AUES

Since 1975

Noncommercial Joint Stock Company

ALMATY UNIVERSITY OF POWER ENGINEERING AND TELECOMMUNICATIONS

Department
for Language Studies

PROFESSIONAL ORIENTED FOREIGN LANGUAGE. ENGLISH.

Methodological instructions for students of specialty
5B100200 – Information security. Extra texts for self study

Almaty 2019

AUTHORS: G.S. Akhetova. I.K Izembayeva Professional oriented foreign language. English. Methodical Recommendations for students of –“5B100200 – Security of information systems” specialty. – Almaty: AUPET, 2019. - 45 p.

Methodological instructions are intended for conducting practical lessons on professional oriented foreign language with the 2nd year students of information security speciality-5B100200. In this work, technical texts and lexical-grammar exercises are developed for the improvement of speaking, reading, writing and translation skills considering peculiarities of both languages. These Methodological Recommendations give more opportunities ‘for self- studying of security information systems and consist of seven sections including glossary .

References – 16 items.

Reviewer: Senior Lecturer Y.S. Kim

Published according to the plan of publications of noncommercial JSC “Almaty university of power engineering and telecommunications” for 2019.

Introduction

Methodological Recommendations include themes according to the curriculum for teaching Professional oriented foreign language to Bachelor students of the 3d year. Professional technical texts are the basis of these Recommendations. Special attention is drawn to the lexis as well as some English grammar peculiarities which are important for translating.

There are exercises to develop speech activities as reading, speaking, writing, and translating.

These Methodological Recommendations can be used for self - study and for individual work of the students.

Unit 1

Text 1

What is Information security?

1. Read the following text and say what new information you have learnt about security systems.

Information security is the process of protecting the availability, privacy, and integrity of data.

While the term often describes measures and methods of increasing compute security, it also refers to the protection of any type of important data, such as personal diaries or the classified plot details of an upcoming book.

No security system is foolproof, but taking basic and practical steps to protect data is critical for good information security.

Password Protection.

Using passwords is one of the most basic methods of improving information security.

This measure reduces the number of people who have easy access to the information, since only those with approved codes can reach it.

Unfortunately, passwords are not foolproof, and hacking programs can run through millions of possible codes in just seconds.

Passwords can also be breached through carelessness, such as by leaving a public computer logged into an account or using a too simple code, like "password" or "1234". To make access as secure as possible, users should create passwords that use a mix of upper and lower case letters, numbers, and symbols, and avoid easily guessed combinations such as birthdays or family names.

People should not write down passwords on papers left near the computer, and should use different passwords for each account.

For better security, a computer user may want to consider switching to a new password every few months.

Antivirus and Malware Protection.

One way that hackers gain access to secure information is through malware, which includes computer viruses, spyware, worms, and other programs.

These pieces of code are installed on computers to steal information, limit usability, record user actions, or destroy data.

Using strong antivirus software is one of the best ways of improving information security. Antivirus programs scan the system to check for any known malicious software, and most will warn the user if he or she is on a webpage that contains a potential virus.

Most programs will also perform a scan of the entire system on command, identifying and destroying any harmful objects.

Most operating systems include a basic antivirus program that will help protect the computer to some degree. The most secure programs are typically those available for a monthly subscription or one - time fee, and which can be downloaded online or purchased in a store.

Antivirus software can also be downloaded for free online, although these programs may offer fewer features and less protection than paid versions.

Even the best antivirus programs usually need to be updated regularly to keep up with the new malware, and most software will alert the user when a new update is available for downloading.

Users must be aware of the name and contact method of each antivirus program they own, however, as some viruses will pose as security programs in order to get an unsuspecting user to download and install more malware.

Running a full computer scan on a weekly basis is a good way to weed out potentially malicious programs.

Firewalls.

A firewall helps maintain computer information security by preventing unauthorized access to a network. There are several ways to do this, including by limiting the types of data allowed in and out of the network, rerouting network information through a proxy server to hide the real address of the computer, or by monitoring the characteristics of then data to determine if it’s trustworthy.

2. How much do you know about Internet security? Check your knowledge Do the following Quiz.

1. Hackers break into home systems using which of the following methods.

A) Social engineering.

B) Utilizing network administration tools.

C) Trojan programs.

D) None of the above.

E) All of the above.

2. The term "Hacker" refers to…

A) An antisocial individual bent on destroying any computer they can.

B) Someone who likes figuring out how computers work.

C) Ax murderer.

D) None of the above.

E) All of the above.

3. The computer term "cracker" refers to …

A) A hacker that uses their knowledge for criminal activity.

B) A saltine snack.

C) A thief that can open a safe.

D) None of the above.

4. Which of the following is not considered a computer crime?

A) Breaking into other computers for fun.

B) Knowingly distributing computer viruses.

C) Stealing credit cards numbers from others computers and using them to charge things.

D) Writing programs that are used to do harm to other PCs.

E) All the above are computer crimes.

5. It is easier to "hack" into a PC that has a DSL or cable modem connection to the Internet, than a "dial-up" connection.

A) True.

B) False.

6. What must a hacker know to hack into your PC?

A) Your IP address.

B) Your operating system.

C) Your systems vulnerabilities.

D) All of the above.

E) None of the above.

7. Which of the following is not a good defense measure against hackers?

A) Firewall.

B) Antivirus program.

C) Not clicking on files that end in .DLL or .EXE.

D) Using a dial-up modem.

E) All of the above are very good defense measures.

8. How are most computer viruses spread?

A) Floppy diskette.

B) Downloaded off of the Internet.

C) E-mail.

D) Air-borne.

9. Encryption is used for …

A) Sending secure e-mail.

B) Sending credit card information securely over the Internet.

C) Confidential military information.

D) All of the above.

10. A firewall prevents hackers from breaking into your computer.

A) True.

B) False.

11. You will know your computer is infected with a Trojan program when odd things start to happen.

A) True.

B) False.

12. A good password …

A) Is longer that 5 characters.

B) Has a mix of numbers and upper and lower case letters.

C) Should be written and stored in a safe place.

D) All of the above.

E) Two of the above.

3. How could you keep your password secure? Make a list of suggestions for Internet "newbies".

4. Give a short summary of the text.

Text 2

Information security

1. Read the following text and say what new information you have learnt about security systems.

What is information security and why are it systems so important? So what is information security? It is usually understood as the security of information and the entire company from intentional or accidental actions that lead to damage to its owners or users. Ensuring information security should be aimed primarily at preventing risks, rather than eliminating their consequences. It is the adoption of preventive measures to ensure the confidentiality, integrity and availability of information that is the most correct approach in the creation of an information security system.

Any information leakage can lead to serious problems for the company - from significant financial losses to complete liquidation. Of course, the problem of leaks did not appear today, industrial espionage and poaching of qualified specialists existed even before the era of computerization. But it is with the advent of the PC and the Internet have new methods of illegal information. If earlier it was necessary to steal and take out the whole piles of paper documents from the company, now huge amounts of important information can be easily merged into a flash drive, placed in a purse, sent over the network, resorting to the use of a family of rootkits, Trojans, backdoors, key loggers and botnets, or simply destroyed by viruses, arranging a diversion. Often "leaked" from the documents of a financial nature, technological and engineering developments, usernames and passwords to log in to a network of other organizations. But the leakage of personal data of employees can also cause serious harm. This is especially true for Western countries, where lawsuits due to such leaks often lead to huge fines, after the payment of which companies suffer serious losses.

It also happens that the leak harms the company a few months or years after it happened, falling into the hands of competitors or journalists. That is why protection must be comprehensive. Everything that concerns the company's activities and is not intended for publication should remain within the company and be protected from threats.

2. How much do you know about information security? Check your knowledge.

1. Information security is specific to securing information, whereas information systems security is focused on the security of the systems that house the information.

A) True.

B) False.

2. Software manufacturers limit their liability when selling software using which of the following?

A) End user licensing agreements.

B) Software development agreements.

C) By developing error-free software and code so there is no liability.

D) None of the above.

3. The _____ tenet of information systems security is concerned with the recovery time objective.

A) Confidentiality.

B) Integrity.

C) Availability.

D) All of the above.

E) None of the above.

4. Encrypting data on storage devices or hard drives is a main strategy to ensure data integrity.

A) True.

B) False.

5. Organizations that require customer-service representatives to access private customer data can best protect customer privacy and make it easy to access other customer data by using which of the following security controls?

