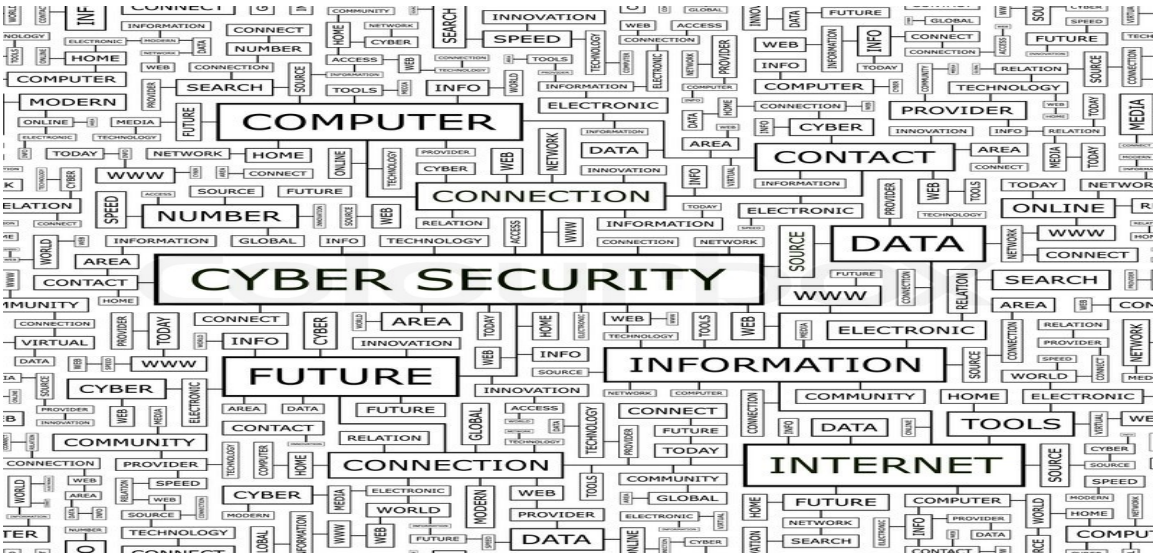
УНИВЕРСИТЕТ ИТМО

А.С. Сомко
Е.А. Федорова

ПРОФЕССИОНАЛЬНЫЙ ИНОСТРАННЫЙ ЯЗЫК ДЛЯ СПЕЦИАЛИСТОВ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ



Санкт-Петербург
2016

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

А.С. Сомко
Е.А. Федорова

ПРОФЕССИОНАЛЬНЫЙ ИНОСТРАННЫЙ ЯЗЫК ДЛЯ СПЕЦИАЛИСТОВ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург

2016

Сомко А.С., Федорова Е.А. Профессиональный иностранный язык для специалистов в области компьютерной безопасности. – СПб: Университет ИТМО, 2016. – 33 с.

Учебно-методическое пособие «Профессиональный иностранный язык для специалистов в области компьютерной безопасности» предназначено для изучения английского языка для специальных целей студентами Факультета информационной безопасности и компьютерных технологий. Пособие может быть использовано как на аудиторных занятиях, так и для самостоятельной работы студентов.
В пособии представлены оригинальные тексты, знакомящие студентов с основами информационной безопасности. Каждый урок снабжен терминологическими и коммуникативными упражнениями по изучаемой тематике.

Пособие предназначено для занятий по дисциплине «иностранный язык» со студентами, обучающимися в рамках направлений подготовки бакалавриата и магистратуры 10.03.01, 10.04.01 – «Информационная безопасность».

Рекомендовано к печати Ученым советом Института ИМРиП 25 января 2016 года, протокол №3.

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Contents

Unit 1

The Need for Network Security

The Internet continues to grow exponentially. Personal, government, and business applications continue to multiply on the Internet, with immediate benefits to end users. However, network-based applications and services can pose security risks to individuals and to the information resources of companies and governments. Information is an asset that must be protected.

Security has one purpose: to protect assets. For most of history, this meant building strong walls to stop the enemy and establishing small, well-guarded doors to provide secure access for friends. This strategy worked well for the centralized, fortress-like world of mainframe computers and closed networks.

The closed network typically consists of a network designed and implemented in a corporate environment and provides connectivity only to known parties and sites without connecting to public networks. Networks were designed this way in the past and thought to be reasonably secure because of no outside connectivity.

With the advent of personal computers, LANs, and the wide-open world of the Internet, the networks of today are more open. As e-business and Internet applications continue to grow, the key to network security lies in defining the balance between a closed and open network and differentiating the good guys from the bad guys.

With the increased number of LANs and personal computers, the Internet began to create untold numbers of security risks. Firewall devices, which are software or hardware that enforce an access control policy between two or more networks, were introduced. This technology gave users a balance between security and simple outbound access to the Internet, which was mostly used for e-mail and web surfing.

This balance was short-lived as the use of extranets began to grow, which connected internal and external business processes. Businesses were soon realizing tremendous cost savings by connecting supply-chain management and enterprise resource planning systems to their business partners, and by connecting sales-force automation systems to mobile employees, and by providing electronic commerce connections to business customers and consumers. The firewall began to include intrusion detection, authentication, authorization, and vulnerability-assessment systems. Today, successful companies have again struck a balance by keeping the enemies out with increasingly complex ways of letting friends in.

Most people expect security measures to ensure the following:

•Users can perform only authorized tasks.

•Users can obtain only authorized information.

•Users cannot cause damage to the data, applications, or operating environment of a system.

The word *security* means protection against malicious attacks by outsiders and by insiders. Statistically, there are more attacks from inside sources.

Security also involves controlling the effects of errors and equipment failures. Anything that can protect against an attack will probably prevent random misfortunes, too.

Exercise 1. ***Answer the questions using the information from the text.***

1. Who can be put at risk by network-based applications?
2. What strategy was effective in the period of mainframe computers and closed networks?
3. What is a closed network?
4. What is considered to be the key to network security nowadays?
5. How do firewall devices benefit users?
6. What advantages does connecting internal and external business processes give to companies?
7. What functions do firewall devices need as a result of growing use of extranets?
8. What do most people expect from security measures?
9. What does network security involve except for protection against malicious attacks?

