-pass the control facilities and permit direct access to files. Trap-door entry points often are created deliberately during the design and development stage to simplify the insertion of authorized program changes by legitimate system programmers, with the intent of closing the trap-door prior to operational use. There is also the risk of implicit trap-doors that may exist because of incomplete system design-i.e., loopholes in the protection mechanisms.

Another potential mode of active infiltration is the use of a special terminal illegally tied into the communication system. Such a terminal can be used to intercept information flowing between a legitimate terminal and the central processor, or to manipulate the system.

Active infiltration also can be by an agent operating within the secure organization. This technique may be restricted to taking advantage of system protection inadequacies in order to commit acts that appear accidental but which are disruptive to the system or to its users, or which could result in acquisition of classified information. At the other extreme, the agent may actively seek to obtain removable files or to create trap doors that can be exploited at a later date Finally, an agent might be placed in the organization simply to learn about the system.

4. In passive subversion, means are applied to monitor information resident within the system or being transmitted through the communication lines without any corollary attempt to interfere with or manipulate the system. The most obvious method of passive infiltration is the wire tap. If communications between remote terminals and the central processor are over unprotected circuits, the problem of applying a wire tap to the computer line is similar to that of bugging a telephone call.

It is also possible to monitor the electromagnetic emanations that are radiated by the high-speed electronic circuits that characterize so much of the equipment used in computational systems. Energy given off in this form can be remotely recorded without having to gain physical access to the system or to any of its components or communication lines. The possibility of successful exploitation of this technique must always be considered.

XV. Find a term in the text above to match the following definitions.

1) A failure of components, equipment, software, or subsystems, resulting in an exposure of information or violation of any element of the system.

2) Wire tapping and monitoring of electromagnetic emanations.

3) An attempt to enter the system so as to obtain data from the files or to interfere with data files or the system.

4) An intentional and covert attempt to obtain information contained in the system, cause the system to operate to the advantage of the threatening party, or manipulate the system so as to render it unreliable or unusable to the legitimate operator.

XVI. Match the terms and their explanations:

1. Virus	a) is an acronym that stands for Security Administrator Tool for Analyzing Networks. It was designed to help network administrators scan their computers for security weaknesses, but has been used effectively by hackers to break into systems. It is so user-friendly that very little computer experience or knowledge is required to launch automated attacks on systems;
2. Clobbering	b) is any opportunity to penetrate, subvert, mislead, or by-pass security controls through on idiosyncrasy of the software, hardware, procedural controls;
3. Hacking	c) is a code fragment that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources which are then not available to authorized users;
4. Trap door	d) is intentional misuse of authorized system access and unauthorized system access;
5. Software piracy	e) is rendering files or programs unusable;
6. SATAN	f) is unauthorized copying of software.

XVII. The following are some notable, less-than-bright errors that people and IT professionals commit when it comes to computer security. Read the text and complete it with your recommendations.

People regularly lock their houses, demand airbags in their vehicles and install smoke alarms in their homes. But put them in front of a computer, and you'd think the word security was magically erased from their brains. People

are more careless with computers than perhaps any other thing of value in their lives.

Top Five Security Mistakes

Post-it-notes, those sticky yellow things, can undo the most elaborate security measures. Too lazy to remember their passwords, users place them where they and everyone else can see them: stuck to the front of their monitors.

Recommendation One: … .

You may think that certain security measures are necessary, but not all end users agree, which leads them to do an end-run around you. People blithely turn things off they think have a good reason to bypass. Antivirus software is an example. They think it slows down their machine.

Recommendation Two: … .

Dan Bent, CIO at Benefits Systems Inc. in Indianapolis, says he's amazed at the number of users who leave their machines on, without protection, and walk away. Who needs a password?

Recommendation Three: … .

If there's a bugaboo among security experts, it's poorly chosen passwords. Ken Hill, vice president of IT at General Dynamics Corp. in Falls Church, Va., recently attended a demonstration with about 20 of his top engineers and some antihacking experts from NASA. Within 30 minutes, the NASA folks broke 60 percent of the engineers' passwords. Paul Raines, global head of information risk management at London-based Barclays Capital, recommends that users take a common phrase and use its initials for a password. For example: "I pledge allegiance to the flag" becomes "ipa2tf." "That's a difficult password to break because it's a combination of letters and numbers," says Raines.

Recommendation Four: … .

People often talk in public places about things they shouldn't. They will say at a bar, 'I changed my password and added the number 2,' and someone sitting two stools down hears this.

Recommendation Five: … .

XVIII. Can your password be a threat to the computer system? Read the text below and make a list of recommendations to a computer novice about a password.

Some information from the texts in this Unit which you have already read can be useful too.

The choice of a password, a nearly universal user activity and usually a user's first activity on a system, provides a striking example of poor security. Although passwords are employed to control access to most information systems, few users are instructed on the need for password security, on the manner in which to create a password or on penalties for misuse of the system.

Without guidance, many users choose obvious passwords that may be easily ascertained, such as family or pet names, joke words or words related to the task. After logging in to the system, untrained users may display passwords on the side of terminals, share user identification codes and passwords, and leave open access-control doors into high security areas. These are threshold security problems that arise from entering a room, switching on a computer or terminal, possessing a password and logging in.

XIX. Read the texts (time limit – 40 min).

Snooping (Passive Wiretapping). Snooping is a passive attack that involves tapping into the network wire and listening for data that might be valuable. Tapping into the network cable is usually done to acquire information (such as passwords) that might be useful later in a more active attack, especially in an electronic commerce environment.

In a secure configuration, the wire has some type of physical protection to ensure it is not tapped into. Thus, by physically inspecting the hardware for tampering, you can rule out any possibility of a snooping attack having taken place on your network.

Spoofing (Active Wiretapping). Spoofing involves deceiving someone or deceiving the system itself. This is usually done by tapping into the wire and injecting information in an attempt to intercept valuable data destined for a valid user or workstation. Whereas a snooping attacker can use the network adapter to listen in promiscuous mode, the spoofing attacker uses the network adapter (or some other part of the network) to inject data or command packets into the data stream. The hardware or program at the receiving point is "spoofed" into believing that the disingenuous data has come from an authentic source.

Most often the purpose of spoofing is to gain access control to the system by posing as a more privileged user. In another spoofing scenario, known as the "false address" attack, the intruder seeks to acquire a valid workstation address. This type of attack is a threat for every network.

Spoofing Login Programs to Collect Passwords. Spoofing often implies the misuse of a physical hardware address for some purpose other than what it is intended for. However, the login program spoofing attack is designed to acquire a user's identification secrets through some deceptive means, such as

getting the user to reveal the secret when protection does not exist. In this attack, the objective is to obtain login IDs and passwords of end-users or administrators. While other types of spoofing attacks attempt to confuse the actual source with injected information, the spoofing login attack is not intended to confuse anything. Spoofing login is aimed strictly at gaining authentication secrets which can be used at another time.

Password Attacks (Brute-force and Dictionary). *Brute force* password attacks are basic guessing attacks. A *dictionary* attack employs a predefined list of common combinations in an attempt to arrive at a complete username and password. With no security protections in place, anyone can sit down at a workstation and begin attempts to enter the correct username and password. If usernames can be obtained without much effort, or if an actual username is known, all that remains is for the intruder to try to guess the password. If the intruder can view the end-user's actions at entry time, the attack becomes that much easier. While these attacks do not require physical access to the server, they can take place much more easily with physical access.

IP Session Hijacking. This is a relatively sophisticated attack, first described by Steve Bellovin. This is very dangerous, however, because there are now toolkits available in the underground community that allow otherwise unskilled bad-guy-wannabes to perpetrate this attack. IP Session Hijacking is an attack whereby a user's session is taken over, being in the control of the attacker. If the user was in the middle of email, the attacker is looking at the email, and then can execute any commands he wishes as the attacked user. The attacked user simply sees his session dropped, and may simply login again, perhaps not even noticing that the attacker is still logged in and doing things.