A) Preventing customer-service representatives from accessing private customer data.

B) Blocking out customer private data details and allowing access only to the last four digits of Social Security numbers or account numbers.

C) Encrypting all customer data.

D) Implementing second-tier authentication when accessing customer databases .

E) All of the above.

6. The ________ is the weakest link in an IT infrastructure.

A) System/Application Domain.

B) LAN-to-WAN Domain.

C) WAN Domain.

D) Remote Access Domain.

E) User Domain.

7. Which of the following security controls can help mitigate malicious e-mail attachments?

A) E-mail filtering and quarantining.

B) E-mail attachment antivirus scanning.

C) Verifying with users that e-mail source is reputable.

D) Holding all inbound e-mails with unknown attachments.

E) All of the above.

8. You can help ensure confidentiality by implementing ________ .

A) An acceptable use policy.

B) A data classification standard.

C) An IT security policy framework.

D) A virtual private network for remote access.

E) Secure access controls.

9. Encrypting e-mail communications is needed if you are sending confidential information within an e-mail message through the public Internet.

A) True.

B) False.

10. Using security policies, standards, procedures, and guidelines helps organizations decrease risks and threats.

A) True.

B) False.

11. A data classification standard is usually part of which policy definition?

A) Asset protection policy.

B) Acceptable use policy.

C) Vulnerability assessment and management policy.

D) Security awareness policy.

E) Threat assessment and monitoring policy.

12. The SSCP professional certification is geared toward which of the following information systems security positions?

A) IT security practitioner.

B) Manager of IT security.

C) Director of IT security.

D) Chief security officer.

E) IT security consultant.

Comprehension check.

3. Make up 10 questions according to the text.

4. Give a short summary of the text.

Unit 2

Text 1

Basic principles of information systems

1. Read the following text and say what new information you have learnt about information security systems.

The CIA triad of confidentiality, integrity, and availability is at the heart of information security. (The members of the classic InfoSec triad — confidentiality, integrity and availability — are interchangeably referred to in the literature as security attributes, properties, security goals, fundamental aspects, information criteria, critical information characteristics and basic building blocks). There is continuous debate about extending this classic trio. Other principles such as Accountability have sometimes been proposed for addition - it has been pointed out that issues such as Non-Repudiation do not fit well within the three core concepts.

In 1992 and revised in 2002, the OECD's Guidelines for the Security of Information Systems and Networks proposed the nine generally accepted principles: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment. Building upon those, in 2004 the NIST's Engineering Principles for Information Technology Security proposed 33 principles. From each of these derived guidelines and practices.

In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. The merits of the Parkerian hexad are a subject of debate amongst security professionals.

In 2013, based on a thorough analysis of Information Assurance and Security (IAS) literature, the IAS-octave was proposed as an extension of the CIA-triad. The IAS-octave includes Confidentiality, Integrity, Availability, Accountability, Auditability, Authenticity/Trustworthiness, Non-repudiation and Privacy. The completeness and accuracy of the IAS-octave was evaluated via a series of interviews with IAS academics and experts. The IAS-octave is one of the dimensions of a Reference Model of Information Assurance and Security (RMIAS), which summarizes the IAS knowledge in one all-encompassing model.

Grammar practice.

Passive voice

Passives are very common in technical writing where we are more interested in facts, processes, and events than in people. We use the passive by using the appropriate tenses of the verb to be followed by the past participle of the verb we are using.

Examples:

1) Active.

Many people use the Internet to access and download music and movies (Present Simple).

2) Passive.

The Internet is often used to access and download music and movies (Present Simple).

Present Simple	New users on the Internet *are* sometimes "*called* newbies"
Present Continuous	The blogs *are being* largely *used* as easily-updatable online diaries now
Present Perfect	For as long as people have needed to conduct private conversations across distances, a variety of encryption methods *have been used* to protect secret communications
Past Simple	HTTP *was* originally *designed* by Tim Berners-Lee to support the special demands of web communications
Past Continuous	The movements of users through the website pages *were being tracked* by their IP addresses
Past Perfect	By 2006 new services such as Gmail and Google Video *had been* already *launched* by Google company
Future Simple	In some areas Wi-Fi networks *will be installed*
Future Perfect	Broadband access *will have been provided* in areas with low population density by next year
Modals	Sometimes you *might be asked* if you want to proceed with the immediate installation of the plugin

1. Put each verb in brackets into a suitable passive tense.

1. Dial-up Internet access _____________ (replace) by broadband access in many parts of the world now.

2. By 1990, ARPANET _________ (overtake) and __________ (replace) by newer networking technologies and the project came to a close.

3. The communities of the developing countries ______________ (soon affect) by the capabilities the Internet is brining to individual communications.

4. Bandwidth ___________ (price) by large Internet service providers by several methods, such as at a fixed rate for constant availability of a certain number of megabits per second, or by a variety of use methods that amount to a cost per gigabyte.

5. With the continued doubling of computer capability every couple of years, the “virtual reality” ______________ (integrate) with Internet shortly.

6. Dozens of innovative web browsers ______________ (develop) by various people and teams over the years.

7. In the fifties most communication networks __________ (limit) by their nature to only allow communications between the stations on the network.

2. Rewrite the following sentences using the Passive Voice.

1. We can view the Internet protocol suite as a set of layers.

2. According to the research, people send about 31 billion e-mails worldwide every day.

3. HTML uses tags to describe how and where one should display text, images and any other content.

4. A core group of designers has always driven the architecture of the Internet, but the form of that group has changed as the number of interested parties has grown.

5. Electronics has extended man’s intellectual power.

6. Scientists are looking for new ways for the improvement of Internet technology.

Comprehension check.

2. Make up 10 questions according to the text

3. Give a short summary of the text.

Text 2

Integrity

1. Read the following text and say what new information you have learnt about integrity.

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically provide message integrity in addition to data confidentiality.

Availability.

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

Authenticity.

In computing and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as “digital signatures”, which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

Non-repudiation.

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation.

Electronic commerce uses technology such as digital signatures and public key encryption to establish authenticity and non-repudiation.

Vocabulary.

2. Learn the following definitions.

1. The Bootloader - the software that manages the boot process of your computer. For most users, this will simply be a splash screen that pops up and eventually goes away to boot into the operating system.

2. The kernel - this is the one piece of the whole that is actually called “Linux”. The kernel is the core of the system and manages the CPU, memory, and peripheral devices. The kernel is the “lowest” level of the OS.

3. Daemons - these are background services (printing, sound, scheduling, etc) that either start up during boot, or after you log into the desktop.

4. The Shell - you’ve probably heard mention of the Linux command line. This is the shell – a command process that allows you to control the computer via commands typed into a text interface. This is what, at one time, scared people away from Linux the most (assuming they had to learn a seemingly archaic command line structure to make Linux work). This is no longer the case. With modern desktop Linux, there is no need to ever touch the command line.

5. Graphical Server - this is the sub-system that displays the graphics on your monitor. It is commonly referred to as the X server or just “X”.

6. Desktop Environment - this is the piece of the puzzle that the users actually interact with. There are many desktop environments to choose from

(Unity, GNOME, Cinnamon, Enlightenment, KDE, XFCE, etc). Each desktop environment includes built-in applications (such as file managers, configuration tools, web browsers, games, etc).

7. MINIX (sometimes written as Minix) is a small, open source UNIX clone that was first released in January 1987. It is now best known for its role in inspiring Linus Torvalds to develop Linux.

8. Open source licenses are licenses that comply with the Open Source Definition — in brief, they allow software to be freely used, modified, and shared. To be approved by the Open Source Initiative (also known as the OSI), a license must go through the Open Source Initiative's license review process.

9. Database is a set of data that has a regular structure and that is organized in such a way that a computer can easily find the desired information.

10. Web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients.

11. Malware refers to software programs designed to damage or do other unwanted actions on a computer system. In Spanish, "mal" is a prefix that means "bad", making the term "bad ware", which is a good way to remember it (even if you're not Spanish).

12. The kernel is a program that constitutes the central core of a computer operating system. It has complete control over everything that occurs in the system.

Grammar practice.

Compound Nouns

In English, words, particularly adjectives and nouns, are combined into compound structures in a variety of ways. And once they are formed, they sometimes metamorphose over time. There is only one sure way to know how to spell compounds in English: use an authoritative dictionary.