Exercise 2. ***True or false?***

1. The firewall device is used to prevent connecting to public networks.
2. The use of extranets gave businesses a lot of new opportunities.
3. The Internet became more secure when the number of personal computers increased.
4. Vulnerability-assessment systems cannot be included into firewall devices.
5. Networks are more often attacked by insiders than by outsiders.

Exercise 3. ***Write a short summary of the text.***

Exercise 4. ***Use the words and expressions from the box to complete the sentences.***

vulnerability-assessment	connectivity	e-business	firewall	LAN
public network	authorization	application	authentication	access

1. Before connecting to a _____, make sure your system is fully up to date with the latest patches.
2. End users have great difficulty using this file permission system to create security policies for file _____.

3. _____ is the process of determining whether someone or something is, in fact, who or what it is declared to be.
4. _____ is the process used in verifying that someone who has requested or initiated an action has the right to do so.
5. _____ is capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line; but the distances are limited and there is also a limit on the number of computers that can be attached to it.
6. Sometimes a new and popular _____ arises which only runs on one platform, increasing the desirability of that platform.
7. If security holes are found as a result of _____, a vulnerability disclosure may be required.
8. When organizations go online, they have to decide which _____ models best suit their goals.
9. Persistent _____ is impossible in a mobile world, which means it is also impossible for employees to access their enterprise applications when they need them most—when they're in the field doing their jobs.
10. When a packet passes through a _____, it filters the packet on a protocol/port number basis.

Exercise 5. ***Match the verbs and the nouns. Sometimes, more than one option is possible.***

1. surf	**a.** a task
2. provide	**b.** access
3. connect to	**c.** the web
4. perform	**d.** damage
5. cause	**e.** a network

Unit 2

Threats to Network Security

Vulnerability is a weakness that is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves. Threats are the people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses. There are four primary classes of threats to network security.

Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker’s skills can still do serious damage to an individual or an organization. For example, if an external company website is hacked, the

integrity of the company is damaged. Even if the external website is separate from the internal information that sits behind a protective firewall, the public does not know that. All the public knows is that the site is not a safe environment to conduct business.

Structured threats come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies.

External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers.

Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network.

As the types of threats, attacks, and exploits have evolved, various terms have been coined to describe different groups of individuals. Some of the most common terms are as follows:

•Hacker—is a general term that has historically been used to describe a computer programming expert. More recently, this term is commonly used in a negative way to describe an individual who attempts to gain unauthorized access to network resources with malicious intent.

•Cracker—is the term that is generally regarded as the more accurate word that is used to describe an individual who attempts to gain unauthorized access to network resources with malicious intent.

•Phreaker—is an individual who manipulates the phone network to cause it to perform a function that is normally not allowed. A common goal of phreaking is breaking into the phone network, usually through a payphone, to make free long-distance calls.

•Spammer—is an individual who sends large numbers of unsolicited e-mail messages. Spammers often use viruses to take control of home computers to use these computers to send out their bulk messages.

•Phisher—is an individual who uses e-mail or other means in an attempt to trick others into providing sensitive information, such as credit card numbers or passwords. Phishers masquerade as a trusted party that would have a legitimate need for the sensitive information.

•White hat—is a term used to describe individuals who use their abilities to find vulnerabilities in systems or networks and then report these vulnerabilities to the owners of the system so that they can be fixed.

•Black hat—is another term for individuals who use their knowledge of computer systems to break into systems or networks that they are not authorized to use.

Exercise 1. ***Answer the questions using the information from the text.***

1. What is vulnerability in network security?
2. Who are considered to be threats to network security?
3. How dangerous can unstructured threats be to users?
4. What is the difference between structured and unstructured threats?
5. How can external threats get access to computer systems or networks?
6. What people can be considered internal threat?
7. What is the most accurate term to describe an individual attempting to gain unauthorized access to network resources with malicious intent?
8. What is a common goal of phreaking?
9. How do phishers usually get the information they need?
10. What is the goal of white hats' activity?

Exercise 2. ***True or false?***

1. Exploit code and scripts are often developed by inexperienced individuals.
2. It is impossible to get access to computer systems through the Internet.
3. Hacker is a term that has recently been used to describe a computer programming expert.
4. A common goal of spammers is to get sensitive information.
5. Black hats do not help to fix vulnerabilities.

Exercise 3. ***Write a short summary of the text.***

Exercise 4. ***Use the words and expressions from the box to complete the sentences.***

password cracker	router	white hat	phone network	damage
sensitive information	exploit	black hat	hacking tool	server

1. In the case of a _____, the data is transmitted not to a central hub in a small network of devices (as it is with Wi-Fi) or even directly from device to device (as it is with Bluetooth), but through a global network of transmitters and receivers.
2. An example of a _____ is a computer worm.
3. A _____ may include a firewall, VPN handling, and other security functions, or these may be handled by separate devices.
4. _____ can be used to recover a forgotten password.
5. The scale of the _____ depends on the targets of the virus and sometimes the results of its activity are imperceptible.
6. A _____ hacker may work as a consultant or be a permanent employee on a company's payroll.

7. A local _____ requires prior access to the vulnerable system and usually increases the privileges past those granted by the system administrator.
8. The purpose of a _____ is to share data as well as to share resources and distribute work.
9. The credit card files of the company's customers were very _____, so they hired a team of experts to devise security measures for it.
10. _____ hackers can inflict major damage on both individual computer users and large organizations by stealing personal financial information, compromising the security of major systems, or shutting down or altering the function of websites and networks.

Exercise 5. ***Match the verbs and the nouns. Sometimes, more than one option is possible.***

1. enforce	**a.** access
2. fix	**b.** a policy
3. gain	**c.** a script
4. develop	**d.** a website
5. hack	**e.** a vulnerability

Unit 3

Attacks

Four primary classes of attacks exist: (1) reconnaissance, (2) access, (3) denial of service, and (4) worms, viruses, and Trojan horses.

Reconnaissance is an unauthorized discovery and mapping of systems, services, or vulnerabilities. It is also known as information gathering and, in most cases, it precedes an actual access or denial-of-service attack. Reconnaissance is somewhat analogous to a thief casing a neighborhood for vulnerable homes to break into, such as an unoccupied residence, easy-to-open doors, or open windows.

System access is the ability for an unauthorized intruder to gain access to a device for which the intruder does not have an account or a password. Entering or accessing systems to which one does not have authority to access usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.