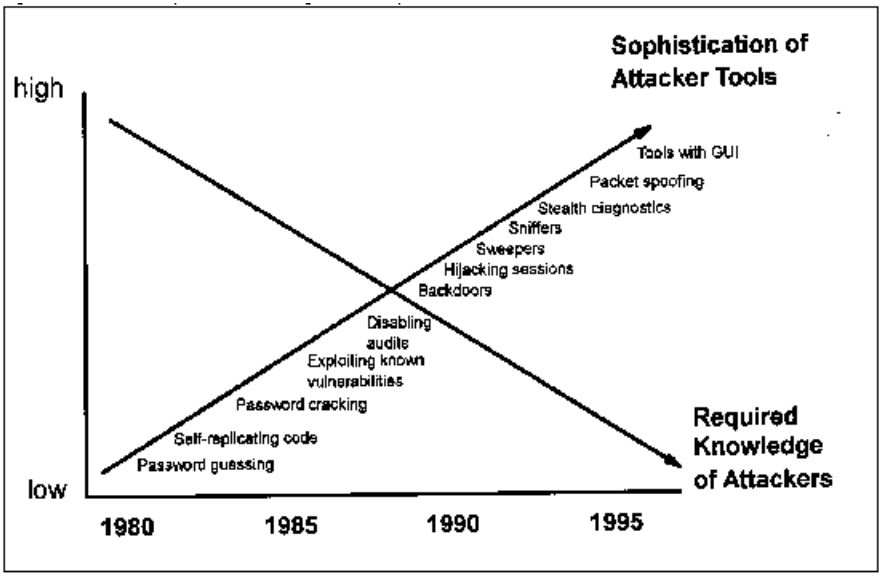
For the description of the attack, let's have a look at the example. A user on host A is carrying on a session with host G. Perhaps this is a telnet session, where the user is reading his email, or using a Unix shell account from home. Somewhere in the network between A and B sits host H which is run by a naughty person. The naughty person on host H watches the traffic between A and G, and runs a tool which starts to impersonate A to G, and at the same time tells A to shut up, perhaps trying to convince it that G is no longer on the net (which might happen in the event of a crash, or major network outage). After a few seconds of this, if the attack is successful, naughty person has "hijacked" the session of our user. Anything that the user can do legitimately can now be done by the attacker, illegitimately. As far as G knows, nothing has happened.

This can be solved by replacing standard telnet-type applications with encrypted versions of the same thing. In this case, the attacker can still take

over the session, but he'll see only "gibberish" because the session is encrypted. The attacker will not have the needed cryptographic key(s) to decrypt the data stream from G, and will, therefore, be unable to do anything with the session.

XX. Study the information on Fig. 6.

The problem is attackers use a variety of tools and techniques to identify and exploit system vulnerabilities and to collect information passing through networks. As technology has advanced over the past two decades, so have the tools and techniques of those who attempt to break into systems. Comment on how the technical knowledge required by an attacker decreases as the sophistication of the tools and techniques increases.



Source: Department of Defense.

Fig. 6

XXI. Surf the Internet to find the up-to-date information on the problem discussed in Unit 2.

Unit 3. VULNERABILITIES

Trust no one ... .

I. Warm-up discussion.

1. What is a vulnerability?

2. What vulnerabilities do you know?

3. What kind of vulnerabilities related to the computer software/ hardware do you know?

4. What are the reasons of their occurrence?

5. What kind of problems can they cause?

6. What are the main factors that can increase the vulnerability of your computer system?

7. Does the technological development make the protection of information system more secure?

8. How does the growth of networks affect system security?

9. Is it easy to detect unauthorized attack on the computer system?

10. How can you get to know about "the visit of unwanted quests"?

II. Translate the following word combinations:

1) security vulnerability, to find a vulnerability, to present a vulnerability, a triggered vulnerability, potential vulnerability;

2) indirect loss, financial loss, quantifiable loss, to result in loss, risks of loss;

3) hardware failure, to cause a failure, undetected failure, possible information system failure, simultaneous failure;

4) intended access, desirable access, unauthorized access, to give an access;

5) password files, to retrieve a password, to crack a password, password snooping, a leaked password.

III. Read the text below and find the answers to the following questions.

1. What factors can increase the system vulnerabilities?

2. How does the growth of networks affect the dependability of information system?

As use of information systems has increased enormously, generating many benefits, it has, in its wake, created an ever larger gap between the need to protect systems and the degree of protection presently utilised. Society, including business, public services and individuals, has become very dependent on technologies that are not yet sufficiently dependable. All the uses of information systems identified above are vulnerable to attacks upon or failures of information systems. There are risks of loss from unauthorised access, use,

misappropriation, modification or destruction of information systems, which may be caused accidentally or result from purposeful activity. Certain information systems, both public and private, such as those used in military or defence installations, nuclear power plants, hospitals, transport systems, and securities exchanges, offer fertile ground for anti-social behaviour or terrorism.

The developments identified above, proliferation of computers, increased computing power, interconnectivity, decentralisation, growth of networks and the number of users, while enhancing the utility of information systems, also increase system vulnerability. It may be harder to locate a system problem and its causes, to correct it in balance with other system functions and requirements, and to prevent its recurrence or the occurrence of other lapses. As systems decentralise and grow larger, it is important to keep account of their interdependent components, which, increasingly, may come from multiple vendors and sources. Moreover, the growing interconnectivity of network systems and use of external networks multiply points of possible information system failures. These externalities lie outside the direct control of the system operators and the rights and duties of the parties in the event of breaches may be unclear.

Technical change is uneven. It leaps ahead in some areas while lagging in others. Inability to adapt to and absorb technological developments at the same rate at which they occur, such as failure adequately to test or co-ordinate system changes, may lead to system problems. Technological developments may be implemented before all their ramifications and relations to existing technologies are understood. Unequal distribution of system capabilities may give some persons more control of and access to information systems than is intended or desirable. Increasing numbers of users have access to information systems, while, at the same time, they are decreasingly directly controlled by system owners or providers.

Failures of information systems may result in direct financial loss, such as loss of orders or payment, or in losses that are more indirect or perhaps less quantifiable by, for example, disclosure of information that is personal, important to national security, of competitive value, or otherwise sensitive or confidential.

The evolution of the law is not always in step with technological progress. It is sometimes insufficient at the national level and in a number of cases still undeveloped at the international level. Harmonization of legislation is an important goal to be actively pursued.

IV. Explain the following expressions from the text above:

1) enhancing the utility of information system;
2) unauthorized access;
3) purposeful activity;
4) interdependent components;
5) a failure of information system.

V. Check if the statements below are true (T) or false (F). Give your reasons.

1. Business and services dependent on technologies are the most vulnerable areas to unauthorized access and failures of information system.

2. At present any event of breaches can be immediately detected by the authorized system operators.

3. There is often a large gap between the technological progress and the legislation system.

4. The main reason most companies pay much attention to information security is just possible direct financial losses.

5. Growth of networks is not considered as a serious vulnerability.

VI. Put down 10 sentences to explain what security vulnerability is.

VII. Read the text (Task VIII) and select the questions to the paragraphs.

1. What does "password cracking" mean?
2. What are two common ways to leak a password?
3. What does "a network sniffer" mean?
4. Is it possible to steal private information from an on-line bookstore?
5. What does "a cookie" mean?
6. How can commerce on the Internet contribute credit card fraud?

A. Companies on the Internet may be opening themselves to allow hackers to find sensitive data from the firm, such as employee's personal records, which may include their home address, any disciplinary actions taken against them, their wages and deductions. Other information that may be tapped are files from the accounting department, files on projects that are in development and other information the company does not wish to make public record.

Another big security issue is credit cards. With the potential to literally create a world wide market, commerce opens a very large hole to credit card fraud. While orders are being made, credit card numbers can be picked up by a third party without knowledge from both the merchant and the customer. Credit card numbers on file inside a companies data base can also be taken. It's already happened once at the Internet Provider (ISP) Netcom of San Jose. While commerce on the Internet is becoming a multimillion dollar business, it is also becoming a large concern for credit card companions and their customers.

Privacy has become an issue as well on the Internet. When Microsoft released Windows 95 in late August in the 1995, the largest software company

in the world thought it would be nice to allow their customers to register the product on-line. What Microsoft neglected to tell anyone was that the customers entire hard drive had been searched and cataloged and that information went up to Redmond's favorite software company's database along with the registration. While this was not directly related to the Internet, you can log into a companies web page and they then can connect to your machine and make queries about it. One method is using "cookies". A cookie is a simple text file that keeps track of where you've been, how long you've been there and other items pertaining to your surf on the web. Currently, only Netscape's Navigator 3.x allows you to adjust your settings to allow for prompting the user to except or deny cookie access when a server requests it.