There are three forms of compound words:

- the closed form, in which the words are melded together, such as firefly, secondhand, softball, childlike, crosstown, redhead, keyboard, makeup, notebook;
- the hyphenated form, such as daughter-in-law, master-at-arms, over-the-counter, six-pack, six-year-old, mass-produced;
- and the open form, such as post office, real estate, middle class, full moon, half sister, attorney general.

Compound noun phrase

It is common to find one noun modifying another: student body, book cover, water commission. But when we create a long string of attributive nouns or modifiers, we create difficulties:

People who author web-pages have become aware of what is now known as the uniform resource locator protocol problem.

The difficulty we have here is knowing what is modifying what. Also, the reader keeps expecting the string to end, so the energy of the sentence (and our attention) dwindles into a series of false endings. Such phrases are a particular temptation in technical writing. Usually, the solution to an over-ly extended compound noun phrase is to start the translation with the last noun.

3. Identify the form of compound words and translate them.

Firewall, web page, web site, network, net news, software, malware, spyware, computer-aided, computer-assisted, computer-generated, computer-literate, computer-mediated, computer-oriented, computer phobia, online chat, online service, mail filter, mail gateway, mail bomb, mailbox, narrow-band, navigation tool.

4. Translate the following compound nouns and compound noun phrases.

Technology: high technology; analog technology; communication technology; compatible technologies; packet communication technology; advanced technology; artificial intelligence technology; well-proven technology.

Data: missed data; asynchronous data; encoded data; input data; raw data; digitized data; data flow; data compression.

Network: asynchronous network; backbone network; baseband network; baseband-switched network; broadband integrated-service digital network; data-computing network; data-transmission network; dial-up network; packet wire-less communication network.

Packet: packet filtering; packet sniffer; packet switching; packet assembly; Packet Switch Node; packet switching network.

Server: access server; client/server architecture (CSA); backup server; client software; load server; database server; dedicated server; staging server, asynchronous-communication server.

5. What do these abbreviations mean? Look up the ones you don't know in a dictionary.

ARPANET, ISP, RTSP, NCP, WAN, VPN, ADSL, PKC, URI, FTP, CSS, SSI, HTTP, XML, VOIP, BBS, FAQ, RSS, UDP, POP, SMTP, DNS, CIDR, SSL.

Unit 3

Text 1

Threat

1. Read the following text and say what new information you have learnt about threats.

Computer system threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Intellectual property is the ownership of property usually consisting of some form of protection. Theft of software is probably the most common in IT businesses today. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile. Cell phones are prone to theft and have also become far more desirable as the amount of data capacity increases. Sabotage usually consists of the destruction of an organization′s website in an attempt to cause loss of confidence to its customers. Information extortion consists of theft of a company′s property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner. There are many ways to help protect yourself from some of these attacks but one of the most functional precautions is user carefulness.

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

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, as well as damage to the company's reputation. Protecting confidential information is a business requirement and in many cases also an ethical and legal requirement. Hence a key concern for organizations today is to derive the optimal information security investment. The renowned Gordon-Loeb Model actually provides a powerful mathematical economic approach for addressing this critical concern.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

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

2. How much do you know about threats? Check your knowledge.

1. The main goal of a cyberattack is to affect one or more IT assets.

A) True.

B) False.

2. Which of the following best describes intellectual property (IP)?

A) The items a business has copyrighted.

B) All patents owned by a business.

C) The unique knowledge a business possesses.

D) The personnel engaged in unique research.

3. Which of the following terms best describes a person with very little skill?

A) Hacker.

B) Script kiddie.

C) Cracker.

D) Wannabe.

4. Which type if attacks result in legitimate users not having access to a system resource?

A) DoS.

B) IPS.

C) Man in the middle.

D) Trojan.

5. A SYN Hood attack floods a target with invalid network packets.

A) True.

B) False.

6. Which type of document defines unacceptable computer behavior?

A) IDS.

B) DoS.

C) AIJP.

D) PII.

7. Which of the following steps can best protect your computer from worms?

A) Installing anti-malware software.

B) Configuring a firewall to block all ports.

C) Encrypting all disks.

D) Enforcing strong passwords for all users.

8. A war dialer is a legacy tool no longer in use.

A) True.

B) False.

9. A dictionary attack is a simple attack that primarily relies on users making poor password choices.

A) True.

B) False.

10. Which type of attack involves capturing data packets from a network and transmitting them later to produce an unauthorized effect?

A) Man in the middle.

B) SYN flood.

C) Replay.

D) Smurf.

11. Which type of malware is a self-contained program that replicates and sends copies of itself to other computers, generally across a network.

A) Virus.

B) Worm.

C) Trojan.

D) Rootkit.

12. Which group is responsible for responding to any reported cyberattack?

A) Emergency response team.

B) IT security department.

C) Disaster response team.

D) Incident response team.

Grammar practice.

1. The infinitive constructions.

In Modern English we distinguish the following predicative constructions with the Infinitive:

1) The Objective-with-the-Infinitive Construction, e.g. we know all data to be translated into binary code before being stored in main storage (subject + verb + object + to-Infinitive).

2) The Subjective-with-the-Infinitive Construction, e.g. they are expected to be the most commonly used devices (subject + verb (usually in Passive Voice) + to-Infinitive)).

3) The For-to-Infinitive Construction, e.g. there is no reason for computer experts to use computers of the first generation nowadays (object + for + noun/pronoun + to-Infinitive).

4) The Absolute Infinitive (it is used only in literary style, It is translated into Russian with the help of a clause with such conjunctions as при этом/причем), e.g. the claims should be forwarded by a registered letter, the text to be written in English. (Subject + to-Infinitive).

2. Translate the sentences and name each Infinitive construction.

1. It is considered to be very good netiquette to share your knowledge and help with others who ask questions by e-mail, in news groups, on mailing lists, and in chat rooms.

2. As a result, network application developers will find it easier to develop and deploy emerging applications for data communication using VoIP.

3. Anytime you visit a web page that includes more than simple HTML content, you are likely to need at least one plug-in.

4. VoIP is said to be cheap, but most people use it for free.

5. The main reason for people to turn massively to this new technology is the cost.

6. If a page seems to be taking a long time to load, don't hesitate to stop the connection and then select the link again.

7. You don't have to wait for a page to load to click a link, press the back button, or select a new link from your bookmarks.

8. Mosaic was the first popular Web browser, the knowledge of the Web to be spread quickly across the world.

Comprehension check.

3. Make up 10 questions according to the text.

4. Give a short summary of the text.

Text 2

Internet security

1. Read the following text and say what new information you have learnt about internet security.

Internet security is a branch of computer security specifically related to not only the Internet, often involving browser security and the World Wide Web, but also network security on as it applies to other applications or operating systems as a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information which leads to a high risk of intrusion or fraud, such as phishing, online viruses, Trojans, worms and more.

Many methods are used to protect the transfer of data, including encryption and from-the-ground-up engineering. The current focus is on prevention as much as on real time protection against well known and new threats.

Threats for internet security:

1) Malicious software.

2) Denial-of-service attacks.

3) Phishing.

4) Application vulnerabilities.

An internet user can be tricked or forced into downloading software onto a computer that is of malicious intent. Such software comes in many forms, such as viruses, Trojan horses, spyware, and worms.

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term bad ware is sometimes used, and applied to both true (malicious) malware and unintentionally harmful software.

A botnet is a network of zombie computers that have been taken over by a robot or bot that performs large-scale malicious acts for the creator of the botnet.

Computer Viruses are programs that can replicate their structures or effects by infecting other files or structures on a computer. The common use of a virus is to take over a computer to steal data.

Computer worms are programs that can replicate themselves throughout a computer network, performing malicious tasks throughout.

Ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.

Scareware is scam software of usually limited or no benefit, containing malicious payloads, that is sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety, or the perception of a threat, generally directed at an unsuspecting user.

Spyware refers to programs that surreptitiously monitor activity on a computer system and report that information to others without the user's consent.

One particular kind of spyware is key logging malware. Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard.

A Trojan horse, commonly known as a Trojan, is a general term for malicious software that pretends to be harmless, so that a user willingly allows it to be downloaded onto the computer.

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Another way of understanding DDoS is seeing it as attacks in cloud computing environment that are growing due to the essential characteristics of cloud computing. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. According to businesses who participated in an international business security survey, 25% of respondents experienced a DoS attack in 2007 and 16.8% experienced one in 2010. DoS attacks often use bots (or a botnet) to carry out the attack.

