Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ПОЛІТЕХНІКА»

Кафедра іноземних мов

МЕТОДИЧНІ ВКАЗІВКИ ДО ПРАКТИЧНИХ ЗАНЯТЬ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНОЗЕМНА МОВА» ДЛЯ ЗДОБУВАЧІВ ПЕРШОГО (БАКАЛАВРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ ДЕННОЇ ТА ЗАОЧНОЇ ФОРМИ НАВЧАННЯ, ЗА СПЕЦІАЛЬНІСТЮ F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Одеса
Одеська політехніка
2026

Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ПОЛІТЕХНІКА»

Кафедра іноземних мов

МЕТОДИЧНІ ВКАЗІВКИ ДО ПРАКТИЧНИХ ЗАНЯТЬ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНОЗЕМНА МОВА» ДЛЯ ЗДОБУВАЧІВ ПЕРШОГО (БАКАЛАВРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ ДЕННОЇ ТА ЗАОЧНОЇ ФОРМИ НАВЧАННЯ, ЗА СПЕЦІАЛЬНІСТЮ F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

для студентів І курсу

Затверджено
на засіданні кафедри
іноземних мов
Протокол № 5
від 9 січня 2026

Одеса
Одеська політехніка
2026

Методичні вказівки до практичних занять з навчальної дисципліни «Іноземна мова» для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форми навчання, за спеціальністю F5 Кібербезпека та захист інформації для студентів І курсу / Укл., Є.Б. Гродська, О.В. Гвоздь, О.В. Лебедєва - О. Одеська політехніка: 2026.- 47 с.

Укладачі: **Є. Б. Гродська,** кандидат філол. наук, доцент
О.В. Гвоздь, ст.викладач
О.В. Лебедєва, ст.викладач

ЗМІСТ

Передмова.....5
Lesson 1.....6
Lesson 2.....8
Lesson 3.....11
Lesson 5.....17
Lesson 6.....20
Lesson 7.....22
Lesson 8.....24
Lesson 9.....27
Lesson 10.....29
Lesson 11.....32
Lesson 12.....35
Lesson 13.....38
Lesson 14.....41
Lesson 15.....43

Передмова

Методичні вказівки до практичних занять з навчальної дисципліни «Іноземна мова» для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форми навчання, призначені для здобувачів І рівня вищої освіти, спеціальності 125 Кібербезпека та захист інформації.

Метою методичних вказівок є взаємозв'язане формування у здобувачів вмінь та навичок в різних видах мовної комунікації (читання, письма та говоріння англійською мовою) відповідно до Програми за тематикою включених напрямків.

За рахунок тренування в читанні текстів і виконання завдань комунікативного характеру здобувачі підвищують рівень практичного володіння англійською мовою за напрямком з рівня В1 до рівня В2 (за критеріями Документа Ради Європи «Загальноєвропейські компетенції володіння іноземною мовою: Вивчення, викладання, оцінка» - CEFR), що дає можливість: вільно читати оригінальну літературу іноземною мовою у відповідній галузі знань; оформляти витягнуту з іноземних джерел інформацію у вигляді перекладу або резюме; робити повідомлення і доповіді іноземною мовою на теми, пов'язані з науковою роботою майбутнього фахівця; вести бесіду за напрямком.

Методичні вказівки містять 15 основних цикли (Lessons), об єднаних за тематикою вказаних напрямків і є ідентичними у структурному відношенні. Цикли складаються з 15 автентичних текстів та комплексу мовних вправ, які розраховані на удосконалення навичок активізації словарного і грамматичного мінімуму професійного спрямування.

Автори.

Lesson 1

Мета заняття: Мета заняття: вміти знаходити необхідну інформацію в технічній літературі, наукових базах даних та інших джерелах інформації, критично оцінювати і аналізувати її.

What is cybersecurity all about?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users through ransomware; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

A successful cybersecurity posture has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, a unified threat management gateway system can automate integrations across products and accelerate key security operations functions: detection, investigation, and remediation. People, processes, and technology must all complement one another to create an effective defense from cyberattacks. Users must understand and comply with basic data protection and privacy security principles like choosing strong passwords, being wary of attachments in email, and backing up data. Organizations must have a framework for how they deal with both attempted and successful cyberattacks. Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyberattacks. Three main entities must be protected: endpoint devices like computers, smart devices, and routers; networks; and the cloud.