B. A major reason most companies do pay little attention to security is solely due to ignorance. They just do not realize how easy it is to exploit someone's connection to the Internet. A very large number of companies do have security in place on their systems; however, they forget to lock the door! An Internet only magazine, C|Net, did a story on poor security implementation. The investigating reporters were able to "break" into two sites databases. Booksite, an on-line bookstore, left their door wide open and C|Net was able to walk away with a complete list of credit card numbers of the sites customers. The reporters were also able to "break" into Upside's database and retrieve their mail list. "It didn't require an Olympian effort to get into their site," said C|Net reporter Nick Wingfield. What in fact happened was both companies had left the security feature of the database off.

Even though C|Net returned the stolen items to the proper companies, both were baffled to why the magazine would break into their service's in the name of journalism. The database company, Thunderstone Software of Cleveland, was very disturbed by the break in's and have questioned the legality of the investigation.

C. Most "breaches" occur from the retrieval of passwords. The recent break in into San Jose State's web pages was made possible by a leaked password (as believed by the San Jose Police Department.) There are many methods of password snooping such as, Network Sniffers, grabbing of password files from WIAS Servers, leaks and by users who write their passwords down somewhere that is not secured. Password cracking is a method of many hackers who are able to grab the "passwd" file (the name of the file were passwords sit in on UNIX machines) from getting into a WIAS server which serves to speed logins of users of a web server. The hacker usually will be able to

"crack" the files encryption and then have everyone's password on that system. A more sophisticated way of getting someone's password is to use a sniffer. A sniffer sits between the user and the computer host. The computer simply "sniffs" everything that goes between it, keeps the information and then passes it back into the stream. Neither user or the host know that there is a sniffer on the network. Then there are the non technical ways: someone writes their password down on their desk or tells someone else the password. As hard as it is to believe, it is these two ways that most password are retrieved for abusive use.

VIII. Match the words from the text with their definitions:

1) to adjust	a) to make unfair use of something;
2) abusive	b) spying;
3) snooping	c) treating badly or cruelly;
4) to leak	d) to make suitable or convenient for use, to put in order;
5) to tap	e) to become known in spite of efforts to hide;
6) sniffing	f) taking quick breaths through your nose in order to smell something;
7) to exploit	g) to burst suddenly into, interrupt;
8) query	h) the act of finding and bringing something;
9) to break into	i) a question, request fuller information about;
10) retrieval	j) to obtain something secretly.

IX. Read the text below and put the proper headline to each part.

1. Software Leakage Points.
2. Communication Leakage Points.
3. Hardware Leakage Points.
4. Leakage Point Ecology.
5. Organisational Leakage Points.

A. Hardware portions of the system are subject to malfunctions that can result directly in a leak or cause a failure of security protection mechanisms elsewhere in the system, including inducing a software malfunction. In addition, properly operating equipment is susceptible to being tapped or otherwise exploited. The types of failures that most directly affect security include malfunctioning of the circuits for such protections as bounds registers, memory read-write protect, privileged mode operation, or priority interrupt. Any hardware failure potentially can affect security controls; e.g., a single-bit error in memory.

Both active and passive penetration techniques can be used against hardware leakage points. In the passive mode, the intervener may attempt to

monitor the system by tapping into communication lines, or by monitoring compromising emanations. Wholly isolated systems can be physically shielded to eliminate emanations beyond the limits of the secure installation, but with geographically dispersed systems comprehensive shielding is more difficult and expensive.

Although difficult to accomplish, the possibility exists that covert monitoring devices can be installed within the central processor. The problem is that the computer hardware involved is of such complexity that it is easy for a knowledgeable person to incorporate the necessary equipment in such a way as to make detection very difficult. His capability to do so assumes access to the equipment during manufacture or major maintenance. Equipment is also vulnerable to deliberate or accidental rewiring by maintenance personnel so that installed hardware appears to function normally, but in fact by-passes or changes the protection mechanisms.

Remote consoles also present potential radiation vulnerabilities. Moreover, there is a possibility that recording devices might be attached to a console to pirate information. Other remote or peripheral equipment can present dangers. Printer ribbons or platens may bear impressions that can be analyzed; removable storage media (magnetic tapes, disc packs, even punchcards) can be stolen, or at least removed long enough to be copied.

B. Software leakage points include all vulnerabilities directly related to the software in the computer system. Of special concern is the operating system and the supplementary programs that support the operating system because they contain the software safeguards. Weaknesses can result from improper design or from failure to check adequately for combinations of circumstances that can lead to unpredictable consequences. More serious, however, is the fact that operating systems are very large, complex structures, and thus it is impossible to exhaustively test for every conceivable set of conditions that might arise. Unanticipated behavior can be triggered by a particular user program or by a rare combination of user actions. Malfunctions might only disrupt a particular user's files or programs; as such, there might be no risk to security, but there is a serious implication for system reliability and utility. On the other hand, operating system malfunctions might couple information from one program (or user) to another; clobber information in the system (including information within the operating system software itself); or change classification of users, files, or programs. Thus, malfunctions in the system software represent potentially serious security risks. Conceivably, a clever attacker might establish a capability to induce software malfunctions

deliberately; hiding beneath the apparently genuine trouble, an on-site agent may be able to tap files or to interfere with system operation over long periods without detection.

The security safeguards provided by the operating system software include access controls, user identification, memory bounds control, etc. As a result of a hardware malfunction, especially a transient one, such controls can become inoperative.

Probably the most serious risk in system software is incomplete design, in the sense that inadvertent loopholes exist in the protective barriers and have not been foreseen by the designers.

There may result a security breach, a suspension or modification of software safeguards (perhaps undetected), or wholesale clobbering of internal programs, data, and files. It is conceivable that an attacker could mount a deliberate search for such loopholes with the expectation of exploiting them to acquire information either from the system or about the system e.g., the details of its information safe guards.

C. The communications linking the central processor, the switching center and the remote terminals present a potential vulnerability. Wiretapping may be employed to steal information from land lines and radio intercept equipment can do the same to microwave links. Techniques for intercepting compromising emanations may be employed against the communications equipment even more readily than against the central processor or terminal equipment. For example, crosstalk between communications lines or within the switching central itself can present a vulnerability. Lastly, the switch gear itself is subject to error and can link the central processor to the wrong user terminal.

D. There are two prime organizational leakage points, personnel security clearances and institutional operating procedures. The first concerns the structure, administration, and mechanism of the national apparatus for granting personnel security clearances. It is accepted that adequate standards and techniques exist and are used by the cognizant authority to insure the reliability of those cleared. This does not, however, relieve the system designer of a severe obligation to incorporate techniques that minimize the damage that can be done by a subversive individual working from within the secure organization. A secure system must be based on the concept of isolating any given individual from all elements of the system to which he has no need for access. In the past, this was accomplished by denying physical access to anyone without a security clearance of the appropriate level.

The second element of organizational leakage points concerns institutional operating procedures. The consequences of inadequate organizational procedures, or of their haphazard application and unsupervised use, can be just as severe as any other malfunction. Procedures include the insertion of clearance and status information into the security checking mechanisms of the machine system, the methods of authenticating users and of receipting for classified information, the scheduling of computing operations and maintenance periods, the provisions for storing and keeping track of removable storage media, the handling of printed machine output and reports, the monitoring and control of machine-generated records for the security apparatus, and all other functions whose purpose is to insure reliable but unobtrusive operation from a security control viewpoint. Procedural shortcomings represent an area of potential weakness that can be exploited or manipulated, and which can provide an agent with innumerable opportunities for system subversion. Thus, the installation operating procedures have the dual function of providing overall management efficiency and of providing the administrative bridge between the security control apparatus and the computing system and its users.

E. In dealing with threats to system security, the various leakage points cannot be considered only individually. Almost any imaginable deliberate attempt to exploit weaknesses will necessarily involve a combination of factors. Deliberate acts mounted against the system to take advantage of or to create leakage points would usually require both a system design shortcoming, either unforeseen or undetected, and the placement of someone in a position to initiate action. Thus, espionage activity is based on exploiting a combination of deficiencies and circumstances. A software leak may be caused by a hardware malfunction. The capability to tap or tamper with hardware may be enhanced because of deficiencies in software checking routines. A minor weakness in one area, in combination with similar shortcomings in seemingly unrelated activities, may add up to a serious potential for system subversion.