Phishing is an attack which targets online users for extraction of their sensitive information such as username, password and credit card information. Phishing occurs when the attacker pretends to be a trustworthy entity, either via email or web page. Victims are directed to fake web pages, which are dressed to look legitimate, via spoof emails, instant messenger/social media or other avenues. Often tactics such as email spoofing are used to make emails appear to be from legitimate senders, or long complex subdomains hide the real website host. Insurance group RSA said that phishing accounted for worldwide losses of $10.8 billion in 2016.

Applications used to access Internet resources may contain security vulnerabilities such as memory safety bugs or flawed authentication checks. The most severe of these bugs can give network attackers full control over the computer. Most security applications and suites are incapable of adequate defense against these kinds of attacks.

Internet security products are antivirus, password managers and security suites.

Antivirus software and Internet security programs can protect a programmable device from attack by detecting and eliminating malware; Antivirus software was mainly shareware in the early years of the Internet, but there are now several free security applications on the Internet to choose from for all platforms.

A password manager is a software application that helps a user store and organize passwords. Password managers usually store passwords encrypted, requiring the user to create a master password; a single, ideally very strong password which grants the user access to their entire password database from top to bottom.

2. Learn the following definitions.

The Internet (contraction of interconnected network) is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide.

Internet security is a branch of computer security specifically related to not only the Internet, often involving browser security and the World Wide Web, but also network security on as it applies to other applications or operating systems as a whole.

The World Wide Web (WWW) is a network of online content that is formatted in HTML and accessed via HTTP.

Network security is an over-arching term that describes that the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources.

An operating system (OS) is system software that manages computer hardware and software resources and provides common services for computer programs.

A computer virus is a malicious program that self-replicates by copying itself to another program.

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

A botnet is a network of zombie computers that have been taken over by a robot or bot that performs large-scale malicious acts for the creator of the botnet.

Computer Viruses are programs that can replicate their structures or effects by infecting other files or structures on a computer.

Computer worms are programs that can replicate themselves throughout a computer network, performing malicious tasks throughout.

Ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.

Scareware is scam software of usually limited or no benefit, containing malicious payloads, that is sold to consumers via certain unethical marketing practices.

Spyware refers to programs that surreptitiously monitor activity on a computer system and report that information to others without the user's consent.

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard.

A Trojan horse, commonly known as a Trojan, is a general term for malicious software that pretends to be harmless, so that a user willingly allows it to be downloaded onto the computer.

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.

Phishing is an attack which targets online users for extraction of their sensitive information such as username, password and credit card information.

RSA (Rivets–Shamir–Adelman) is one of the first public-key cryptosystems and is widely used for secure data transmission.

Antivirus software, or anti-virus software (abbreviated to AV software), also known as anti-malware, is a computer program used to prevent, detect, and remove malware.

A password manager is a software application that helps a user store and organize passwords.

Security suite is a collection of software utilities that protect a user's computer from viruses and other malware.

3. Answer the following questions:
1) What is Internet security and why is it so important?
2) What methods are used to protect data transmission?
3) What kind of threats are existed in the Internet security?
4) What can harm malware?
5) What is the difference between computer viruses and computer worms?
6) How does Trojan harm your computer?
7) How can you protect your computer?

Grammar practice.

The gerund

The -ing form is used:
1) As a noun.
Browsing the web can be very exciting.

2) After love, like, dislike, hate, enjoy. I love surfing the Net.

3) After certain verbs (avoid, admit, confess to, deny, look forward to, mind, object to, prefer, regret, risk, spend, suggest, give up, approve of, depend on, complain of, thank for, insist on, rely on, etc.) I don't mind installing new software.

4) After expressions: to be busy with, to be used to, to be proud of, to be worth (while), it's no use, there's no point (in), to be sure of, to be surprised at, etc.

Any Windows, Macintosh, or Unix computer is capable of running a web server when it is connected to the Internet.

5) After prepositions.

You can multiply your surfing fun by browsing more than one web page at the same time.

4. Fill in the right form of the verb given. Use Gerund, to + Infinitive or bare Infinitive.

1. Once the malware appears on your machine, it can be very challenging ________ (get) rid of. Access to the contents of the mailbox is granted by entering in your password.

2. With VoIP you can speak to someone while ________ (send) her files or even showing yourself using a web cam.

3. I'm tired of pop-up web advertisements, they just keep ___________ (appear) Employees who are about ____________ (lose) their jobs can sometimes leave malware behind on the company system to do damage to their former employer.

4. The primary purpose of the firewall is __________ (prevent) unauthorized users from gaining access to your web server through packet filtering, user authentication, address obfuscation, along with client and server access lists.

5. You can't block pop-up ads by ________ (turn) off a feature or service in the operating system.

6. Regular Internet users with an eye to privacy may succeed in ___________ (achieve) a desirable level of privacy through careful disclosure of personal information and by avoiding spyware.

7. The Internet is the most robust communications network ever designed, able_________ (adapt) itself almost instantaneously to damage or outages to individual sections.

8. Meta-search engines allow you _____________ (submit) a search query to several engines at once.

9. Many phishing scams actually take real URL's and change them ever so slightly to make them _________ (look) like the real ones.

Comprehension check.

5. Give short summary of the text.

Unit 4

Text 1

Security controls

1. Read the following text and say what new information you have learnt about security controls.

Selecting proper controls and implementing those will initially help an organization to bring down risk to acceptable levels. Control selection should follow and should be based on the risk assessment. Controls can vary in nature but fundamentally they are ways of protecting the confidentiality, integrity or availability of information. ISO/IEC 27001:2005 has defined 133 controls in different areas, but this is not exhaustive. Organizations can implement additional controls according to requirement of the organization. ISO 27001:2013 has cut down the number of controls to 113.

Administrative.

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day-to-day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed – the Payment Card Industry Data Security Standard (PCI DSS) required by Visa and MasterCard is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. Administrative controls are of paramount importance.

Logical.

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host-based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls.

An important logical control that is frequently overlooked is the principle of least privilege. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read email and surf the web. Violations of this principle can also occur when an individual collects additional access privileges over time. This happens when employees' job duties change, or they are promoted to a new position, or they transfer to another department. The access privileges required by their new duties are frequently added onto their already existing access privileges which may no longer be necessary or appropriate.

2. How much do you know access controls? Check your knowledge.

1. Access controls are policies or procedures used to control access to certain items.

A) True.

B) False.

2. Which answer best describes the authorization component of access control?

A) Authorization is the method a subject uses to request access to a system.

B) Authorization is the process of creating and maintaining the policies and procedures necessary to ensure proper information is available when an organization is audited.

C) Authorization is the validation or proof that the subject requesting access is indeed the same subject who has been granted that access.

D) Authorization is the process of determining who is approved for access and what resources they are approved for.

3. Which answer best describes the identification component of access control?

A) Identification is the validation or proof that the subject requesting access is indeed the same subject who has been granted that access.

B) Identification is the method a subject uses to request access to a system.

C) Identification is the process of determining who is approved for access and what resources they are approved for.

D) Identification is the process of creating and maintaining the policies and procedures necessary to ensure proper information is available when an organization is audited.

4. Which answer best describes the authentication component of access control?

A) Authentication is the validation or proof that the subject requesting access is indeed the same subject who has been granted that access.

B) Authentication is the process of creating and maintaining the policies and procedures necessary to ensure proper information is available when an organization is audited.

C) Authentication is the process of determining who is approved for access and what resources they are approved for.

D) Authentication is the method a subject uses to request access to a system.

5. Which answer best describes the accountability component of access control?

A) Accountability is the validation or proof that the subject requesting access is indeed the same subject who has been granted that access.

B) Accountability is the method a subject uses to request access to a system.

C) Accountability is the process of creating and maintaining the policies and procedures necessary to ensure proper information is available when an organization is audited.

D) Accountability is the process of determining who is approved for access and what resources they are approved for.

6. Physical access controls deter physical access to resources, such as buildings or gated parking lots.

A) True.

B) False.

7. When you log on to a network, you are presented with some combination of username, password, token, smart card, or biometrics. You are then authorized or denied access by the system. This is an example of________.

A) Physical access controls.

B) Logical access controls.

C) Group membership policy.

D) The Biba Integrity Model.

E) None of the above.

8. Access controls cannot be implemented in various forms, restriction levels, and at different levels within the computing environment.

A) True.

B) False.

9. Which of the following is an example of a formal model of access control?

A) Discretionary access control (DAC).

B) Mandatory access control (MAC).