Why is cybersecurity important? In today's connected world, everyone benefits from advanced cybersecurity solutions. At an individual level, a cybersecurity attack can result in everything from identity theft to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

Everyone also benefits from the work of cyberthreat researchers, like the team of 250 threat researchers at Talos, who investigate new and emerging threats and cyberattack strategies. They reveal new vulnerabilities, educate the public on the importance of cybersecurity, and strengthen open-source tools. Their work makes the internet safer for everyone.

Best practices for cybersecurity

Adopting best practices for cybersecurity can significantly reduce the risk of cyberattacks.

1. Regular software and operating system updates
   Updating software and operating systems regularly helps to patch vulnerabilities and enhance security measures against potential threats.
2. Using strong and unique passwords
   Creating strong and unique passwords for each online account can enhance cybersecurity, as cyberattacks often exploit weak or stolen passwords.
3. Implementing multi-factor authentication (MFA)
   Multi-factor authentication involves multiple identification forms before account access, reducing the risk of unauthorized access.

Following these practices enhances cybersecurity and protects digital assets. It's vital to stay vigilant and informed about the latest threats and security measures to stay ahead of cybercriminals.

Exercise 1. Read and memorize using a dictionary:

to be aimed at, extorting money, ransomware, challenging, multiple layers of protection, to accelerate, detection, remediation, to complement, to be wary of, entity, to reveal, vulnerability, significantly, to patch, to enhance, to exploit, assets, vigilant.

Exercise 2. Make up 5 sentences with new words.

Exercise 3. Answer the questions:

1. What is cybersecurity, and what types of digital attacks does it aim to prevent?
2. Why is implementing effective cybersecurity measures particularly challenging today?
3. What are the main goals of cyberattacks such as ransomware and other malicious activities?
4. What elements must work together in an organization to create an effective defense against cyberattacks?
5. Which three main entities must be protected to ensure strong cybersecurity?
6. Why is cybersecurity important for both individuals and critical infrastructure in today's connected world?
7. What are three best practices that can significantly reduce the risk of cyberattacks?

Exercise 4. Match the left part with the right:

A	B
1.Cybersecurity is the practice of protecting systems, networks, and programs	A. sensitive information and extorting money through ransomware.
2. Cyberattacks often aim at accessing or destroying	B. from digital attacks.
3. A successful cybersecurity posture has multiple layers of protection	C. choosing strong passwords and being cautious with email attachments.
4. Users must follow basic data protection principles such as	D. to deal with attempted and successful cyberattacks.
5. Organizations need a framework	E. reduce the risk of unauthorized access.
6. Three main entities that must be protected are	F. endpoint devices, networks, and the cloud.
7. Multi-factor authentication helps	G. across computers, networks, programs, and data.

Exercise 5. Exercise 5. Fill in the gaps with the suggested words:

wary comply essential routers attempted entities protect

Users must understand and 1. _____ with basic data protection and privacy security principles like choosing strong passwords, being 2. _____ of attachments in email, and backing up data. Organizations must have a framework for how they deal with both 3. _____ and successful cyberattacks. Technology is 4. _____ to giving organizations and individuals the computer security tools needed to 5._____ themselves from cyberattacks. Three main 6._____ must be protected: endpoint devices like computers, smart devices, and 7._____; networks; and the cloud.

Exercise 6. Compose a story on one of the topics (up to 100 words):

1. Cybersecurity.

2. Best practices for cybersecurity

Lesson 2

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

Cyber safety tips

In today's digital age, cybersecurity is a critical field that protects data, networks, and systems from malicious attacks. For IT students, gaining a solid foundation in cybersecurity is not just beneficial but essential. As cyber threats become more sophisticated, the demand for skilled cybersecurity professionals continues to grow.

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security.