X. Read the following professional pieces of advice and match them with the proper type of leakage points (Task IX).

1. Currently, the only practical solutions are those used to protect communications systems. – . . . . . .

2. The machine room staff must have the capability and responsibility to control the movement of personnel into and within the central computing area in order to insure that only authorized individuals operate equipment located there, have access to removable storage media, and have access to any machine parts not ordinarily open to casual inspection. – . . . . . .

3. The system designer must be aware of the totality of potential leakage points in any system in order to create or prescribe techniques and procedures to block entry and exploitation. The security problem of specific computer systems must be solved on a case-by-case basis employing the best judgment of a team consisting of system programmers, technical, hardware, and communications specialists, and security experts. – . . . . . .

4. The authentication and verification mechanisms built into the machine system can be relied upon only to the degree that the data on personnel and on operational characteristics provided it by the security apparatus are accurate. – . . . . . .

5. The simultaneous failure of both the protection feature and its check mechanism must always be regarded as a possibility. With proper design and awareness of the risk, it appears possible to reduce the probability of undetected failure of software safeguards to an acceptable level. – . . . . . .

6. It should be emphasized, however, that control of spurious emanations must be applied not only to the main computing center, but to the remote equipment as well. – . . . . . .

7. System designers should be aware that the phenomena of retentivity in magnetic materials is inadequately understood, and is a threat to system security. – . . . . . .

XI. Translate the following word combinations.

1) A program code, an arbitrary code, a malicious code, a demonstration exploit code, to find a code, to execute a code;

2) to monitor emanations, to eliminate emanations, to control spurious emanations, to intercept compromising emanations;

3) an internal file, an original file, an encrypted file, to disrupt a file, to clobber a file, to tap a file, to decrypt a file;

4) to exploit loopholes, to induce a loophole, to search for inadvertent loopholes;

5) a hardware malfunction, a system software malfunction, a circuit malfunction, an operating system malfunction, to induce software malfunctions deliberately.

XII. Arrange the words and word combinations into 4 groups according to the type of vulnerability.

Improper design, remote consoles, procedural shortcomings, safeguards, wiretapping, security clearance, microwave links, deliberate rewiring, inadvertent loopholes, unsupervised use, intercepting emanations, system

shielding, cognizant authority, clobbering information, operating procedures, monitoring devices.

Hardware Leakage Points	*Software Leakage Points*	*Communication Leakage Points*	*Organisational Leakage Points*

XIII. Make up a short report on the most common vulnerabilities.

Words from Ex. XII can be useful. Begin your report with the following pessimistic statement by Sven L.L. Rafferty. "Nothing is full proof or 100 % secure. The only way to absolutely secure your computer is … to turn the power off."

XIV. Study the brief report below on a security vulnerability in Microsoft Internet Explorer and Outlook Express uncovered by Georgi Guninski.

***Date*:** Apr 21 2001 01:19 (UTC/GMT).

***Brief Description*:** The security vulnerability allows IE and Outlook Express to execute arbitrary code without user intervention.

A remote user can create HTML on a web page or in an e-mail message that will cause the web surfer's IE browser or the e-mail recipient's Outlook Express to execute Active Scripting even if Active Scripting is disabled in all security zones. The vulnerability can be triggered via XML stylesheets that contain Active Scripting.

Fig. 7

Some demonstration exploit code is contained in the source message.

***Impact*:** A remote user can create HTML on a web page or in an e-mail message that will cause the web surfer's IE browser or the e-mail recipient's Outlook Express to execute arbitrary code even if Active Scripting is disabled in all security zones.

***Version(s)*:** Internet Explorer 5.x.

***Cause*:** state error.

***Solution*:** No solution was available at the time of this entry.

***Reported By*:** Georgi Guninski <guninski@guninski.com>

XV. Look through the texts below and make up two similar reports.

***Date*:**
***Brief Description*:**
***Impact*:**
***Version*(*s*):**
***Cause*:**
***Solution*:**
***Reported by*:**

Text One. Microsoft Addresses Encryption Flaw In Win2K By Brian McWilliams, Newsbytes REDMOND, WASHINGTON, U.S.A. 11 Jul 2001, 11:42 AM CST.

A flaw in Windows 2000 could allow attackers to read copies of sensitive data that has been encrypted on the computer, Microsoft has acknowledged.

The vulnerability stems from a crash-recovery mechanism in the Encrypting File System (EFS) feature introduced in Windows 2000. In some instances, EFS automatically creates plain-text backups of files as it encrypts or decrypts them, according to a bulletin about the issue at the Microsoft site.

While EFS deletes the backup copies once the original file is successfully encrypted or decrypted, the data may still be present on the drive. This is because Windows 2000, like many operating systems, does not actually remove deleted data but instead de-allocates it so the space can be used by another file.

As a result, an attacker with physical access to the computer could potentially read the deleted data using a low-level disk editor or other tool, Microsoft warned.

According to the Microsoft site, the Windows 2000 encryption feature is designed to protect business users in the event that their laptops are stolen. The Windows 2000 server is also used widely by businesses, including Barnes & Noble and Radio Shack, for their online operations.

The weakness in the Windows 2000 EFS feature was originally reported to the company by Clem Colman of Colman Communications Consulting Pty Ltd.

Colman's advisory on the EFS weaknesses is on the Web at http://www.colmancomm.com/news/20010612efs.htm.

Microsoft's description of the new security tool is here: http://www.microsoft.com/technet/itsolutins/security/tools/cipher.asp.

Text Two. Microsoft Patches Another Serious IIS Web Server Hole

By Steven Bonisteel, Newsbytes REDMOND, WASHINGTON, U.S.A., 19 Jun 2001, 9:33 AM CST.

Microsoft Corp. [NASDAQ:MSFT] has acknowledged another serious security hole in out-of-the-box installations of its Web server software, and it is urging customers to apply a patch it released Monday.

The Redmond, Wash., software giant said the vulnerability – which could afford a hacker access to any files on a compromised system – can be found on Windows NT 4.0, Windows 2000 and the Beta version of its new XP platform, as long as the company's IIS Web server has also been installed.

The problem, discovered by Internet security firm eEye Digital Security of Aliso Viejo, Calif., is rooted in program code supporting functionality known as Microsoft Index Server 2.0 on Windows NT and as Indexing Services on Windows 2000 and XP.

Even if users have no plans to use the indexing technology, a default installation of IIS will load ISAPI extensions supporting the technology, including the code in the file IDQ.DLL, a component used to execute indexing-service scripts.

Researchers at EEye Digital said they found IDQ.DLL code fails to accommodate input that exceeds the memory allocated for such data. That makes the component susceptible to what's known as a buffer overrun (or overflow).

Buffer overruns allow hackers to inject malicious code into areas of computer memory where legitimate programs should run. That rogue software might then execute functions that grant a hacker access to the exploited machine.

Microsoft said that, because IDQ.DLL's code runs at the most-trusted level of security, hackers who exploit the hole could gain system access equivalent to that of a server's administrator.

EEye Digital estimated that at least half of the Internet's several million IIS Web servers may be vulnerable, simply because the indexing technology installs by default.

Microsoft's bulletin on the new problem and information on patches for Windows NT and Windows 2000 systems is available here:

http://www.microsoft.com/technet/security/bulletin/MSO1-033asp.

XVII. Translate the following text (time – 40 min).

Web Scripts. "The project will not aim … to use sophisticated network authorization systems. Data will be either readable by the world (literally), or will be readable only on one files system. All network traffic will be public." – Tim Berners-Lee, creator of World Wide Web.

This quote by Mr. Berners-Lee, currently the Vice President of Netscape Communications, outlines the thinking behind the Web … make it wide open

and hide nothing. This has caused one of the largest problem to securing machines on the Internet. Because of it's "public" centric attitude, the web as allowed a new avenue for hackers to travel down. When a user contacts a web site, that user will become "root" for an instant. Root is a super user on an UNIX machine. The root user can do anything they wish and go anywhere on the server. Since the browser is a client, the user can not exploit this fact; however, smart hackers can fool web servers into thinking they are contacting the host from a browser when in fact they are not. Once the connection is made, the hacker is able to get into the server and as they say on in Reno, "sky's the limit."