Denial of service (DoS) implies that an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users. DoS attacks involve either crashing the system or slowing it down to the point that it is unusable. But DoS can also be as simple as deleting or corrupting information. In most cases, performing the attack simply involves running a

hack or script. The attacker does not need prior access to the target because a way to access it is all that is usually required. For these reasons, DoS attacks are the most feared.

Malicious software (worms, viruses, and Trojan horses) is inserted onto a host to damage a system; corrupt a system; replicate itself; or deny services or access to networks, systems or services. They can also allow sensitive information to be copied or echoed to other systems.

Trojan horses can be used to ask the user to enter sensitive information in a commonly trusted screen. For example, an attacker might log in to a Windows box and run a program that looks like the true Windows logon screen, prompting a user to type his username and password. The program would then send the information to the attacker and then give the Windows error for bad password. The user would then log out, and the correct Windows logon screen would appear; the user is none the wiser that his password has just been stolen.

Even worse, the nature of all these threats is changing—from the relatively simple viruses of the 1980s to the more complex and damaging viruses, DoS attacks, and hacking tools in recent years. Today, these hacking tools are powerful and widespread, with the new dangers of selfspreading blended worms and network DoS attacks. Also, the old days of attacks that take days or weeks to spread are over. Threats now spread worldwide in a matter of minutes.

The next generations of attacks are expected to spread in just seconds. These worms and viruses could do more than just wreak havoc by overloading network resources with the amount of traffic they generate, they could also be used to deploy damaging payloads that steal vital information or erase hard drives. Also, there is a strong concern that the threats of tomorrow will be directed at the very infrastructure of the Internet.

Exercise 1. ***Answer the questions using the information from the text.***

1. What is a common classification of attacks?
2. What are the objectives of reconnaissance?
3. When can accessing a system be considered an attack?
4. What do DoS attacks usually involve?
5. What examples of malicious software exist?
6. What damage is malicious software able to cause to a system?
7. How can Trojan horses be used to steal passwords?
8. How are attacks changing over the time?
9. What are the next generations of attacks expected to be like?

Exercise 2. ***True or false?***

1. Reconnaissance is often used as the first step of a major attack.
2. DoS attacks are dangerous because most of them are very simple to perform.

3. Viruses spread considerably faster nowadays than before.
4. Selfspreading blended worms originate from the 1980s.
5. The next generations of attacks could erase hard drives.

Exercise 3. ***Write a short summary of the text.***

Exercise 4. ***Use the words and expressions from the box to complete the sentences.***

malicious software	denial of service	worm	logon screen	username
password	reconnaissance	payload	hard drive	intruder

1. Windows makes it possible to change the _____ that appears when you start your computer without any third-party software, but this setting is well hidden.
2. A _____ attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have.
3. The _____detection technique tries to identify people behind attacks by analyzing their computational behaviour.
4. Nowadays, it is a common practice for computer systems to hide a _____ as it is typed.
5. Spyware or other _____ is sometimes found embedded in programs supplied officially by companies, e.g., downloadable from websites, that appear useful or attractive, but may have, for example, additional hidden tracking functionality that gathers marketing statistics.
6. In a computer, a _____ is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.
7. Your _____ can be used to create a custom link to your profile that you can give out to people or post on external websites.
8. Active _____ is a type of computer attack in which an intruder engages with the targeted system to gather information about vulnerabilities.
9. In computer security, _____ refers to the part of malware which performs a malicious action.
10. Computers have a _____ and use it to store files for the operating system and software that run on the computer, as well as files created or downloaded to the computer by a user.

Exercise 5. ***Match the verbs and the nouns. Sometimes, more than one option is possible.***

1. deny	**a.** a hard drive
2. type	**b.** a payload
3. map	**c.** a username
4. erase	**d.** a service

5. deploy **e.** a system

Unit 4

The Most Devastating Cyber Attacks of 2015

US Office of Personnel Management. This breach was one of the biggest ever of US government systems. Although not proved, the attack was believed to be perpetrated by Chinese hackers. The data theft consisted of stealing addresses, health and financial details of 19.7 million people who had been subjected to government background checks as well as 1.8 million others.

FBI portal breach. A portal used by police and the FBI to share intelligence and arrest suspects was hacked in November this year and data on arrestees stolen. While the FBI didn't announce figures on how many people were affected, this attack is thought to be one of the biggest law enforcement hacks this year. It was perpetrated by the same hackers who accessed CIA director John Brennan's personal email account earlier this year.

TalkTalk. Last October saw one of the UK's biggest hacks this year and one that dominated news headlines for weeks. The mobile phone provider was the target of a bunch of teenage hackers who stole the details of over 20,000 customers. The hackers were quickly identified and dealt with, but the company has been left with a bill of up to £35 million, having had millions wiped off its share price, and is facing law suits from customers and investors.

Anthem. It emerged in October that Chinese hackers had targeted health insurance company Anthem in a bit to learn more about how medical coverage is set up in the US. Apparently, Anthem has not been the only target, with smaller insurer Premera saying it had been hacked in March, exposing details of about 11 million people. Healthcare data has become some of the most valuable information that can be sold in the online black market, making healthcare companies a prime target for hackers.

Carphone Warehouse. One of the biggest breaches in the UK this year was when the details of almost 2.5 million customers was stolen back in August, with almost 90,000 having encrypted credit card information stolen. The company said it had been the victim of a sophisticated cyber attack that is being investigated by the industry watchdog.

Multiple US financial institutions and media companies. Hackers stole the details of over 100 million people with banks accounts in what authorities dubbed "securities fraud on cyber steroids". At least nine banks and other financial institutions, including JP Morgan, plus Dow Jones, the parent company of the WSJ, were targeted by hackers who gained access to a number of systems that helped them to make money from illegal activities, including running a digital currency exchange, gambling websites and inflating stock prices. Three men have been prosecuted.

Vodafone. Another UK telco was involved in a data breach in October, when hackers stole the personal and financial details of 2000 customers. Hackers used emails addresses and passwords acquired from an unknown source to get names, phone numbers, bank sort codes and the last four digits from bank accounts.

Samsung Electronics. The electronics giant's subsidiary, LoopPay, was hacked back in March this year. LoopPay developed the payment system used to run Samsung Pay, a competitor to Apple Pay, but Samsung said that no user data was compromised during the hack, which lasted several months before detection.