The term "cybersecurity" applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- **Information security** protects the integrity and privacy of data, both in storage and in transit.
- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Cyber safety tips - protect yourself against cyberattacks

How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

1. **Update your software and operating system:** This means you benefit from the latest security patches.
2. **Use anti-virus software:** Security solutions like Kaspersky Premium will detect and removes threats. Keep your software updated for the best level of protection.
3. **Use strong passwords:** Ensure your passwords are not easily guessable.
4. **Do not open email attachments from unknown senders:** These could be infected with malware.
5. **Do not click on links in emails from unknown senders or unfamiliar websites:** This is a common way that malware is spread.
6. **Avoid using unsecure WiFi networks in public places:** Unsecure networks leave you vulnerable to man-in-the-middle attacks.

Exercise 1. Read and memorize using a dictionary:

beneficial, sophisticated, malicious, intruder, targeted attacker, opportunistic malware, application security, compromised application, to be deployed, operating capacity, accidentally, otherwise, suspicious, to plug in, security patches, to be not easily guessable, vulnerable.

Exercise 2. Make up 5 sentences with new words.

Exercise 3. Answer the questions:

1. Why is gaining a solid foundation in cybersecurity essential for IT students in today's digital age?
2. What is cybersecurity, and what types of devices and systems does it protect?
3. What is network security, and what kinds of threats does it defend against?
4. How does application security help protect data before a program or device is deployed?
5. What is the difference between disaster recovery and business continuity in cybersecurity?
6. Why is end-user education considered a vital part of cybersecurity?
7. What are three cyber safety tips that help individuals and businesses protect themselves against cyberattacks?

Exercise 4. Match the left part with the right:

A	B
1. Network security	A. Focuses on protecting the integrity and privacy of data in storage and transit.
2. Application security	B. Helps prevent unauthorized access by making accounts difficult to guess
3. Information security	C. Secures a computer network from intruders and malware.
4. Disaster recovery	D. Restores operations and data after a cybersecurity incident.
5. End-user education	E. Protects users from man-in-the-middle attacks.
6. Using strong passwords	F. Keeps software and devices free from threats, starting at the design stage.
7. Avoiding unsecure public WiFi	G. Teaches people not to open suspicious attachments or use unknown USB drives.

Exercise 5. Fill in the gaps with the suggested words:

attachments software vulnerable guessable patches malware detect

Here are our top cyber safety tips:

1. Update your 1. _____and operating system: This means you benefit from the latest security2. _____.
2. Use anti-virus software: Security solutions like Kaspersky Premium will 3. _____ and removes threats. Keep your software updated for the best level of protection.
3. Use strong passwords: Ensure your passwords are not easily4. _____.
4. Do not open email 5. _____from unknown senders: These could be infected with malware.

5. Do not click on links in emails from unknown senders or unfamiliar websites: This is a common way that 6. _____is spread.
6. Avoid using unsecure WiFi networks in public places: Unsecure networks leave you 7. _____ to man-in-the-middle attacks.

Exercise 6. Compose a story on one of the topics (up to 100 words):

1. Why is cybersecurity important?
2. Essential cyber safety tips

Lesson 3

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

Types of cybersecurity threats

Cloud security

Cloud security provides rapid threat detection and remediation, enhancing visibility and intelligence to prevent malware impacts. It delivers robust protection in multicloud environments, streamlining security without affecting user productivity, and is essential for the safety of applications, data, and users in both hybrid and remote work settings. The scalable nature of cloud security allows for the defense of an expanding array of users, devices, and cloud applications, ensuring comprehensive coverage across all points of potential attack.

Identity security and access management involve safeguarding the digital identities of individuals, devices, and organizations. This involves implementing security processes, tools, and policies that control user access to accounts and enable productivity with frictionless access to important information without risk.

The three main goals of identity security are to:

- Authenticate a user's identity
- Authorize access to appropriate resources
- Monitor access activity for weak posture and suspicious activity

Malware

Malware is a type of software designed to gain unauthorized access or to cause damage to a computer.

Phishing

Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data, such as credit card numbers and login information, and is the most common type of cyberattack. You can help protect yourself through education or a technology solution that filters malicious emails.

Ransomware

Ransomware is a type of malicious software that is designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered or the system restored.