C) Non-discretionary access control.

D) The Clark and Wilson Integrity Model.

E) All of the above

10. Physical access, security bypass, and eavesdropping are examples of how access controls can be_______ .

A) Stolen.

B) Compromised.

C) Audited.

D) Authorized.

11. Challenges to access control include which of the following?

A) Laptop loss.

B) Exploiting hardware.

C) Eavesdropping.

D) Exploiting applications.

E) All of the above.

12. When the owner of the resource determines the access and changes permissions as needed, it's known as_______ .

A) Mandatory access control (MAC).

B) Discretionary access control (DAC).

C) Non-discretionary access control.

D) Content-dependent access control.

E) Role based access control.

13. The process of identifying, quantifying, and prioritizing the vulnerabilities in a system is known as a_______ .

A) Vulnerability policy.

B) Vulnerability deterrent.

C) Vulnerability authorization.

D) Vulnerability assessment.

14. The security kernel enforces access control of computer systems.

A) True.

B) False.

15. When it comes to privacy, organizations are concerned about which of the following?

A) Liability in harassment suits.

B) Skyrocketing losses from employee theft.

C) Productivity losses from employees shopping or performing other non-work-related tasks online.

D) All of the above.

Comprehension check.

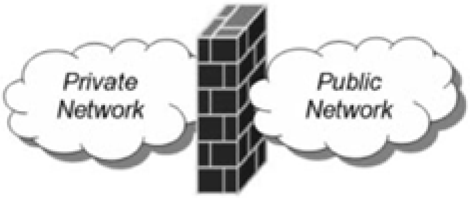
3. Make up 10 questions according to the text

4. Give a short summary of the text.

Text 2

Firewalls

1. Read the following text and say what new information you have learnt about firewalls.



As traffic increases dramatically on the Internet, so, too, do the risks that an institution's data may be sabotaged or stolen. As a result, network firewalls have become a hot topic. Relatively new creations, Internet firewalls, barriers placed between a network and the outside world to prevent potentially damaging intrusion, have their roots in control mechanisms and security measures that have long been standard practice in the main-frame community. But today's networked world has grown from the bottom up rather than from the top down, with millions of new connections originating from personal computers and small networks. It's no longer possible to know who or what is on the other end of a network connection unless extraordinary measures are taken.

Just as no physical fire wall is perfect protection against a fire, no digital firewall can make a network 100 percent secure against outside intrusion. But they can come remarkably close if there is a comprehensive security policy. Firewalls can be built in several ways, using a variety of mechanisms. The most common are:

1) Router-based filters.

2) Host computer gateways', or bastions.

3) A separate, isolation network. The cost of a firewall can range from a SI 00,000 turnkey (installed and maintained by an outside vendor,) hardware/software system, to do it yourself software.

Perhaps the simplest approach to creating a firewall involves using a programmable router – the type of device normally used to create a permanent Internet connection to the outside world. Routers work by controlling traffic at the IP, i. e., the Internet Provider level, selectively passing or blocking data packets based on source/destination address or port information. While reasonably good firewalls can be created with routers alone, it may prove difficult to program the router to exclude everything that you want kept out. Unfortunately, most routers come configured with a minimum of built-in protection, and many organizations simply install them this way without customizing them.

Another approach to firewall construction is to use a computer rather than a router. This system, also called a bastion host, offers many more capabilities, including the ability to log all the activity over the gateway. While a router-based firewall monitors data packets at the IP level, hosts exert their control at an application level, where traffic can be examined more thoroughly. However, host-based firewalls must use specialized software applications gateways and service proxies to plug existing security holes. These are, in essence, stripped down versions of the original programs; they are less flexible and pass along mail messages only after verifying that they fit within the programmed restriction.

A third way to establish a firewall, similar to the host-based systems just described, is to create another network, i.e., an isolated subnetwork that sits be-tween the external and internal networks. Typically, this network is configured so that both the Internet and the private network can access it, but traffic across the isolation network is blocked.

Sometimes, simply foiling an outside attack isn't enough. One high-powered deterrent is Sidewinder, a complete turnkey firewall system advertised as "security that strikes back." Its operating system is secure in and of itself, requiring no proxies or gateway applications. The patented mechanism wherein the operating system and its applications stay secure is called Type Enforcement. Data and processes are assigned to class types and interaction between them is strictly regulated.

It provides defense in depth, that is, even if a determined hacker were able to break into the Sidewinder platform itself, he or she would be left stranded in one domain without access to any other applications or processes. And breaking in is made more difficult because Sidewinder can filter any data that passes the network boundary. One of Sidewinder's most interesting features is that it can strike back. When Sidewinder detects a hacker, it immediately sends a silent alarm to the system administrator for a decision. The system can let the intruder in and permit certain activities up to a point, all the while collecting information on the source of the probe and what types of actions the hacker takes. The system can also provide dummy password files, dead-end traps, and other stealthy defenses - a veritable "hall of mirrors", where nothing is quite the way it appears. More-over, Sidewinder can also force a disconnection from any outside network.

2. Decide whether the statements below are True or False according to the text, justify your decision by quoting the relevant words from the text.

1. Internet firewalls are derived from the mainframe procedures.

2. Most of the router-based filters are adjusted to the needs of the customers using them.

3. Host-based firewalls offer more reliable verification of the message traffic than that given at IP level.

4. Service proxies are more limited in function than the original programs.

5. Sidewinder can filter both incoming and outgoing messages.

6. Sidewinder is described as a complete turnkey firewall system because it provides multi-level reaction, a retaliatory capacity and built-in traffic con-trol.

7. Sidewinder strikes back by isolating the hacker before he accesses network domains.

3. Basing on the information from the text, write grammatically correct one-sentence definitions for TWO of the following terms.

Firewall Type Enforcement Isolation Network Sidewinder

1. ____
____
____

2. ____
____
____

4. Complete the following sentences using the logical connectors given below. There are 2 extra words.

while ● similarly ● so	●	i.e. ● possibly
despite ● therefore	●	because

The walls of medieval cities were useless unless they had gateways 1) __________, private computer networks have gateways to the outside world. Firewalls, 2) _______________ sets of computers using filters to allow only authorized messages to pass through, are used as fortified gateways. Large systems with complex firewalls use an inner and outer gateway. The "outside" gateway connected to the Internet, can only reach one machine inside the fire-wall, 3) ________________ the "inside" gateway doesn't trust the outside one, and 4) __________________ only provides it with certain limited services. 5) _______________ messages from outside in such a system may pass first to a firewall router, it takes no messages itself, and 6) _______________ cannot be compromised.

4. What do these abbreviations mean? Look up the ones you don't know in a dictionary.

BPD, SOAP, ADN, Ajax, FDDI, JPEG, REST, SAML, RTSP, SEO, SMDS, SNMP, SQL, TLD, WAIS, UDDI, DHCP, NIC.

Unit 5

Text 1

What is Trojan?

1. Read the following text and say what new information you have learnt about Trojans.

A Trojan (also known as a Trojan, a Trojan horse) is a type of malware that penetrates into a computer under the guise of legal software, unlike viruses and worms that spread spontaneously. This category includes programs that perform various non-user actions: collecting information from it Bank cards. and its transfer to an attacker, its use, deletion or malicious modification, disruption of computer performance, the use of computer resources for mining purposes, the use of IP for illegal trade. Examples of Trojans: Hook Dump, Back Orifice, Pinch, TDL-4, Trojan. Winlock.

Trojans are distributed by people — both directly loaded into computer systems by malicious insiders, and encourage users to download and/or run them on their systems.

To achieve the latter, Trojan horses are placed by attackers on open or indexed resources (file servers and file-sharing systems), information carriers are sent via messaging services (for example, e-mail), get to the computer through security breaches or are downloaded by the user from addresses obtained in one of the listed ways. Sometimes the use of Trojans is only part of a planned multi-stage attack on certain computers, networks or resources (including third-party) Trojans are most often developed for malicious purposes. There is a classification where they are broken down into categories based on how Trojans infiltrate and harm the system. There are 5 main types:

- data destruction;
- loader;
- server;
- security program deactivator.