CGI Scripts. Another way one can breach a web server is by CGI (Common Gateway Interface) scripts. A cgi script is a "program" that is written to perform a given task on a web server. For example, if you go to Microsoft's web site and you wish to download a beta of some of their software, they ask if you first fill out a form that consists of questions of you name, title and e-mail address. Once you've finished entering the data, you click a button called "Send" and then the script comes alive. It is executed with the depression of the send button and it then takes the information entered and takes all the answers and turns it into E-Mail and then sends it to the webmaster for later use. Now this very same script can also be very revealing to a hacker. In the script, it contains information about the server it sits on. A smart hacker can get this script in it's text form and read it like a map to were the "good" stuff is on the server. Another weak point for the cgi script is it can also be exploited while executing. One can "add" to the scripts instructions and have the server return results that will literally open a door for him or her.

Attack Scans. Attack scans is another way people are able to get into one's computer. Widely available diagnostic tools such as "Internet Security Scanner" and "Security Analysis Tool for Auditing Networks" (SATAN) help hackers find holes to exploit. The release for SATAN describes it as "… a tool to help systems administrators. It recognizes several common networking related security problems, and reports the problems without actually exploiting them." The author of the software refused his employer's request to discontinue support of the product (which was and still is made available for free on the Internet) and was terminated from his position with the firm. Basically, if SATAN can recognize networking problems to an administrator, it can also provide the same information to a hacker on the other side of the network … and the hacker will "… actually (exploit) …" it!

IP/DNS Spoofing. It's the classic "I'm you and you're me" scheme, IP/DNS Spoofing. IP, an address of a computer, spoofing is when some one

masquerades as a trusted host by predicting message sequence numbers. This leads the computer to believe you are someone who has a right to be accessing the host when in fact you do not. DNS, a name representing an IP of a computer, is much like IP spoofing as it masquerades as a trusted host by passing a secured hosts name. Hacker Kevin Mitnick has perfected IP Spoofing and created tools that are readily available on the Internet to make this job "easier" to do.

Encryption. If it's your data you seek to secure as it surfs along the waves of the Internet, then encryption is the way to go. Encryption is taking something readable by a person and using complex mathematical formula's and turn it into some gibbers that a person can not read. Now the receiver of the message must decrypt the file in order to read it's contents. A popular e-mail encryption utility Pretty Good Privacy (PGP) was made by Paul Zimmerman and is so good that the U.S. Government demanded that he "cripple" it because the government was unable to crack it and protested that they would not be able to read transmissions by criminals. It wasn't until just last July that the government dropped their legal pursuit of him (he had been living in Canada for the past four years).

XVIII. Surf the Internet to find the up-to-date information on the problem discussed in Unit 3.

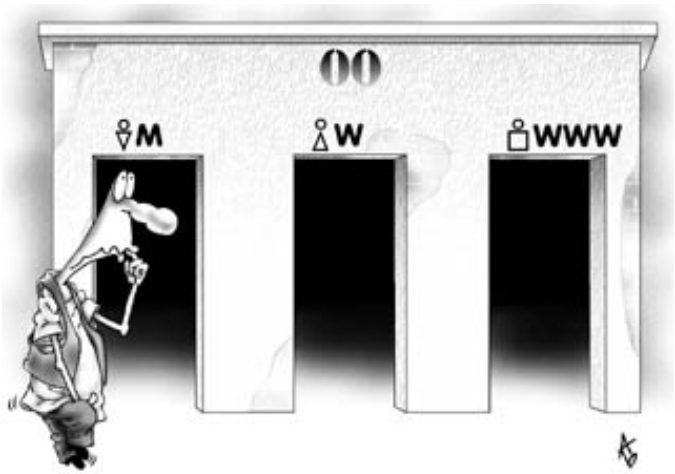


Fig. 8

Unit 4. SECURITY INFORMATION COUNTERMEASURES

A stitch in time saves nine.

I. Warm up discussion.

1. ***What*** *information is valuable?*

2. ***What*** *are the main components of information security?*

3. ***What*** *pops up in your mind when you think about protection?*

4. ***What*** *is precaution?*

5. ***What*** *is warning?*

6. ***What to do*** *if you want to be protected from theft, natural disaster, vandalism, manmade catastrophes, electric surges* (*please, add ...*)*?*

7. ***What to do*** *if you want to be prepared for emergency, to have reliable power supplies and good protection?*

8. ***What to do*** *if you are stuck in an old and decrepit facility?*

9. ***What to do*** *if your budget does not allow to hire full-time security guards?*

10. ***What to do*** *if you want security?*

II. Translate the following word combinations.

Information security, software security, user access security, network security, physical security, user access security, software security;

to back up information, to store information;

to change a password, to share a password, to forbid the use of passwords;

to use properly, to use effectively, to use meaningfully.

III. Match the words with their definitions:

1) protect, safeguard	a) to officially stop the activity;
2) secure	b) to let smth happen;
3) monitor	c) to make a system work in a particular way;
4) control	d) to carefully check the situation to see it changed or progresses;
5) allow	e) to save smth safe from being attacked or harmed;
6) prohibit	f) to keep something safe from harm or damage.

IV. Explain the following.

1. Information and data are synonyms, but information is data with some special meaning.

2. Countermeasures or safeguards are means that are used to prevent the damage.

3. The Information Security Policy is a very important legal document which describes the fundamentals of information security planning, designing and establishing in a organization.

4. A countermeasure is a planned act taken in opposition to another act or potential act.

5. Countermeasures come in a variety of sizes, shapes and levels of complexity.

V. Read the following text and find the answers to the questions.

1. What countermeasures are mentioned?

2. What is the conclusion the authors have made?

The wide use of computers in military and defense installations has long necessitated the application of security rules and regulations. A basic principle underlying the security of computer systems has traditionally been that of' isolation – simply removing the entire system to a physical environment in which penetrability is acceptably minimized. The increasing use of systems in which some equipment components, such as user access terminals, are widely spread geographically has introduced new complexities and issues. These problems are not amenable to solution through the elementary safeguard of physical isolation.

In one sense, the expanded problems of security provoked by resource-sharing systems might be viewed as the price one pays for the advantages these systems have to offer. However, viewing the question from the aspect of such a simplistic tradeoff obscures more fundamental issues. First, the security problem is not unique to any one type of computer system or configuration; it applies across the spectrum of computational technology. While the present paper frames the discussions in terms of time-sharing or multiprogramming, we are really dealing not with system configurations, but with security; today's computational technology has served as catalyst for focusing attention on the problem of protecting classified information resident in computer systems.

Secondly, resource-sharing systems, where the problems of security are admittedly most acute at present, must be designed to protect each user from interference by another user or by the system itself, and must provide some sort of "privacy" protection to users who wish to preserve the integrity of their data and their programs. Thus, designers and manufacturers of resource-sharing systems are concerned with the fundamental problem of protecting information. In protecting classified information, there are differences of degree, and there are new surface problems, but the basic issues are generally

equivalent. The solutions the manufacturer designs into the hardware and software must be augmented and refined to provide the additional level of protection demanded of machines functioning in a security environment.

VI. Explain the following expressions:

application of security rules and regulations;
isolation-simply removing the entire system;
penetrability is acceptably minimized;
new complexities;
elementary safeguard of physical isolation;
expanded problems of security;
resource-sharing systems terms of time-sharing or multiprogramming;
to protect each user from interference by another user;
"privacy" protection;
to preserve the integrity of their data and their programs;
protecting classified information;
to provide the additional level of protection;
a security environment.

VII. Match the words in the left column with their explanation in the right column:

1) natural events	a) the quality or state of being penetrability;
2) intentional acts of destruction	b) making smth safe;
3) unintentional acts of destruction	c) converting data into code, esp. to prevent unauthorized access;
4) encryption	d) deciphering with or without knowledge of the key;
5) decryption	e) a planned step of protection;
6) countermeasure	f) a selected word or phrase;
7) password	g) a hint or indication of difficulty, danger;
8) warning	h) programming errors, accidental downloading of computer viruses;
9) security	i) hacking, viruses;
10) penetrability	j) lightning, ageing, dirt.

VIII. Look through the text and match it with the plan:

a) transmitting the information securely;
b) presenting the information securely;
c) backing up the information properly;
d) storing the information properly.

1. *Use e-mail only for routine office communication*: Never send sensitive information as e-mail. If e-mail absolutely must be used, encrypt the file and send it as an attachment rather than in the text of the e-mail message.