Social engineering

Social engineering is a tactic that adversaries use to trick you into revealing sensitive information. Attackers can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats mentioned above to make you more likely to click on links, download malware, or trust a malicious source.

Threat detection

An effective extended detection and response (XDR) system integrates solutions across the security stack, making it easier for analysts to focus on comprehensive threat detection, prioritize incident response, and improve productivity. With more visibility and context into data security threats, events that would not have been addressed before will surface to a higher level of awareness, thus allowing cybersecurity teams to quickly eliminate any further impact and reduce the severity and scope of the attack.

Zero trust

Zero trust isn't a single product or technology. It's a security strategy that is best implemented by keeping an organization's business operations, risks, and security outcomes in mind. Although there are various paths to achieving zero trust maturity, most organizations prioritize deployment of technologies such as multi-factor authentication (MFA), device posture checks, zero trust network access (ZTNA), and network segmentation as they implement zero-trust security.

Exercise 1. Read and memorize using a dictionary:

remediation, robust, streamlining, scalable, expanding array, implementing, weak posture, suspicious activity, malware, fraudulent, to resemble, ransomware, to extort, ransom, to solicit, to eliminate, severity.

Exercise 2. Make up 5 sentences with new words.

Exercise 3. Answer the questions:

1. What benefits does cloud security provide in terms of threat detection, remediation, and user productivity?
2. Why is cloud security especially important in multicloud, hybrid, and remote work environments?
3. What is identity security and access management, and what does it aim to protect?
4. What are the three main goals of identity security related to user access?
5. What is malware, and what kind of harm is it designed to cause?
6. How does phishing work, and what methods can help protect users from phishing attacks?
7. What is the zero trust security strategy, and which technologies are commonly prioritized when implementing it?

Exercise 4. Match the left part with the right:

A	B
Cloud security	A. A security strategy that assumes no user or device is automatically trusted and often includes MFA and network segmentation.
Identity security and access management	B. Fraudulent emails designed to steal sensitive information such as login credentials or credit card numbers.
Malware	C. Software created to gain unauthorized access or damage a computer system.
Phishing	D. Protection that provides threat detection and safeguards applications, data, and users in cloud environments.
Ransomware	E. A type of malicious software that blocks access to files until money is paid.
Social engineering	F. A tactic used to trick people into revealing confidential information or making payments.
Zero trust	G. Processes and policies that control user access and protect digital identities.

Exercise 5. Fill in the gaps with the suggested words:

array	impacts	threat	robust	enhancing	comprehensive	essential

Cloud security provides rapid 1. _____ detection and remediation, 2. ---------- visibility and intelligence to prevent malware3. ----------. It delivers 4. ---------- protection in multicloud environments, streamlining security without affecting user productivity, and is 5. ---------- for the safety of applications, data, and users in both hybrid and remote work settings. The scalable nature of cloud security allows for the defense of an expanding 6. ---------- of users, devices, and cloud applications, ensuring 7. ---------- coverage across all points of potential attack.

Exercise 6. Compose a story on one of the topics (up to 100 words):

1. Cybersecurity threats
2. Main types of threats

Lesson 4

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

What is the CIA Triad? Confidentiality

The CIA Triad is a model designed to guide information and network security policies within an organization.

The three components of the triad—Confidentiality, Integrity, and Availability—are the essential objectives that organizations must prioritize when designing, implementing, and managing security systems, networks, and policies. Let's define each of these components:

Confidentiality: Ensuring that sensitive data is accessed only by authorized individuals or systems.

Integrity: Ensuring data remains accurate, consistent, and unaltered during transmission or storage.

Availability: Ensuring data and network resources are accessible to authorized users when needed.

These objectives work together to form a comprehensive approach to securing information systems, ensuring that data is protected from unauthorized access, unintentional or malicious alterations, and disruptions that could lead to downtime.

Why is the CIA Triad Important?

In today's digital age, organizations rely heavily on data to run their operations. From personal data to financial records, sensitive business information, and intellectual property, data is a critical asset that needs constant protection.

The CIA Triad serves as a framework to ensure that data is adequately protected across all dimensions:

Confidentiality prevents unauthorized access.

Integrity prevents unauthorized alterations.

Availability ensures access when needed.