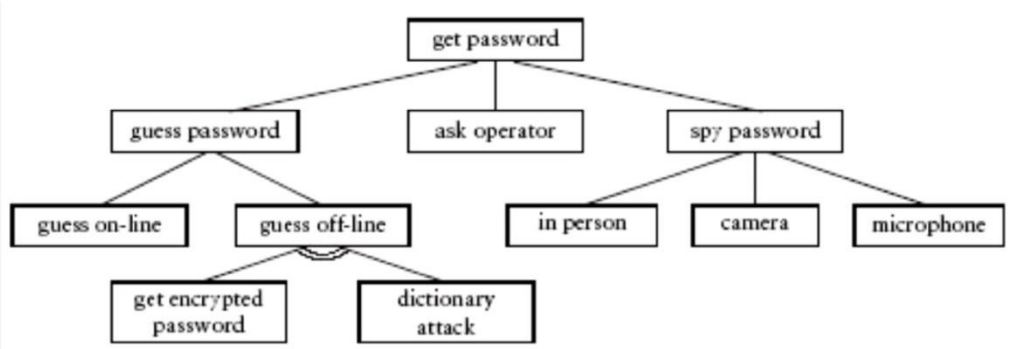
Trojans usually have the following extensions:

- .exe, .com (under the guise of games, office applications and other legal programs, the extension may not be visible if Windows is disabled display extensions, possible files with a "double" extension, for example, image.jpg.exe);
- .js, .vbs, .jse, .vbe, .bat, .cmd, .sh (scripts; extension may not be visible, sometimes files of these formats can be read in the code editor);
- .html, .htm, .shtml, .shtm, .xhtml, .xht, .hta (HTML documents; can download viruses and other malicious programs from the Internet, redirect to virus and false sites; files .hta works outside the browser and can perform dangerous actions directly on the computer);
- .pif (shortcut with the ability to perform malicious actions);
- .docm, .xlsm, etc. (in electronic documents can be dangerous macros, usually the extension ends with "m»);
- .xml, .xsl, .svg, .xaml (XML documents, similar to HTML);
- .(scr, often secretly);
- some others.

Comprehension check.

2. Look at the attack tree and describe the process of obtaining another user’s password.

Attak tree



3. Make up 10 questions according to the text.

4. Give short summary of the text.

Text 2

History of Trojan

1. Read the following text and say what new information you have learnt about history of Trojan.

One of the earliest Trojan horse viruses was detected in the 1980s, when several computers were affected. As it was earlier mentioned Trojan horse viruses are created in order to steal useful information such as passwords. They are developed by hackers, who, after stealing data, can use the information for various purposes, including blackmailing. Some of the first Trojan horse viruses were able to infect Windows32 files, but since then these programs evolved, and today they can cause even more harm.

The name of the Trojan horse comes from a story from Greek mythology about the siege of Troy. Greeks were unable to conquer the city until they built a huge wooden Trojan horse and hid a number of warriors in it. The wooden horse was supposed to be a present from the Greeks, informing that they sailed away and no longer wanted to conquer the city. When the Trojan horse was pulled into the city, the small army of Greeks inside it waited till dark and then invaded the Troy, destroying it, thus leading to the end of the war. In contrast to the wooden Trojan horse, the Trojan horse virus spread worldwide and is still popular today.

According to some online sources the first Trojan horse virus was dubbed the pest trap, also known as Spy Sheriff. This Trojan horse managed to infect about one million PCs worldwide. It did not damage any files on a computer, instead it led to the appearance of a large number of pop-ups, most of them looking like warnings that warned users about the necessity to installs some kind of software application. As soon as the Trojan horse computer virus was installed on the machine, it was quite difficult to get rid of it. In case the user tried to erase it, the Trojan horse would simply reinstall itself from hidden affected data files on the computer.

During the 1980s there was an increase of the Bulletin Board System, which was computer system running software that permitted users to penetrate the system through a phone line. The BBS contributed to a fast spread of Trojan horse viruses, because after users logged in, they carried out such functions as uploading and downloading software and data sharing (some of which was infected). At that time computer viruses were created to aim popular software traders.

2. Learn the following definitions by heart.

1. A Trojan horse - a type of malware that enters a computer under the guise of legitimate software, unlike viruses and worms that spread spontaneously.

2. IP - is a routed TCP/IP stack network layer Protocol. It was IP that became the Protocol that United individual computer networks into the world wide web. Network addressing is an integral part of the Protocol.

3. HookDump is a Keylogger that was used both as a user action control system and as a spy program. The peak of popularity came in the late 1990s.

4. Back Orifice - Trojan remote administration program created by a well-known group of hackers "the Cult of the dead cow" (eng.) in 1998. The program is

intended to remote control the computer with operating system Windows 95/Windows 98.

5. A file server - a dedicated server that performs file I / o operations and stores files of any type. Typically, it has a large amount of disk space, implemented in the form of a RAID-array to ensure smooth operation and increased speed of writing and reading data.

6. File name extension - a sequence of characters added to a file name and intended to identify the type (format) of the file. This is one of the common ways that a user or computer software can determine the type of data stored in a file, for example: name.jpg is the pictures, the name.avi video, etc.

7. Windows - a family of Microsoft's commercial operating systems (OC) that are focused on graphical management. Initially, Windows was just a graphical add-on program over the MS-DOS operating system common in the 80s and 90s.

8. XML - an extensible markup language. Recommended by the world wide web Consortium. The XML specification describes XML documents and partially describes the behavior of XML processors.

9. HTML – Hyper Text Markup Language (hypertext Markup language) is a standardized markup language for documents on the world wide web.

10. FTP - File Transfer Protocol — a Protocol for transferring files over the network. Unlike TFTP, which guarantees the transfer (or issuance of an error) through the use of quitasueno (CH. acknowledge; acknowledgement of transfer and acceptance of structural units of information) of TCP. The standard port for the FTP control connection is 21. A typical use of FTP is to download sites and other documents from a private development device to public hosting servers.

Comprehension check.

3. Make up 10 questions according to the text.

4. Give short summary of the text.

Unit 6

Text 1

Computer security vulnerabilities

1. Read the following text and say what new information you have learnt about computer vulnerabilities.

In computer security, the word vulnerability refers to a weakness in a system allowing an attacker to violate the confidentiality, integrity, availability, access control, consistency or audit mechanisms of the system or the data and applications it hosts. Vulnerabilities may result from bugs or design flaws in the system. A vulnerability can exist either only in theory, or could have a known exploit. Vulnerabilities often result from the carelessness of a programmer, though they may have other causes. Some vulnerabilities arise from un-sanitized user input, often allowing the direct execution of commands or SQL statements (known as SQL injection). Others arise from the programmer's failure to check the size of data buffers, which can then be overflowed, causing corruption of the stack or heap areas of memory (including causing the computer to execute code provided by the attacker). A vulnerability may allow an attacker to misuse an application through bypassing access control checks or executing commands on the system hosting the application.

Vulnerabilities have been found in every major operating system including Windows, Mac OS, various forms of Unix and Linux, OpenVMS, and others. The only way to reduce the chance of a vulnerability being used against a sys-tem is through constant vigilance, including careful system maintenance and best practices in deployment (e. g. the use of firewalls and access controls).

2. Decide whether the statements below are true or false.

1. All vulnerabilities are results of programmers' mistakes.
2. Any vulnerability has the corresponding exploit.
3. Even expensive operating systems have vulnerabilities.
4. Using firewall can prevent your system from being damaged by using vulnerabilities.
5. Not checking size of user input cannot result in execution of malicious code.
6. Discuss the following topic: what should a programmer do in order to write a program without vulnerabilities?
7. What are pros and cons of two methods of disclosing vulnerabilities:

a) full disclosure (to disclose all the details of a security problem which are known);

b) limiting disclosure to the users placed at greatest risk, and only releasing full details after a delay.

4. From the verbs below make nouns by adding the appropriate suffixes. Translate the nouns.

-er, -or.

To control, to compute, to design, to use, to spam, to manufacture, to simulate, to operate, to route, to protect, to process, to deal, to perform, to crack, to program, to execute, to transmit, to lame, to convert, to crawl, to consume, to hack.

-tion, -sion.

To organize, to connect, to combine, to apply, to represent, to encrypt, to corpo-rate, to transact, to extend, to execute, to protect, to substitute, to communicate, to compress, to inform, authenticate.

-ment.

To require, to measure, to equip, to invest, to accomplish, to improve, to develop, to achieve, to displace, to govern, to establish, to replace, to attach.