Hilton Worldwide. The global hotel chain has recently been the victim of an attack that infiltrated its POS terminals, giving hackers unfettered access to customer credit card information. Stolen information included cardholder names and card numbers, security codes and expiry dates, enabling hackers to shop online or by phone.

Exercise 1. ***Answer the questions using the information from the text.***

1. What was the purpose of Chinese hackers?
2. What kind of data was stolen during the FBI attack?
3. What other cosequencies of the hack did TalkTalk have to deal with?
4. What was the weakest point in the UK cyber security?
5. What financial companies and institutions were subject to cyber attacks?
6. How many customers became victim of the attack on Vodafone?
7. How long did the hack of LoopPay last before being detected?
8. What do all these attacks have in common?
9. Which attack affected more people?
10. Which attack may be considered the most devastating?

Exercise 2. ***True or false?***

1. No one was found guilty in the course of US financial institutions and media companies hacks.
2. Anthem wasn't the only insurance company to be attacked in 2015.
3. A credit card information is the most wanted data by hackers.
4. CIA was the only organization to withstand cyber attacks.
5. The cyber crimes are always committed by adults.

Exercise 3. ***Write a short summary of the text.***

Exercise 4. ***Use the words and expressions from the box to complete the sentences.***

perpetrate	devastating	digital currency exchange	prosecute	prime target
subsidiary	law enforcement	gambling websites	law suit	unfettered access

1. Two of the employees filed a _____ against their former employer.
2. The debt crisis that has spread from Greece to much-bigger Italy could massively escalate economic disruption and end in highly _____ outcomes.
3. Internet _____ had increased from just 15 websites in 1996, to 200 websites in 1997.
4. _____ allows you to transfer traditional fiat currency to and from bitcoin.
5. Privacy concerns are legitimate but restrictions on the _____ to information could do a great deal more harm to Hong Kong in the long run.
6. Healthcare organizations are a _____ for cyber attacks.
7. Most _____ is carried out by police officers serving in regional police forces within one of these jurisdictions.
8. The purchase of a controlling interest differs from a merger and the parent corporation can acquire the controlling interest with a smaller investment. Additionally, stockholder approval is not required in the formation of a _____ as it would be in the event of a merger.
9. Somehow she seemed too gentle, too vague to _____ such a brutal crime.
10. Holmes sought their identities, so he could _____ them for violating laws regarding grand jury secrecy.

Exercise 5. ***Find synonyms.***

1. coverage	**a.** gap
2. breach	**b.** deception
3. fraud	**c.** discovery
4. competitor	**d.** robbery
5. detection	**e.** compensation
6. theft	**f.** rival

Unit 5

Encryption

Traditionally, ciphers have used information contained in secret decoding keys to code and decode messages. The process of coding plaintext to create ciphertext is called encryption and the process of decoding ciphertext to produce the plaintext is called decryption. Modern systems of electronic cryptography use digital keys (bit strings) and mathematical algorithms (encryption algorithms) to encrypt and decrypt information. There are two types of encryption: symmetric key encryption and public (asymmetric) key encryption.

Symmetric key and public key encryption are used, often in conjunction, to provide a variety of security functions for network and information security.

Symmetric Key Encryption Encryption algorithms that use the same key for encrypting and for decrypting information are called symmetric-key algorithms. The symmetric key is also called a secret key because it is kept as a shared secret between the sender and receiver of information. Otherwise, the confidentiality of the encrypted information is compromised. Symmetric key encryption is much faster than public key encryption, often by 100 to 1,000 times. Because public key encryption places a much heavier computational load on computer processors than symmetric key encryption, symmetric key technology is generally used to provide secrecy for the bulk encryption and decryption of information.

Symmetric keys are commonly used by security protocols as session keys for confidential online communications. For example, the Transport Layer Security (TLS) and Internet Protocol security (IPSec) protocols use symmetric session keys with standard encryption algorithms to encrypt and decrypt confidential communications between parties. Different session keys are used for each confidential communication session and session keys are sometimes renewed at specified intervals.

Symmetric keys also are commonly used by technologies that provide bulk encryption of persistent data, such as e-mail messages and document files. For example, Secure/Multipurpose Internet Mail Extensions (S/MIME) uses symmetric keys to encrypt messages for confidential mail, and Encrypting File System (EFS) uses symmetric keys to encrypt files for confidentiality. Cryptography-based security technologies use a variety of symmetric key encryption algorithms to provide confidentiality.

Public Key Encryption Encryption algorithms that use different keys for encrypting and decrypting information are most often called public-key algorithms but are sometimes also called asymmetric key algorithms . Public key encryption requires the use of both a private key (a key that is known only to its owner) and a public key (a key that is available to and known to other entities on the network). A user's public key, for example, can be published in the directory so that it is accessible to other people in the organization. The two keys are different but complementary in function. Information that is encrypted with the public key can be decrypted only with the corresponding private key of the set. The RSA digital signature process also uses private keys to encrypt information to form digital signatures. For RSA digital signatures, only the public key can decrypt information encrypted by the corresponding private key of the set. Today, public key encryption plays an increasingly important role in providing strong, scalable security on intranets and the Internet. Public key encryption is commonly used to perform the following functions:

•Encrypt symmetric secret keys to protect the symmetric keys during exchange over the network or while being used, stored, or cached by operating systems.

•Create digital signatures to provide authentication and nonrepudiation for online entities.

•Create digital signatures to provide data integrity for electronic files and documents.

Exercise 1. ***Answer the questions using the information from the text.***

1. What process is called encryption?
2. How many types of encryption are there? What are they?
3. What is a secret key encryption?
4. Which type of encryption is faster and why?
5. What systems and technologies use symmetric key encryption?
6. What do IPS and EFS stand for?
7. What is an asymmetric key encryption?
8. Where can public key encryption be used?

Exercise 2. ***True or false?***

1. Symmetric and public key encryption may be used together.
2. Public key encryption is used for the massive encryption and decryption.
3. A user's public key should be kept as a shared secret between the sender and receiver of information.
4. For digital signatures the information that is encrypted with the public key can be decrypted only with the corresponding private key.
5. Digital signatures prove authorship, finalize contents, and secure against future tampering.