Focusing on only one or two of these aspects can lead to vulnerabilities.

For example, a system with strong confidentiality but no availability controls could suffer from downtime, making it unusable for legitimate users.

Similarly, a system with high availability but poor confidentiality could expose sensitive data to unauthorized parties. Let's examine each element of the CIA Triad to understand how it contributes to network security.

Confidentiality

Confidentiality is the principle of ensuring that information is accessible only to those who are authorized to view it.

In other words, confidential information should remain hidden from unauthorized users while being available to those who require access to it for legitimate purposes.

Confidentiality is often associated with privacy, as it focuses on protecting personal, sensitive, or classified information from being disclosed to unauthorized individuals or entities.

Whether transmitting data over a network or storing it in a database, maintaining confidentiality is crucial to prevent hackers, eavesdroppers, or malicious insiders from accessing that data.

Common Threats to Confidentiality

Eavesdropping: Attackers intercept communication channels (e.g., Wi-Fi networks or phone calls) to monitor sensitive conversations or data transmissions.

Insider Threats: Employees or contractors with legitimate access may misuse their privileges to access and steal confidential data.

Phishing: Attackers trick users into revealing sensitive information through fake emails or websites, such as login credentials or personal details.

Best Practices for Ensuring Confidentiality

Use strong encryption for sensitive data both in transit and at rest.

Implement robust access control mechanisms, including multi-factor authentication.

Regularly audit user access levels to ensure only authorized individuals can access sensitive data.

Educate staff on the dangers of phishing and social engineering attacks.

Exercise 1. Read and memorize using a dictionary:

unaltered, to be accessible to, comprehensive approach, malicious alterations, disruption, to expose, to contribute, to remain, crucial, insider, eavesdropper, credential.

Exercise 2. Make up 5 sentences with new words.

Exercise 3. Answer the questions:

1. What is the CIA Triad, and what is its purpose in information and network security?
2. What are the three core components of the CIA Triad?
3. How does confidentiality contribute to protecting sensitive information within an organization?
4. Why is it risky for an organization to focus on only one or two elements of the CIA Triad?
5. What are some common threats to confidentiality mentioned in the text?
6. How can encryption and access control mechanisms help ensure confidentiality?
7. Why is staff education important in preventing threats such as phishing and social engineering?

Exercise 4. Match the left part with the right:

A	B
Confidentiality	A. Ensures that data and network resources are accessible to authorized users when needed.
Integrity	B. A model that guides information and network security policies within an organization.
Availability	C. Protects information from being accessed by unauthorized individuals.
CIA Triad	D. A security measure that requires more than one method of verification to access systems.
Eavesdropping	E. Ensures that data remains accurate, consistent, and unaltered.

Insider Threats	F. Occurs when attackers intercept communication channels to monitor sensitive data.
Multi-factor authentication	G. Happens when employees misuse their legitimate access to steal confidential information.

Exercise 5. Fill in the gaps with the suggested words:

privacy	require	eavesdroppers	remain	crucial	unauthorized	accessible

Confidentiality is the principle of ensuring that information is 1. _____ only to those who are authorized to view it. In other words, confidential information should 2. _____ hidden from unauthorized users while being available to those who 3. _____access to it for legitimate purposes.

Confidentiality is often associated with 4. _____, as it focuses on protecting personal, sensitive, or classified information from being disclosed to 5._____ individuals or entities.

Whether transmitting data over a network or storing it in a database, maintaining confidentiality is 6. _____ to prevent hackers, 7. _____, or malicious insiders from accessing that data.

Exercise 6. Compose a story on one of the topics (up to 100 words):

1. The CIA Triad
2. Common Threats to Confidentiality

Lesson 5

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

What is the CIA Triad? Integrity and Availability

Integrity refers to the accuracy and trustworthiness of data. It ensures that information remains unaltered during transmission, storage, or processing, except by authorized individuals or systems.

Data integrity guarantees that the information received is strictly as intended, without any unauthorized modifications, deletions, or additions.

Maintaining data integrity is critical in finance, healthcare, and government industries, where data accuracy is paramount.

Any corruption or unauthorized modification of data could have severe consequences, including financial losses, legal penalties, or threats to public safety.