Text 2

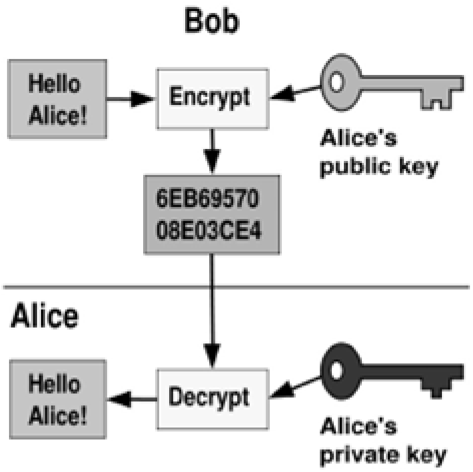
Public key cryptography

1. Read the following text and say what new information you have learnt about cryptography.

The role of cryptography is very important in the design of electronic payment systems. The cryptographic mechanisms include public-key cryptography, one-way hash functions, challenge-response cryptographic protocols, digital signatures and key management protocols.

Public key cryptography, also known as asymmetric cryptography, is a form of cryptography in which a user has a pair of cryptographic keys – a public key and a private key. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key can-not be practically derived from the public key.

A message encrypted with the public key can be decrypted only with the corresponding private key, and a message encrypted with the private key can only be decrypted using the public key. An analogy for public-key encryption is that of a locked mailbox with a mail slot. The mail slot is exposed and accessible to the public; its location is in essence the public key. Anyone knowing the street address can go to the door and drop a written message through the slot; however, only the person who possesses the key can open the mailbox and read the message.



2. Decide whether the statements below are true or false.

1. One should keep his public key in a secret place.
2. Several private keys can be associated with public key.
3. Several public keys can be associated with private key.
4. It is easy to create a private key with the corresponding public key.
5. It is easy to create a public key with the corresponding private key.
6. It is possible to decrypt a message with public key, that was used for encrypting this message.

3. Write the sequence of actions from the list below for the following task: send message that can be read only by the receiver (some actions are not used).

A) The message is transferred from the sender to the receiver.
B) The sender encrypts the message with the receiver's public key.
C) The receiver gets the sender's public key.
D) The receiver decrypts the message with his/her private key.
E) The receiver decrypts the message with sender's public key.

F) The sender gets the receiver's public key.

4. Write the sequence of actions from the list below for the following task: the receiver should be sure that the message was written by the sender and no one changed or faked it (some actions are not used).

A) The message is transferred from the sender to the receiver.
B) The sender gets the receiver's public key.
C) The receiver decrypts the message with the sender’s public key.
D) The sender encrypts the message with his/her private key.
E) The receiver gets the sender’s public key.
F) The sender encrypts the message with the receiver's public key.

4. Give a short summary of the text.

Unit 7

Text 1

Secure HTTP

1. Read the following text and say what new information you have learnt about secure HTTP.

HTTPS is a URI scheme used to indicate a secure HTTP connection. It is syntactically identical to the http:// scheme normally used for accessing resources using HTTP. Using an https://URL indicates that HTTP is to be used, but with a different default TCP port (443) and an additional encryption/authentication layer between the HTTP and TCP. This system was designed by Netscape Communications Corporation to provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

Strictly speaking, HTTPS is not a separate protocol, but refers to a normal HTTP interaction over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) transport mechanism. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided it is properly implemented and the top level certification authorities do their job.

To prepare a web-server for accepting HTTPS connections the administrator must create a public key certificate for the web-server. This certificate must be signed by a certificate authority of one form or another, who certifies that the certificate holder is who they say they are. Web browsers are generally distributed with the signing certificates of major certificate authorities, so that they can verify certificates signed by them.

Organizations may also run their own certificate authority, particularly if they are responsible for setting up browsers to access their own sites, as they can trivially add their own signing certificate to the defaults shipped with the browser.

Some sites use self-signed certificates. Using these provides protection against pure eavesdropping but unless the certificate is verified by some other method and that other method is secure, there is a risk of a man-in-the-middle attack.

The system can also be used for client authentication, in order to restrict access to a web server to only authorized users. For this, typically the site administrator creates certificates for each user which are loaded into their browser, although certificates signed by any certificate authority the server trusts should work. These normally contain the name and e-mail of the authorized user, and are automatically checked by the server on each reconnect to verify the user's identity, potentially without ever entering a password.

2. Read the text once more and answer the following questions.

1. Why it is dangerous to use pure HTTP for transferring security-sensitive information?

2. What are two main functions of HTTPS?

3. What is the difference between eavesdropping and man-in-the-middle attack?

4. What is disadvantage of using self-signed certificates?

5. What should be done in order users be able to access their personal information on the web server without entering passwords?

3. Imagine situation when someone comes to the bank in order to get some money. Perform the following tasks according to this situation.

1. Describe the mechanism of authentication.

2. Describe the mechanism of authorization.

3. Describe the situation when authentication is passed but authorization is failed.

4. Describe the situation when authentication is failed but authorization is passed.

4. Match the terms with their definitions.

1. Catalogue	a) a network in which some of the parts are connected using the public Internet, but the data sent across the Internet is encrypted
2. Fulfilment	b) the process of validating card details to process a transaction
3. Fraud	c) debit card that uses the visa system
4. Settlement period	d) the software package that is used to run and maintain the standard web e-commerce enabled product catalogue

5. Authorisation	e) the three digit number that is printed on the back of a card that is used for extra confirmation that the card user has the original card
6. Virtual Private Network (VPN)	f) the final stage of a purchasing transaction where the goods are delivered to the customer
7. Mobile commerce	g) an open technical standard for the commerce in dustry developed by Visa and MasterCard as a way to facilitate secure payment card transactions over the Internet
8. Card Verification Code (CVC)	h) software that allows easy update and maintenance of a range of products in an e-commerce site
9. Visa Electron	i) the time taken from the moment a transaction is completed to the point where the funds are avail able to the merchant
10. Secure Electronic Transaction (SET	j) a term coined to refer to generically to transactions that are made or facilitated using mobile de - vices
11. Shopping cart	k) a process of deliberately deception to gain goods or services, in the case of credit cards, this might be through the use of a stolen card number

5. Read the text and decide which word best fits each space.

Digital signature

A digital signature is different from a handwritten one. It is unique and different every time it is (1)___________, and is related to the thing or things it is signing (an electronic document, picture, program and so on). It is created by doing a mathematical calculation on the thing that is being signed that produces a unique numerical (2)__________. That value is (3)___________ using a private cryptographic key and the result linked to the things that were signed. So to make a digital signature you have to generate or buy a private cryptographic key and a (4)_________ public key and certificate.

There are basically two kinds of cryptography in use. Secret key (symmetric), and public/private key (asymmetric). With secret key, the same key is used to encrypt information and decrypt information. (5)__________ the operation is symmetric. With public/private key, the two keys are of different values. Encryption is done using one of them, and (6)___________ can then only be done using the other. Hence the operation is asymmetric. You can give your (7)____________ key to everyone. Then, if they want to send something to you they encrypt it with your public key and they know that only you can (8)___________ it. By the same terms, if you encrypt something using your private key, then anyone who has your public key can check to see if they can (9)___________ it, and if they can, they know it must have come from you.

1) A. Proposed. B. Requested. C. Generated. D. Uploaded.

2) A. Value. B. Answer. C. Key. D. Message.
3) A. Increased. B. Checked. C. Encrypted. D. Decrypted.
4) A. Signed. B. Verified. C. Separate. D. Corresponding.
5) A. But. B. Hence. C. Then. D. Nevertheless.
6) A. Decryption. B. Checking. C. Transferring. D. Signing.
7) A. Symmetric. B. Signing. C. Private. D. Public.
8) A. See. B. Read. C. Receive. D. Encrypt.
9) A. Encrypt. B. Decrypt. C. Generate. D. Read.

Glossary

ADSL – an acronym for Asymmetric Digital Subscriber Line, ADSL is a method of transmitting data over traditional copper telephone lines at speeds higher than were previously possible.

Applet – an applet is a small software application, typically in the Java programming language.

Archie – is a software utility for finding files stored on FTP servers, Archie is a system for locating files on the Internet.

ARPANET – Advanced Research Projects Agency Network. It was a network developed in the late 1960’s and early 1970’s by the U.S. Department of Defense. As an experiment in wide area networking (WAN), ARPANet was developed with the goal of being robust enough to sur-vive a nuclear war.

Backbone – is a high-speed line or series of connections that forms a major pathway within a network.

Bandwidth – is the maximum amount of data that can travel a communications path in a given time, usually measured in seconds.

BBS – this is the acronym for Bulletin Board System, a system that lets people read each other's messages and post new ones.