2. *Use dial-up communication only when necessary*: Do so only after the line has been satisfactorily evaluated for security. Do not publicly list dial-up communication telephone numbers.

3. *Encrypt everything before it leaves your workstation*: Even your **password** needs to be encrypted before leaving the workstation on its way to the **network server**-otherwise it could be intercepted as it travels network connections.

4. *Verify the receiver's authenticity before sending information anywhere*: Ensure that users on the receiving end are who they represent themselves to be by verifying.

5. *Practice "views" and "table-design" applications*: A "view" selects only certain fields within a table of information for display, based on the user's access rights. Other table fields are excluded from the user's view and are thus protected from use. For example, although a school record system may contain a range of information about each student, Food Services staff can view only information related to their work and Special Education staff can view only information related to their work. This type of system maintains information much more securely than traditional paper systems, while at the same time increasing statistical utility and accountability options.

6. *Back up not only information, but also the **programs** you use to access information*: Back up **operating system** utilities so that you retain access to them even if your **hard drive** goes down. Also maintain current copies of critical **application software** and documentation as securely as if they were sensitive data. Caution: Some proprietary software providers may limit an organization's legal right to make copies of programs, but most allow for responsible backup procedures. Check with your software provider.

7. *Something they are*-**biometrics** like fingerprinting, **voice recognition**, and retinal scans; these strategies are more expensive but also more secure.

8. *Consider setting up pre-arranged transmission times with regular information trading partners*: If you know to expect transmissions from your trading partners at specific times and suddenly find yourself receiving a message at a different time, you'll know to scrutinize that message more closely. Is it really your trading partner sending the message? Why has the pre-arranged time been ignored? Has the message been intercepted and consequently knocked off schedule?

9. *Maintain security when shipping and receiving materials*: When sending sensitive information through the mail, or by messenger or courier, require that all outside service providers meet or exceed your security requirements.

10. *Use "key identifiers" to link segregated information*: If record information is maintained in a segregated manner (e.g., testing files are kept in a different **database** than special education files) for security purposes, a common file identifier (e.g., a Social Security Number) can be used to match records without unnecessarily divulging the identity of individuals and compromising confidentiality.

11. *Apply recommended storage principles as found in this document to both original and backup files alike*: Backup files require the same levels of security as do the **master files** (e.g., if the original file is confidential, so is its backup). *Clearly label disks, tapes, containers, cabinets, and other storage devices*: Contents and sensitivity should be prominently marked so that there is less chance of mistaken identity.

12. *Segregate sensitive information*: Never store sensitive information in such a way that it commingles with other data on **floppy disks** or other removable data storage media. *Restrict handling of sensitive information to authorized personnel*: Information, programs, and other data should be entered into, or exported from, the system only through acceptable channels and by staff with appropriate clearance.

13. *Inform staff that all messages sent with or over the organization's computers belong to the organization*: This is a nice way of saying that everything in the office is subject to monitoring.

14. *Confirm that outside networks from which there are dial-ins satisfy your security requirements*: Install automatic terminal identification, dial-back, and encryption features (technical schemes that protect transmissions to and from **off-site** users).

15. *Consider using backup software that includes an encryption option when backing up sensitive information*: Encryption provides additional security that is well worth the extra effort, since it ensures that even if unauthorized users access your backup files, they still can't break confidentiality without also having access to your encryption key. If you adopt this recommendation, be sure to change your encryption key regularly.

16. *Physically protect your data encryption devices and **keys***: Store them away from the **computer** but remember where you put them. Use the same common-sense principles of protection you should be giving your bank card's personal identification number (PIN).

IX. Compare it with the original (Task VIII).

1. *Use e-mail only for routine office communication*: Never send sensitive information as e-mail. If e-mail absolutely must be used, encrypt the file and send it as an attachment rather than in the text of the e-mail message.

2. *Encrypt everything before it leaves your workstation*: Even your **password** needs to be encrypted before leaving the workstation on its way to the **network server**-otherwise it could be intercepted as it travels network connections.

3. P*hysically protect your data encryption devices and* ***keys***: Store them away from the **computer** but remember where you put them. Use the same common-sense principles of protection you should be giving your bank card's personal identification number (PIN).

4. *Inform staff that all messages sent with or over the organization's computers belong to the organization*: This is a nice way of saying that everything in the office is subject to monitoring.

5. *Use dial-up communication only when necessary*: Do so only after the line has been satisfactorily evaluated for security. Do not publicly list dial-up communication telephone numbers.

6. *Confirm that outside networks from which there are dial-ins satisfy your security requirements*: Install automatic terminal identification, dial-back, and encryption features (technical schemes that protect transmissions to and from **off-site** users).

7. *Verify the receiver's authenticity before sending information anywhere*: Ensure that users on the receiving end are who they represent themselves to be by verifying.

8. *Something they are*-**biometrics** like fingerprinting, **voice recognition**, and retinal scans; these strategies are more expensive but also more secure.

9. *Consider setting up pre-arranged transmission times with regular information trading partners*: If you know to expect transmissions from your trading partners at specific times and suddenly find yourself receiving a message at a different time, you'll know to scrutinize that message more closely. Is it really your trading partner sending the message? Why has the pre-arranged time been ignored? Has the message been intercepted and consequently knocked off schedule?

10. *Maintain security when shipping and receiving materials*: When sending sensitive information through the mail, or by messenger or courier, require that all outside service providers meet or exceed your security requirements.

11. *Practice "views" and "table-design" applications*: A "view" selects only certain fields within a table of information for display, based on the user's access rights. Other table fields are excluded from the user's view and are thus protected from use. For example, although a school record system may contain a range of information about each student, Food Services staff can view only information related to their work and Special Education staff can view only information related to their work. This type of system maintains information much more securely than traditional paper systems, while at the same time increasing statistical utility and accountability options.

12. *Use "key identifiers" to link segregated information*: If record information is maintained in a segregated manner (e.g., testing files are kept in a different **database** than special education files) for security purposes, a common file identifier (e.g., a Social Security Number) can be used to match records without unnecessarily divulging the identity of individuals and compromising confidentiality.

13. *Back up not only information, but also the **programs** you use to access information*: Back up **operating system** utilities so that you retain access to them even if your **hard drive** goes down. Also maintain current copies of critical **application software** and documentation as securely as if they were sensitive data. Caution: Some proprietary software providers may limit an organization's legal right to make copies of programs, but most allow for responsible backup procedures. Check with your software provider.

14. *Consider using backup software that includes an encryption option when backing up sensitive information*: Encryption provides additional security that is well worth the extra effort, since it ensures that even if unauthorized users access your backup files, they still can't break confidentiality without also having access to your encryption key. If you adopt this recommendation, be sure to change your encryption key regularly.

15. *Apply recommended storage principles as found in this document to both original and backup files alike*: Backup files require the same levels of security as do the **master files** (e.g., if the original file is confidential, so is its backup). *Clearly label disks, tapes, containers, cabinets, and other storage devices*: Contents and sensitivity should be prominently marked so that there is less chance of mistaken identity.

16. *Segregate sensitive information*: Never store sensitive information in such a way that it commingles with other data on **floppy disks** or other removable data storage media. *Restrict handling of sensitive information to authorized personnel*: Information, programs, and other data should be entered into, or exported from, the system only through acceptable channels and by staff with appropriate clearance.

X. Check if the following proverbs may be used for the above ideas.

1. Accidents will happen in the best families.
2. After death the doctor.
3. Any port in a storm.
4. The appetite comes with eating.
5. Best defense is attack.
6. Better a small fish than an empty dish.
7. Better late than never.
8. Better to do well than to say well. Caution is the parent of safety.
9. A close mouth catches no flies.
10. Curiosity killed the cat.

XI. Comment on the following.

The Labour Party must review its electronic security in case the series of damaging leaked memos were captured in cyberspace by a computer hacker, backbenchers said today.

The investigation into the leaks – eight in three months – will almost certainly examine e-mail and other electronic communication between Mr Blair and his closest circle, introduced only over the last few years into Downing Street and Chequers.

Labour backbencher Fraser Kemp, a coordinator in the party's 1997 General Election campaigns, said: "It is certainly the major area of concern that someone is hacking into Downing Street".

"The series of leaks points to a breach of security and I suspect it's electronic".

"I don't know what security levels are on the system but it needs to be looked at".