Exercise 3. ***Write a short summary of the text.***

Exercise 4. ***Use the words and expressions from the box to complete the sentences.***

entities	ciphertext	cryptography	compromise	bulk
directory	complementary	signature	data integrity	scalable security

1. _____ encryption protocols provide safe and cost effective methods for protecting data transmissions from compromise and theft.
2. _____ is unreadable until it has been decrypted with a key.
3. This system provides multimedia application developers with an engine for online _____ verification.
4. In symmetric key cryptography, a single secret key is used between _____ , whereas in public key systems, each entity has different keys, or asymmetric keys.

5. _____ refers to the accuracy and consistency (validity) of data over its lifecycle.
6. A data _____ is an incident involving the breach of a system or network environment where cardholder data is processed, stored or transmitted.
7. _____ service is a software application for organizing information about a computer network's users and resources.
8. Encrypted messages can sometimes be broken by cryptanalysis, also called codebreaking, although modern _____ techniques are virtually unbreakable.
9. In the hybrid approach, the two technologies (symmetric and asymmetric) are used in a _____ manner, with each performing a different function. A symmetric algorithm creates keys that are used for encrypting bulk data, and an asymmetric algorithm creates keys that are used for automated key distribution.
10. _____ of Internet Services and Architecture provides an in-depth analysis of many key scaling technologies.

Exercise 5. ***Find synonyms.***

1. signature	**a.** secretive
2. load	**b.** massive
3. confidential	**c.** connection
4. bulk	**d.** sign
5. conjunction	**e.** steady
6. persistent	**f.** charge

Unit 6

Steganography

Steganography is the art of hiding information in a cover document or file. Therefore, today, steganography is usually accomplished by electronic encryption, which is the encoding of information that can only be decoded by the person possessing the correct electronic key. A cover document contains this hidden encoded information, and usually the transfer of this secret information is very secure.

Steganography now is accomplished in the digital world using mathematical algorithms to encrypt data. One may hide information in a variety of files. Steganography replaces unused parts of data with the secret information. It is possible to hide information in text, for example, in the spaces between words. This type of information hiding is more successful than steganography that consists of hidden information in infrequent spelling errors and in words replaced by synonyms. One of the main requirements for hiding

information in digital sounds and images is redundant, repetitive information. Steganography uses this part of the sound or image to hide the secret information. One unique example of hiding information is the embedding of a mobile telephone conversation into an Integrated Services Digital Network (ISDN) video conferencing system. It is possible to do so without seriously changing the quality of the video, and with the correct key, one could decode the conversation.

The easiest way to hide information is to replace the least significant bit (LSB) of every element with one bit of the secret message. For example, when a picture is the desired cover document, each pixel of the picture contains 24 bits of information, which, to the computer, consists of 0s and 1s. To insert the secret information, one can change these 0s and 1s to bits of secret information. The most useful way to insert these bits is do to do so in a random way according to the secret key. This makes it harder for others to break the code. The updated picture should not appear noticeably different, or else attackers may become suspicious. When attempting this type of encryption, one should also choose a cover image that does not contain a large area of solid colors because any slight change caused from the embedded information will be more apparent.

Watermarking is a type of steganography used when other parties know of the existence of hidden information and may have the desire to remove or change it. Therefore, copyright protection is a common use of watermarks. One can protect the validity and originality of information by embedding information about the source of the data into files. In this case, the watermark provides information about the author, copyright, or license information. Another application of watermarking is fingerprinting, which involves inserting a different watermark into each copy of a file in order to monitor the recipients of the file. Therefore, one can trace back illegally produced copies to the original receiver. Watermarks are also useful in providing information on the copy status of the document. A final application of watermarks is to detect manipulation of the original file. Certain important characteristics about the file are stored in the file itself in the form of a watermark and make it possible to check if the image later has altered characteristics.

Exercise 1. ***Answer the questions using the information from the text.***

1. What is steganography?
2. Where does steganography hide a secret massage?
3. What type of hiding information is more successful?
4. How can a message be encrypted into a picture?
5. What is watermarking?
6. Where can watermarking be applied?
7. What is fingerprinting needed for?
8. How can one check if the characteristics of the image has been altered?

Exercise 2. ***True or false?***

1. Steganography is the encoding of information that can only be decoded by the person possessing the correct electronic key.
2. LSB is replaced with the encrypted information.
3. To insert a hidden message into a picture you should opt for the image that contains a large area of solid colors.
4. Embedding information about the source of the data into files, watermarking protects the original from alterations.
5. The watermark provides information about the sender and the recepient.

Exercise 3. ***Write a short summary of the text.***

Exercise 4. ***Use the words and expressions from the box to complete the sentences.***

cover document	repetitive information	copyright protection		watermark
spelling errors	video conferencing	confidentiality	recipient	fingerprint

1. _____ subsists in original works of authorship fixed in any tangible medium of expression from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.
2. It is possible to use _____ for information hiding, by modifying them or judiciously injecting them to the text.
3. A digital _____ is called *robust* with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations.
4. In general, cryptography can be used also to monitor the integrity of the _____ to confirm the authenticity of the source.
5. Any change in _____ of ciphertext block gives out a hint to the attacker that there is some change in prevailing status.
6. The difficulty with _____ becomes apparent if a document does become public knowledge.
7. Microsoft word being a commonly used communication medium can be well utilized as a _____ to hide the data.
8. For each e-mail message, the sender can specify a list of _____ .
9. This product unifies cloud _____ , simple online meetings, and cross platform group chat into one easy-to-use platform.

Exercise 5. ***Find synonyms.***

1. cover	**a.** change
2. redundant	**b.** untrustworthy

3. validity	**c.** irrelevant
4. suspicious	**d.** coat
5. alteration	**e.** legitimacy
6. insignificant	**f.** excessive

Unit 7

Software Security

Software security is the idea of engineering software so that it continues to function correctly under malicious attack. Most technologists acknowledge this undertaking's importance, but they need some help in understanding how to tackle it.

A central and critical aspect of the computer security problem is a software problem. Software defects with security ramifications—including implementation bugs such as buffer overflows and design flaws such as inconsistent error handling—promise to be with us for years. All too often, malicious intruders can hack into systems by exploiting software defects. Internet-enabled software applications present the most common security risk encountered today, with software's ever-expanding complexity and extensibility adding further fuel to the fire.