Blog – short for web log; usually a chronological record of thoughts, links, events, or actions posted on the web. For examples, see the Yahoo Directory of Weblogs.

Broadband – When the bandwidth of a signal is large, it can simultaneously carry many channels of information. Fiber optic cable, in particular, has a very high bandwidth, and is referred to as broadband.

Browser – a browser is a software program that allows you to view and interact with various kinds of Internet resources available on the World Wide Web. A browser is commonly called a web browser.

Client – a client is a program that uses the services of another program. The client program is used to contact and obtain data or request a service from the server.

Cookie – a cookie is a file sent to a web browser by a web server that is used to record one's activities on a website. For instance, when you buy items from a site and place them in a so-called virtual shopping cart, that in-formation is stored in the cookie.

Cryptography – the process of securing private information that is passed through public networks by mathematically scrambling (encrypting) it in a way that makes it unreadable to anyone except the person or per-sons holding the mathematical "key" that can unscramble (decrypt) it.

CSS – stands for Cascading Style Sheets. It is a technique built into version 4.0 and later browsers that support styles for pages. For example, you can set up styles for fonts and page layouts that will apply automatically to pages developed under a particular style you develop.

Database – a database is a structured format for organizing and maintaining information that can be easily retrieved. A simple example of a data-base is a table or a spreadsheet.

Directory – a directory is a system that your computer uses to organize files on the basis of specific information. Directories can be organized hierarchically so that files appear in a number of different ways, such as the order in which they were created, alphabetically by name or by type, and other ways.

Encryption – a way of coding the information in a file or e-mail message so that if it is intercepted by a third party as it travels over a network it cannot be read. Only the person or persons that have the right type of decoding software can unscramble the message.

Firewall – a firewall is a combination hardware and software buffer that many companies or organizations have in place between their internal net-works and the Internet. A firewall allows only specific kinds of messages from the Internet to flow in and out of the internal network.

Gateway – a gateway refers to hardware or software that bridges the gap between two otherwise incompatible applications or networks so that da-ta can be transferred among different computers.

Gopher – is a text-based internet search engine developed by the University of Minnesota.

Host – a host is any computer directly connected to a network that acts as a repository for services (such as e-mail, Usenet newsgroups, FTP, or World Wide Web) available for other computers on the network.

Internet Service Provider – also called an ISP or access providers, Internet service providers refers to the remote computer system to which you connect your personal computer and through which you connect to the Internet.

IP Address – an IP address is a numeric code that uniquely identifies a particular computer on the Internet. Just as a street address identifies the location of your home or office, every computer or network on the Internet has a unique address, too. Internet addresses are assigned to you by an organization called InterNIC.

Java – is an object-oriented programming language developed by Sun Microsystems, Inc. to create executable content (i.e, self-running applications) that can be easily distributed through networks like the Internet.

MIME – stands for Multipurpose Internet Mail Extension, a standard system for identifying the type of data contained in a file based on its extension. MIME is an Internet protocol that allows you to send binary files across the Internet as attachments to e-mail messages.

Netiquette – is a form of online etiquette – an informal code of conduct that governs what is generally considered to be the acceptable way for users to interact with one another online.

Netscape – was founded in 1994 by Jim Clark and Mark Andreessen, Netscape developed the first commercially successful web browser, Netscape Navigator. The browser, based on the Mosaic software from the National Center for Supercomputing, helped fuel the explosive growth of the World Wide Web.

Network – a network is two or more computers connected to each other so they can share resources. The Internet is a "network of networks", whereby anyone – from an individual at a home with a PC to a large corporate multidepartment system – can freely and easily exchange information.

Newsgroup – a newsgroup is an electronic discussion group consisting of col-lections of related postings (also called articles) on a particular topic that are posted to a news server which then distributes them to other participating servers.

Packet/Packet Switching – a packet is a chunk of information sent over a net-work. Packet-switching is the process by which a carrier breaks up da-ta into these chunks or packets. Each packet contains the address of origin, the address of its destination, and information about how to re-unite with other related packets.

Plug-In – a plug-in extends the capabilities of a web browser, such as Netscape Navigator or Microsoft Internet Explorer, allowing the browser to run multimedia files.

POP Server – a POP server uses the Post Office Protocol, to hold users' incoming e-mail until they read or download it.

PPP – An acronym for Point-to-Point Protocol, PPP is a communications protocol used to transmit network data over telephone lines. It allows you to connect your computer to the Internet itself, rather than logging on through an Internet service provider's host computer and using UNIX commands through a shell.

Router – a router is a piece of hardware or software that connects two or more networks. A router functions as a sorter and interpreter as it looks at addresses and passes bits of information to their proper destinations.

Search Engine – a search engine is a type of software that creates indexes of databases or Internet sites based on the titles of files, keywords, or the full text of files. The search engine has an interface that allows you to type what you're looking for into a blank field. It then gives you a list of the results of the search.

Server – server is a computer that handles requests for data, e-mail, file transfers, and other network services from other computers (i.e., clients).

SMTP – an acronym for Simple Mail Transfer Protocol, SMTP is the protocol used for routing e-mail across the Internet.

SQL – an acronym for Structured Query Language. A specialized language for sending queries to databases. Most industrial-strength and many smaller database applications can be addressed using SQL.

SSL – an acronym for Secure Socket Layer, SSL is a protocol developed by Netscape Communications Corporation for securing data transmission in commercial transactions on the Internet. Using public-key cryptography, SSL provides server authentication, data encryption, and data integrity for client/server communications.

String/Search String – a string refers to a sequence of characters, words, or other elements that are connected to each other in some way. A search string usually refers to a string of words or a phrase that is used to search and locate or retrieve a specific piece of information contained in a database or a set of documents.

Tags – are descriptive formatting codes used in HTML documents that instruct a web browser how to display text and graphics on a web page. For example, to make text bold, the tag <B> is used at the beginning and end of the text.

TCP/IP – stands for Transmission Control Protocol/Internet Protocol, the language governing communications between all computers on the Internet. TCP/IP is a set of instructions that dictates how packets of information are sent across multiple networks.

USENET – refers to the collection of newsgroups (sometimes called the Big Eight hierarchies) and a set of agreed-upon rules for distributing and maintaining them.

URL – an acronym for Uniform Resource Locator, a URL is the address for a resource or site (usually a directory or file) on the World Wide Web and the convention that web browsers use for locating files and other remote services.

WAIS – an acronym for Wide Area Information Servers, WAIS is a network information retrieval service that you can use to search for keywords or phrases in specially indexed files.

WAN – an acronym for Wide Area Network, WAN refers to a network that connects computers over long distances via telephone lines or satellite links. In a WAN, the computers are physically and sometimes geographically far apart.

References

1 Charlton M. A Handbook of Information Technology. – Delhi: Global Media, 2009. – 395 p.

2 Computer world: Учебное пособие для студентов дневного отделения ФИСТ / сост. Т.А. Матросова. – Ульяновск: УлГТУ, 2007. − 118 с.

3 Demetriades D. Information Technology Workshop. – Oxford: Oxford University Press, 2003. – 29 p.

4 Evans V. Career Paths English: Information Technology / V. Evans,J. Dooley, S. Wright. – Newbury: Express Publishing, 2011. – 80 p.

5 Henderson H. Encyclopedia of Computer Science and Technology. – New York, 2009. – 580 p.

6 Internet Economics / edited by Lee W. McKnight, Joseph P. Bailey. – Massachusetts: Massachusetts Institute of Technology, 2000. – 511 p.

7 Joe Harris. Cisco Network Security Little Black Book. Cisco Press, 2002. – 293 p.

8 Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. - М.: Кудиц-образ, 2001. - 368 с.

9 English grammar in use. Murphy, R. Cambridge university Press, 2004.

10 Michael E. Whitman, Herbert J. Matto. Principles of Information Security. 2011. - 598 p.

11 William Stallings. Cryptography and Network Security: Principles and Practice, 2011. - 744 p.

12 David Kim and Michel G. Solomon “Fundamental of information Systems Security” copy right 2012 by Jones Bartlett learning L.L.C.

13 Edited by Christos Kalloniatis “Security Enhanced Applications for Information Systems”. Published by InTech 2012.

14 Таненбаум Э. Компьютерные сети. – СПб: Питер, 2003. - 992 с.

15 V.N. Vichugov, T.I. Krasnova “English for internet technologies”. - Tomsk, 2012.