Labour's Dr Ian Gibson, who sits on the Science and Technology Select Committee said: "It has not been made clear whether these memos were on e-mail or other electronic systems".

"But I would never put anything sensitive on an e-mail, even to a close contact, because nothing's 100 % secure".

"I will now be asking whether Downing Street have someone who is responsible to ensure security of their electronic systems".

Downing Street's computer system, equipped with "firewalls" and other security devices, is supposedly so secure that even senior No. 1 staff have in the past admitted they would rather not use it because the procedure was too laborious.

But an expert in electronic security said a hacker with a "modicum of computing talent" could break just about any security measures given the right equipment and enough determination.

News editor of Secure Computing magazine Steve Gold said: "There are very few systems that aren't crack able given the right amount of computing force and human ingenuity".

The expert, who in the early 1980s was the first Briton convicted for hacking, a verdict later quashed, added: "But given the background of the Labour Party, which had a scare a couple of years ago when it was revealed the pager frequencies were being monitored, I would be surprised if they had used insecure e-mail".

Barrister Alistair Kelman, who specialises in electronic security cases, said: "It's possible that a hacker came out with these memos but, reading the politics of it, I think it's more likely that someone within the Prime Minister's inner circle is briefing against him".

If this was a breach of electronic security, it may not have been a case of computer hacking, he suggested.

The memos may have been found by someone examining a discarded computer disk which had appeared at first glance to have been deleted.

Special Branch detectives may be called in to the leak inquiry if a serious suspect for emerges, but in the past investigations of this kind have frequently proved fruitless.

XII. Translate the following text (time – 40 min).

Keep ***critical systems*** *separate from* ***general*** *systems*: Prioritise equipment based on its criticality and its role in processing sensitive information. Store it in secured areas based on those priorities.

House computer equipment wisely: Equipment should not be able to be seen or reached from window and door openings, nor should it be housed near radiators, heating vents, air conditioners, or other duct work. Workstations that do not routinely display sensitive information should always be stored in open, visible spaces to prevent covert use.

Protect cabling, plugs, and other wires from foot traffic: Tripping over loose wires is dangerous to both personnel and equipment.

Keep a record of your equipment: Maintain up-to-date logs of equipment manufacturers, models, and serial numbers in a secure location. Be sure to include a list of all attached **peripheral equipment**. Consider videotaping the equipment (including close-up shots) as well. Such clear evidence of ownership can be helpful when dealing with insurance companies.

Maintain and repair equipment: Have plans in place for emergency repair of critical equipment. Either have a technician who is trained to do repairs on staff or make arrangements with someone who has ready access to the site when repair work is needed. If funds allow, consider setting up **maintenance contracts** for your critical equipment. Local computer suppliers often offer service contracts for equipment they sell, and many workstation and **mainframe vendors** also provide such services. Once you've set up the contract, be sure that contact information is kept readily available. **Technical support** telephone numbers, maintenance contract numbers, customer identification numbers, equipment serial numbers, and mail-in information should be posted or kept in a log book near the system for easy reference. Remember that computer repair technicians may be in a position to access your **confidential information**, so make sure that they know and follow your policies regarding outside employees and contractors who access your system.

Fig. 9

Identify your equipment as yours in an overt way: Mark your equipment in an obvious, permanent, and easily identifiable way. Use bright (even fluorescent) paint on **keyboards**, **monitor** backs and sides, and computer bodies. It may decrease the resale value of the components, but thieves cannot remove these types of identifiers as easily as they can adhesive labels.

Identify your equipment as yours in a covert way: Label the inside of equipment with the organization's name and contact information to serve as powerful evidence of ownership.

Fig. 10

Make unauthorized tampering with equipment difficult: Replace regular body case screws with Allen-type screws or comparable devices that require a special tool (e.g., an Allen wrench) to open them.

Limit and monitor access to equipment areas: Keep an up-to-date list of personnel authorized to access sensitive areas. Never allow equipment to be moved or serviced unless the task is pre-authorized and the service

personnel can produce an authentic work order and verify who they are. Require picture or other forms of identification if necessary. Logs of all such activity should be maintained. Staff should be trained to always err on the cautious side (and the organization must support such caution even when it proves to be inconvenient).

Store laptop computers wisely: Secure laptops in a hotel safe rather than a hotel room, in a hotel room rather than a car, and in a car trunk rather than the back seat.

Stow laptop computers appropriately: Just because a car trunk is safer than its back seat doesn't mean that the laptop won't be damaged by an unsecured tire jack. Even if the machine isn't stolen, it can be ruined all the same. Stow the laptop and its battery safely!

Don't leave a laptop computer in a car trunk overnight or for long periods of time: In cold weather, condensation can form and damage the machine. In warm weather, high temperatures (amplified by the confined space) can also damage **hard drives**.

Be prepared for fluctuations in the electrical power supply: Do so by (1) plugging all electrical equipment into surge suppressors or electrical power filters; and (2) using Uninterruptible Power Sources (UPSs) to serve as auxiliary electrical supplies to critical equipment in the event of power outages.

Protect power supplies from environmental threats: Consider having a professional electrician design or redesign your electrical system to better withstand fires, floods, and other disasters.

Select outlet use carefully: Although little thought generally goes into plugging equipment into an outlet, machines that draw heavily from a power source can affect, and be affected by, smaller equipment that draws energy from the same outlet.

Guard against the negative effects of static electricity in the office place: Install anti-static carpeting and anti-static pads, use anti-static sprays, and encourage staff to refrain from touching metal and other static-causing agents before using computer equipment.

Keep photocopiers, *fax machines*, *and scanners in public view*: These types of equipment are very powerful tools for disseminating information – so powerful, in fact, that their use must be monitored.

*Assign printers to **users** with similar security clearances*: You don't want employees looking at sensitive financial information (e.g., staff salaries) or confidential student information (e.g., individual records) while they are waiting for their documents to print. It is better to dedicate a **printer** to the

Director of Finance than to have sensitive **data** scattered around a general use printer. Don't hesitate to put printers in locked rooms if that is what the situation demands.

Label printed information appropriately: Confidential printouts should be clearly identified as such.

Demand suitable security procedures of common carriers when shipping/receiving confidential information: Mail, delivery, messenger, and courier services should be required to meet your organization's security standards when handling your confidential information.

Dispose of confidential waste adequately: Print copies of confidential information should not be placed in common dumpsters unless shredded.

XIII. Make up the countermeasures checklist (10 check points).

1. Has contact information for repair technicians (*e.g.*, *telephone numbers*, *customer numbers*, *maintenance contract numbers*) *been stored in a secure but accessible place?*

2. … … .

XIV. Surf the Internet to find the up-to-date information on the problem discussed in Unit 4.

[*D*]*DoS* ([*Distributed*] *Denial of Service*)	відмова служби	отказ службы
access	доступ	доступ
access authorization	санкціонування доступу	санкционирование доступа
access control	контроль, керування доступом	контроль, управление доступом
access right (*permission*)	право (дозвіл) доступу	право (разрешение) доступа
accidental disclosure	випадкове розголошення (витік)	случайное разглашение (утечка)
assessment (*efficiency, risk or damage*)	оцінка (ефективності, ризику або ушкоджень)	оценка (эффективности, риска или повреждений)
attack	атака	атака
audit	аудит, перевірка	аудит, проверка
authentication	автентифікація (перевірка достовірності)	аутентификация (проверка подлинности)
authorized person	уповноважена особа	уполномоченное лицо
availability of information	доступність інформації	доступность информации
back[-]*up*	резервування, резерв	резервирование, резерв
breach	"дірка" (у захисті, системі безпеки)	"дыра" (в защите, системе безопасности)
bug	помилка, "глюк"	ошибка, "глюк"
channel	канал (зв'язку, витоку та ін.)	канал (связи, утечки и т. п.)