Pondering the question, "What is the most effective way to protect software?" can help untangle software security and application security. On one hand, software security is about building secure software: designing software to be secure, making sure that software is secure and educating software developers, architects and users about how to build secure things. On the other hand, application security is about protecting software and the systems that software runs in a post facto way, after development is complete. Issues critical to this subfield include sandboxing code (as the Java virtual machine does), protecting against malicious code, obfuscating code, locking down executables, monitoring programs as they run (especially their input), enforcing the software use policy with technology and dealing with extensible systems.

Application security follows naturally from a network-centric approach to security, by embracing standard approaches such as penetrate and patch and input filtering (trying to block malicious input) and by providing value in a reactive way. One reason that application security technologies such as firewalls have evolved the way they have is because operations people dreamed them up. In most corporations and large organizations, security is the domain of the infrastructure people who set up and maintain firewalls, intrusion detection systems, and antivirus engines (all of which are reactive technologies).

However, these people are operators, not builders. Given the fact that they don't build the software they have to operate, it's no surprise that their approach is to move standard security techniques "down" to the desktop and application

levels. The gist of the idea is to protect vulnerable things (in this case, software) from attack, but the problem is that vulnerabilities in the software let malicious hackers skirt standard security technologies with impunity. If this were not the case, then the security vulnerability problem would not be expanding the way that it is. Clearly, this emphasizes the need to get builders to do a better job on the software in the first place.

On the road to making such a fundamental change, we must first agree that software security is not security software. This is a subtle point often lost on development people who tend to focus on functionality. Obviously, there are security functions, and most modern software includes security features, but adding features such as SSL (for cryptographically protecting communications) does not present a complete solution to the security problem. Software security is a system-wide issue that takes into account both security mechanisms (such as access control) and design for security (such as robust design that makes software attacks difficult). Software security must be part of a full life cycle approach. Just as you can't test quality into a piece of software, you can't spray paint security features onto a design and expect it to become secure. There's no such thing as a magic crypto fairy dust—we need to focus on software security from the ground up.

Exercise 1. ***Answer the questions using the information from the text.***

1. How can the concept of software security be described?
2. Why is software the central aspect of computer security?
3. What does software security involve?
4. What does application security involve?
5. What standard approaches of application security exist?
6. Why do application security techniques prevail nowadays?
7. Why do not application security techniques always work well?
8. What is the difference between software security and security software?
9. When should software developers start focusing on security?

Exercise 2. ***True or false?***

1. Engineering secure software is a complicated issue for most technologists.
2. The problem of implementation bugs is likely to be solved in the short term.
3. Internet-enabled software applications are relatively secure.
4. The more complex software is, the less risk it presents.
5. Modern software should never include security features.

Exercise 3. ***Write a short summary of the text.***

Exercise 4. ***Use the words and expressions from the box to complete the sentences.***

executable	use policy	sandbox	full life cycle	robust design
desktop	buffer overflow	bug	antivirus engines	design flaws

1. Here are some examples of _____: broken authentication mechanism (that could be authentication bypass), failure to authorize after authentication, not explicitly validating all data or understanding how integrated external components change the attack surface.
2. A _____ is a set of rules applied by the owner, creator or administrator of a network, website, or service, that restrict the ways in which the network, website or system may be used, and sets guide lines as to how it should be used.
3. Multiscanning is running multiple anti-malware or _____ concurrently.
4. In Windows operating system, an _____ usually has a file name extension of .bat, .com, or .exe.
5. Systems development life cycle (SDLC) and systems analysis and design (SAD) are cornerstones of _____ product and system planning.
6. _____ is a set of engineering methods widely successful in reducing sensitivity to such noise factors as customer use conditions, manufacturing variability, and degradation of a system over time.
7. In general, a _____ is an isolated computing environment in which a program or file can be executed without affecting the application in which it runs.
8. A _____ occurs when a program or process tries to store more data in a temporary data storage area than it was intended to hold.
9. If an inconsistency is encountered, the program may immediately halt so that the _____ may be located and fixed.
10. An all-in-one _____ computer typically combines the case and monitor in one unit.

Exercise 5. ***Match the verbs and the nouns. Sometimes, more than one option is possible.***

1. filter	**a.** a system
2. handle	**b.** information
3. run	**c.** an error
4. enter	**d.** an intrusion
5. detect	**e.** input

Unit 8

Self-encrypting Hard Drive

A SED is a self-encrypting hard drive with a circuit built into the disk drive controller chip that encrypts all data to the magnetic media and decrypts all the data from the media automatically. All SEDs encrypt all the time from the factory onwards, performing like any other hard drive, with the encryption being completely transparent or invisible to the user.

To protect the data from theft, the user provides a password. This password is used by the drive to encrypt or decrypt the media encryption key. In this way even the media encryption key cannot be known without knowing the password. Very strong passwords are permitted by the Trusted Computing Group specification for SEDs of up to 32 bytes. With such a password, it is practically impossible for a would-be data thief to recover the media encryption key and access data on the hard drive. In January 2009, the Trusted Computing Group (TCG) published final specifications for SEDs that are widely supported by PC, server drive and application providers. In March 2009, hard drive suppliers started shipping SEDs based on the TCG's specifications.

How does a SED work? The encryption key used in SEDs is called the Media Encryption Key (MEK). Locking and unlocking a drive requires another key, called the Key Encryption Key (KEK) supplied by the user (or the platform, or the network). As the name implies, the KEK is used to encrypt or decrypt the MEK. The KEK is never stored in plaintext inside the drive. If no KEK is set, the drive is always unlocked and appears not to be encrypting even though it is. If a KEK is set, the drive will power up locked until the correct KEK is given to the drive by the user. When a locked self-encrypting drive is powered up, the BIOS first sees a shadow disk that is much smaller than the real disk. The shadow disk is usually around 100 megabytes. The software in the shadow disk is read-only, and this software requires the KEK from the user to unlock the real disk for use and to decrypt the MEK so the real disk can be read and written to. The shadow disk software stores a cryptographic hash of the KEK so it can recognise if the user gives the right KEK. When the user enters the passcode (KEK) the shadow disk creates a hash of that passcode and compares it with the stored hash of the KEK. If the two match, the MEK is decrypted and put into the encryption/decryption circuit inside the drive, the BIOS is called to start from the disk again, but now this is the much bigger real disk with a capacity in gigabytes rather than megabytes, and the operating system boots normally. This shows one of the chief benefits of SEDs. By design, SEDs do all the cryptography within the disk drive controller, which means the disk encryption keys are never present in the computer's processor or memory, where they could be accessed by hackers. Likewise, authentication of the user is done within the SED and never exposed within the memory or operating system of the computer, which means attacks on vulnerabilities in the operating system cannot be used against a SED's pre-boot process.