cipher (*decipher*) *key*	ключ шифрування (розшифровки)	ключ шифрования (расшифровки)
classification level (*security label*)	рівень (категорія) таємності	уровень (категория) секретности
classified information	конфіденційна інформація з категорією таємності або державна таємниця	конфиденциальная информация с категорией секретности или государственная тайна
communication interface	комунікаційний інтерфейс	коммуникационный интерфейс
compromise	компрометація (розголошення) конфіденційної інформації	компрометация (разглашение) конфиденциальной информации
computer (*system*) *security* (*COMSEC*)	безпека комп'ютерних систем	безопасность компьютерных систем
confidentiality of information	конфіденційність, нерозголошення інформації	конфиденциальность, неразглашение информации
contingency planning	планування непередбачуваних подій	планирование непредвиденных происшествий
corruption of information	пошкодження інформації	повреждение информации
cost-risk analysis	аналіз ризику і суми втрат	анализ риска и суммы потерь
cryptogram	криптограма	криптограмма
cryptology (*cryptography and cryptanalysis*)	криптологія (криптографія і криптоаналіз)	криптология (криптография и криптоанализ)
decryption	розшифровка, декодування	расшифровка, декодирование

dedicated mode	виділений режим	выделенный режим
denial	відмова (в роботі)	отказ (в работе)
DES (*Data Encryption Standard*)	алгоритм шифрування DES	алгоритм шифрования DES
digital signature	цифровий підпис	цифровая подпись
disclosure	розголошення (конфіденційної інформації)	разглашение (конфиденциальной информации)
emission (*emanations*) *security* (*EMSEC*)	захист від побічних електромагнітних випромінювань і наведень (ПЕВіН)	защита от побочных электромагнитных излучений и наводок (ПЭМИН)
encryption method	алгоритм шифрування	алгоритм шифрования
environment	оточення (обчислювальне та ін.)	окружение (вычислительное и др.)
erasure of information	стирання (знищення) інформації	стирание (уничтожение) информации
evaluation	оцінка (ефективності і т. д.)	оценка (эффективности и т. д.)
file	файл	файл
firewall	брандмауер, міжмережний екран	брандмауэр, межсетевой экран
fork (*logic*) *bomb*	логічна бомба	логическая бомба
gateway	шлюз	шлюз
global area network	глобальна мережа	глобальная сеть
hacker (*cracker*)	хакер (крекер), зломник комп'ютерних систем	хакер (крекер), взломщик компьютерных систем
hanging	зависання системи	зависание системы

hard disk [*drive*]	жорсткий диск	жесткий диск
hardware	устаткування, апаратура	оборудование, аппаратура
hub	концентратор	концентратор
information [*systems*] *security* (*INFOSEC*)	безпека (захист) інформації (інформаційних систем)	безопасность (защита) информации (информационных систем)
information carrier	носій інформації	носитель информации
integrity of information	цілісність інформації	целостность информации
interface	інтерфейс	интерфейс
intrusion detection	виявлення вторгнення	обнаружение вторжения
leakage of information	витік інформації	утечка информации
leakage point	канал витоку	канал утечки
local area network (*LAN*)	локальна мережа	локальная сеть
log	журнал, протокол	журнал, протокол
log on, log in (*log off, log out*)	вхід у систему (вихід із системи)	вход в систему (выход из системы)
login [*name*]	ім'я входу	имя входа
malicious code	шкідливий програмний код (віруси, черв'яки, "троянські коні" і т. п.)	вредоносный программный код (вирусы, черви, "троянские кони" и т. п.)
modem	модем	модем
need-to-know	принцип необхідного знання	принцип необходимого знания
network architecture	архітектура мережі	архитектура сети

network node (*host*)	вузол (хост) мережі	узел (хост) сети
online	інтерактивний, діючий	интерактивный, действующий
operating system	операційна система	операционная система
password protection (*security*)	захист паролем	защита паролем
PC (*Personal Computer*)	ПЕОМ, персональний комп'ютер	ПЭВМ, персональный компьютер
penetration	(несанкціоноване) проникнення	(несанкционированное) проникновение
PGP (*Pretty Good Privacy*)	алгоритм шифрування PGP	алгоритм шифрования PGP
phreaking	фрікінг (злом телефонних мереж)	фрикинг (взлом телефонных сетей)
piggy back	пігібекінг (несанкціоноване проникнення за допомогою з'єднання законного користувача)	пиггибеккинг (несанкционированное проникновение с помощью соединения законного пользователя)
processing of information	обробка інформації	обработка информации
protocol	протокол	протокол
proxy-server	проксі-сервер	прокси-сервер
recovery	відновлення (інформації)	восстановление (информации)
remote access	віддалений доступ	удаленный доступ
risk management	керування ризиком	управление риском
risk assessment	оцінка ризику	оценка риска
safeguards (*countermeasures*)	міри безпеки (контрзаходи)	меры безопасности (контрмеры)

secret	секретна інформація	секретная информация
security (*protection*) *system*	система безпеки (захисту)	система безопасности (защиты)
security policy	політика безпеки	политика безопасности
sensitivity of information	таємність, критичність інформації	секретность, критичность информации
server	сервер	сервер
shared access	загальний доступ	общий доступ
shared resources	ресурси загального користування	ресурсы общего пользования
software	програмне забезпечення	программное обеспечение
steganography	стеганографія	стеганография
TEMPEST	дослідження і контроль побічних випромінювань	исследование и контроль побочных излучений
threat	загроза (витоку, пошкодження, вторгнення)	угроза (утечки, повреждения, вторжения)
top secret	державна таємниця, інформація з категорії "цілком таємно"	государственная тайна, информация из категории "совершенно секретно"
traffic	трафік, потік даних	трафик, поток данных
Trojan horse	програма типу "троянський кінь"	программа типа "троянский конь"
unauthorized access (*illegal access*)	несанкціонований доступ	несанкционированный доступ
user account	обліковий запис (рахунок) користувача	учетная запись (счет) пользователя

virus (*computer virus*)	комп'ютерний вірус	компьютерный вирус
vulnerability of information	уразливість інформації (характеристика, зворотна до захищеності)	уязвимость информации (характеристика, обратная защищенности)
wide area network (*WAN*)	розподілена мережа	распределенная сеть
worm	програма типу "черв'як"	программа типа "червь"
WWW (*World Wide Web*), *the Web*	"всесвітня павутина"	"всемирная паутина"

CONTENTS

Навчальне видання

ФІЛІППОВА Ніна Михайлівна
СМУГЛЯКОВА Марина Костянтинівна

INFORMATION SECURITY

Методичні вказівки з вивчення англійської мови для студентів за напрямом "Захист інформації"

(*анлійською та українською мовами*)

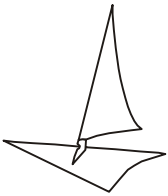
Редактор *О.Є. Вакула*
Комп'ютерна правка та верстка *О.М. Черевата*
Коректор *М.О. Паненко*

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції ДК № 2506 від 25.05.2006 р.

Підписано до друку 05.09.07. Папір офсетний. Формат 60×84/16. Друк офсетний. Гарнітура "Таймс". Ум. друк. арк. 3,7. Обл.-вид. арк. 4,0. Тираж 100 прим. Вид. № 3. Зам. № 277. Ціна договірна.

Видавець і виготівник Національний університет кораблебудування, 54002, м. Миколаїв, вул. Скороходова, 5

ВИДАВНИЦТВО НАЦІОНАЛЬНОГО
УНІВЕРСИТЕТУ КОРАБЛЕБУДУВАННЯ



Шановні панове!

Запрошуємо Вас ознайомитись з можливостями книжкового видавництва, висококваліфіковані спеціалісти якого забезпечать оперативне та якісне виконання замовлення будь-якого рівня складності.

Наш головний принцип – задовольнити потреби замовника у повному комплексі поліграфічних послуг, починаючи з розробки та підготовки оригіналу-макета, що виконується на базі IBM PC, і закінчуючи друком на офсетних машинах.

Крім цього, ми маємо повний комплекс післядрукарського обладнання, що дає можливість виконувати:

- ✓ аркушепідбір;
- ✓ брошурування на скобу, клей;
- ✓ порізку на гільйотинах;
- ✓ ламінування.

Видавництво також оснащено сучасним цифровим дублікатором фірми "Duplo" формату А3, що дає можливість тиражувати зі швидкістю до 130 копій за хвилину.

Для постійних клієнтів – гнучка система знижок.

Отже, якщо вам потрібно надрукувати ***підручники, книги, брошури, журнали, каталоги, рекламні листівки, прайс-листи, бланки, візитні картки,*** *– ми до Ваших послуг.*

© Національний університет кораблебудування
✉ Україна, 54002, м. Миколаїв, вул. Скороходова, 5,
видавництво НУК
☎ 8(0512) 47-83-86; 39-81-41; 39-73-39; fax 8(0512) 39-73-26;