Exercise 1. ***Answer the questions using the information from the text.***

1. What is a SED?
2. Who sets the password for the SED?
3. What passwords are considered trustworthy?
4. What does TCG stand for?
5. What is the difference between the KEK and the MEK? How do they interact?
6. When does the BIOS first see a shadow disk?
7. What is a shadow disk used for? What capacity does it have?
8. Where is all the cryptography done by SEDs?

Exercise 2. ***True or false?***

1. 64 bytes is the perfect size for a dependent password.
2. The MEK is always stored in the cyphertext.
3. If the MEK and the KEK match the boot of the real disc starts.
4. The shadow and the real disk have the same capacity.
5. All encryption keys are held in the computer's processor or memory.

Exercise 3. ***Write a short summary of the text.***

Exercise 4. ***Use the words and expressions from the box to complete the sentences.***

specification	self-encrypting drive	plaintext
real disk	pre-boot authentication	shadow disc

1. If a laptop using a _____ is stolen or lost while in sleep mode, the security of its data can't be guaranteed.
2. In cryptography _____ is information a sender wants to transmit to a receiver.
3. This redundant storage allows the _____ or set of disks to pick up the load in case of a disk crash on the _____ or disks; thus the users never see a crashed disk.
4. _____ is the process of validating user login credentials before unlocking contents of the hard drive.
5. A datasheet or a _____ sheet is a document that summarizes the performance and other technical characteristics of a product, machine, component (e.g., an electronic component), material, a subsystem (e.g., a power supply) or software in sufficient detail to be used by a design engineer to integrate the component into a system.

Exercise 5. ***Find synonyms.***

1. recovery	**a.** restrainer
2. circuit	**b.** obvious
3. capacity	**c.** mending

4. controller
5. transparent
6. passcode

d. countersign
e. transmitter
f. volume

Unit 9

Building Usable Security

One of the most overlooked aspects of application security is usability. Users are often the weakest link in a software system. If security controls embedded in software systems hinder users' ability to accomplish their tasks, users will ignore or try to bypass such controls, a common occurrence in today's systems. Building usable security functions is a significant component of building secure systems.

Security engineers generally lack experience in usability engineering. One of the main reasons why application security violations continue to rise, is the fact that many deployed security mechanisms are not user friendly, limiting their effectiveness. Unless engineers start thinking more about how to make security more usable, progress in securing systems will be limited.

Many people believe that there is an inherent tradeoff between security and usability. However, that does not have to be the case, since today most security pop-ups are overlooked, most scan reminders are ignored and most updates are automated or not taken care of. In such a situation, it becomes important for the developers to come up with workable solutions. These could be by making security more understandable and usable through the following ways:

•Invisibly strengthening security i.e. working behind the scenes; strengthening the spam filters and various algorithms used to scan attachments, emails and downloads i.e. strengthening the anti-virus software algorithms and training them to work better.

•Making security understandable. Various tools may be helpful in making the user realize when he/she faces a threat. Security pop-ups when a malicious script is executed or the browser address bar turning red in case of an insecure website being accessed are some possible ways.

•Training the user. Various web and mobile applications today aim to train the user to make them realize what an actual threat looks like and how to cope with it. For example, a system generated phishing email could be sent to users who on clicking the link, reach a page which educates them about the consequences if the email had really been a phishing link.

The challenge to security tools, applications and services can be dealt with by giving the user the control to privacy and security of their systems. This can only be done in an effective way if the security measures implemented are understandable and easy to maneuver for a lay user and instance of which could be—instead of having 13 different screens as in Windows to change file permissions, have a single, comprehensible one. New user interfaces need to be

developed effectively and efficiently to support users in managing the privacy and security policies that they themselves implement and also the ones implemented by their system.

Exercise 1. ***Answer the questions using the information from the text.***

1. What aspect of application security is ignored the most, according to the author?
2. Why might users be the weakest link in a software system?
3. What are the consequences of security mechanisms not being user friendly?
4. How do users usually deal with security notifications?
5. What are the three ways to raise the effectiveness of security mechanisms?
6. How can security be invisibly strengthened?
7. How can developers make security more understandable?
8. What example of training the user do you know?
9. What is crucial to provide the user with the control of their systems?

Exercise 2. ***True or false?***

1. Users cannot bypass security controls which prevent them from accomplishing their tasks.
2. Progress in securing systems depends on raising their usability.
3. Some security attacks may be used to educate the user.
4. It is useless for an unprofessional user to understand the security measures.
5. Changing file permissions should be as complicated as possible so that the user cannot cause any damage.

Exercise 3. ***Write a short summary of the text.***

Exercise 4. ***Use the words and expressions from the box to complete the sentences.***

algorithm	spam filter	update	usability	download
attachment	address bar	pop-up	browser	privacy

1. When that _____ is opened, the Trojan is unleashed, giving the adversary control of the unlucky computer.
2. In computer systems, an _____ is basically an instance of logic written in software by software developers to be effective for the intended "target" computer(s) to produce output from given input.
3. Tools used to protect _____ on the Internet include encryption tools and anonymizing services.

4. The primary purpose of a web _____ is to bring information resources to the user, allowing them to view the information, and then access other information.
5. Our database receives an _____ every morning at 3 AM.
6. Ordinarily users respond by dismissing a _____ through the "close" or "cancel" feature of the window hosting the it.
7. The _____ allows the user to enter a URL or IP address of the page they want to visit or save that page for later.
8. _____ considerations, such as who the users are and their experience with similar systems must be examined.
9. The simplest and earliest versions of the _____ can be set to watch for particular words in the subject line of messages and to exclude these from the user's inbox.
10. All of our products are available for _____ on our website.

Exercise 5. ***Match the verbs and the nouns. Sometimes, more than one option is possible.***

1. bypass	**a.** updates
2. execute	**b.** security controls
3. strengthen	**c.** a task
4. accomplish	**d.** a script
5. automate	**e.** security

Unit 10

Staying safe on social networking sites

Although the features of social networking sites may differ, they all allow you to provide information about yourself and offer some type of communication mechanism (forums, chat rooms, email, instant messenger) that enables you to connect with other users. On some sites, you can browse for people based on certain criteria, while other sites require that you be "introduced" to new people through a connection you share. Many of the sites have communities or subgroups that may be based on a particular interest. While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of personal information that's available.

How can you protect yourself?

•Limit the amount of personal information you post - Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be

comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.

•Remember that the Internet is a public resource - Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove the information from a site, saved or cached versions may still exist on other people's machines.

•Evaluate your settings - Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so don't post anything that you wouldn't want the public to see. Sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.

•Be wary of third-party applications - Third-party applications may provide entertainment or functionality, but use caution when deciding which applications to enable. Avoid applications that seem suspicious, and modify your settings to limit the amount of information the applications can access.

•Use strong passwords - Protect your account with passwords that cannot easily be guessed. If your password is compromised, someone else may be able to access your account and pretend to be you.

•Check privacy policies - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join.

•Keep software, particularly your web browser, up to date - Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.

•Use and maintain anti-virus software - Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage. Because attackers are continually writing new viruses, it is important to keep your definitions up to date.

Regardless of how restrictive you make your security settings, they may not offer complete privacy. An attacker or application may take advantage of software vulnerabilities, or another user may repost your information. When using social networking services, be responsible and always consider the risks. Operate as if all of the content is public, and only post information you would be comfortable sharing with other people.

Exercise 1. ***Answer the questions using the information from the text.***

1. What are the purposes of social networking sites?

2. What can be referred to social networking sites?
3. Is there any type of information that makes you vulnerable? Give examples.
4. How can the information remain online if you remove it?
5. In what way you may customize your settings at different sites?
6. Why should you be wary of third-party applications?
7. How do spammers get your address?
8. Why is it so important to keep web browser and anti-virus software up to date?
9. What does 'being responsible' when using social networking services mean?

Exercise 2. ***True or false?***

1. A dependent password is enough to protect your data over social networking sites.
2. The best policy to remain safe is not to post any private information.
3. If you keep an eye on anti-virus updates you are totally protected.
4. Most social networks unintentionally share your data with spammers.
5. No information posted on social media sites can totally be retrieved.

Exercise 3. ***Write a short summary of the text.***

Exercise 4. ***Use the words and expressions from the box to complete the sentences.***

customize	referral	functionality	default settings
third-party applications	restrictive	security settings	cached version

1. Sign in to see if your _____ are up to date.
2. The online service Backupurl offers another way to create a _____ of a website.
3. To _____ means to specify options related to user interface.
4. _____ can be standalone programs or they can be small plugins that add functionality to an existing parent program.
5. Controls of a computer hardware or software (or of a device, equipment, or machine) as preset by its manufacturer. Some types of _____ may be altered or customized by the user.
6. A unique number assigned to your account is called _____ code.
7. The effective implementation of _____ measures can reinforce cyber security.
8. _____ testing refers to whether the software does what it supposed to do. Usability testing refers to whether the design of the

software (especially the User Interface), the behaviour and the User Interaction make sense.

Exercise 5. ***Find synonyms.***

1. connection	**a.** modernisation
2. community	**b.** description
3. profile	**c.** relation
4. update	**d.** subgroup
5. definition	**e.** warning
6. caution	**f.** account

Literature

1. Alexander Adamov, «Computer Threats: Methods of Detection and Analysis», Kaspersky Lab, Moscow 2009.
2. Infosecurity Magazine: Phishing and the economics of e-crime, Sep 2007.
3. C. Zou, L. Gao, W. Gong, and D. Towsley, “Monitoring and early warning of Internet worms,” in ACM Conference on Computer and Communications Security (CCS’03), 2003.
4. M. Rajab, F. Monrose, and A. Terzis, “Fast and evasive attacks: Highlighting the challenges ahead,” in 9th International Symposium on Recent Advances in Intrusion Detection (RAID’04), 2006.
5. www.wikipedia.com
6. www.securelist.com, «Examples and Descriptions of Various Common Vulnerabilities», Encyclopaedia.
7. www.securelist.com, «Skype and Corporate Network Security», Infowatch, SecurityLab.ru, 4.04.2007.
8. http://searchsecurity.techtarget.com

УНИВЕРСИТЕТ ИТМО

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА ИНОСТРАННЫХ ЯЗЫКОВ

Объединенная кафедра иностранных языков, являющаяся подразделением Института Международного Развития и Партнерства, с 2015 года получила возможность - в частности, в рамках программы 5-100 - реализовать программы коммуникативного курса английского языка. Количество часов, предусмотренное для изучения иностранных языков, было увеличено в несколько раз, массово внедряются современные учебные материалы и пособия. В 2014-2015 учебном году процесс затронул только ряд факультетов, а в 2015-2016 распространился уже на всех студентов бакалавриата.

Студенты получили возможность изучать английский язык в большом объеме и по самым продвинутым методикам. Это потребовало от преподавателей дополнительной подготовки и переподготовки по коммуникативным методикам. В результате кафедра вышла на новый уровень образовательной деятельности, которая охватывает не только студентов бакалавриата, но и магистратуры и аспирантуры. Для аспирантов был введен новый курс делового английского языка, по-новому строится курс английского языка для специальных целей, создана Лаборатория Академического Письма, готовятся электронные образовательные платформы и ресурсы.

Безусловно, английский язык занимает главное место в сфере образовательной деятельности кафедры, но немецкий и французский языки также преподаются на высоком профессиональном уровне, и при небольшом количестве студентов подготавливаются элитные кадры, владеющие несколькими иностранными языками.

Каждое из направлений работы открывает перед кафедрой новые горизонты, требует постоянного совершенствования методической и практической подготовки преподавателей, делает работу преподавателей и сотрудников творческой, привлекает на кафедру новые кадры. Кафедра иностранных языков готова ответить на любые запросы Университета – у нее есть все возможности, ресурсы и кадры для того, чтобы предложить самые современные решения.

Сомко Анна Сергеевна
Федорова Екатерина Андреевна

Профессиональный иностранный язык для специалистов в области компьютерной безопасности

Учебно-методическое пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ № 3697
Тираж 100
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49