Common Threats to Integrity

Man-in-the-Middle (MitM) Attacks: Attackers intercept and modify communication between two parties without their knowledge.

Malware: Malicious software can alter or corrupt files, leading to data integrity issues.

Data Corruption: Hardware failures, software bugs, or transmission errors can unintentionally corrupt data.

Best Practices for Ensuring Integrity

Use cryptographic hash functions (e.g., SHA-2) to verify data integrity.

Employ digital signatures for essential communications and transactions.

Implement regular data backups and audits to identify and recover from integrity breaches.

Deploy malware detection systems to prevent unauthorized modifications to data.

Availability ensures authorized users have reliable and timely access to systems, networks, and data when needed.

This component of the CIA Triad is crucial for maintaining business continuity, as downtime or unavailability of critical systems can lead to financial losses, reputational damage, and operational disruptions.

Availability ensures that a system's hardware and software components function correctly and can handle both anticipated and unexpected loads.

In addition, mechanisms must be in place to prevent and mitigate potential threats to availability, such as distributed denial-of-service (DDoS) attacks, hardware failures, or natural disasters.

Common Threats to Availability

DoS (Denial of Service) and DDoS (Distributed Denial of Service) Attacks: Attackers flood a network or system with excessive traffic, rendering it unavailable to legitimate users.

Hardware Failures: Physical components, such as servers or storage devices, may fail, causing service unavailability.

Natural Disasters: Events such as fires, floods, or earthquakes can damage infrastructure, resulting in prolonged downtime.

Best Practices for Ensuring Availability

Regularly maintain and update hardware and software systems to prevent failures.
Implement redundancy and failover mechanisms to ensure continuous operation during failures.
Use load balancers and traffic management tools to handle high-traffic situations.
Develop and rehearse disaster recovery plans to minimize downtime in case of emergencies.
The CIATriad—Confidentiality, Integrity, and Availability—forms the foundation of any comprehensive cybersecurity strategy.
By focusing on these three critical objectives, organizations can ensure that their networks, systems, and data remain secure, accurate, and available to authorized users.
Failing to uphold these principles can lead to devastating consequences, including data breaches, financial losses, legal issues, and reputational damage.

Exercise 1. Read and memorize using a dictionary:

deletion, paramount, severe consequences, penalties, intercept, unintentionally, hash functions, deploy, anticipated, to mitigate, to render, failover mechanisms, rehearse, data breaches.

Exercise 2. Make up 5 sentences with new words.

Exercise 3. Answer the questions:

1. What does integrity mean in the context of information security?
2. Why is maintaining data integrity especially critical in industries such as finance, healthcare, and government?
3. What are some common threats that can compromise data integrity?
4. How do cryptographic hash functions and digital signatures help ensure data integrity?
5. What does availability guarantee within the CIA Triad framework?
6. What are the main threats to availability mentioned in the text?
7. Why can failing to uphold confidentiality, integrity, and availability lead to severe consequences for organizations?

Exercise 4. Match the left part with the right:

A	B
Integrity	A. A method used to verify that data has not been altered by generating a unique digital fingerprint.
Man-in-the-Middle (MitM) attack	B. Ensures that systems and data are accessible to authorized users when needed.
Cryptographic hash function	C. Occurs when attackers intercept and modify communication between two parties.
Availability	D. The accuracy and trustworthiness of data during storage, transmission, and processing.
DDoS attack	E. A situation where physical components such as servers stop functioning, causing downtime.
Redundancy and failover mechanisms	F. A strategy that provides backup systems to maintain continuous operation during failures.

Hardware failure	G. An attack that floods a system or network with excessive traffic to make it unavailable.

Exercise 5. Fill in the gaps with the suggested words:

severe	refers	paramount	deletions	penalties	unaltered	strictly

Integrity 1. _____ to the accuracy and trustworthiness of data. It ensures that information remains 2. _____ during transmission, storage, or processing, 3. _____ by authorized individuals or systems.

Data integrity guarantees that the information received is 3. _____ as intended, without any unauthorized modifications, 4. _____, or additions.

Maintaining data integrity is critical in finance, healthcare, and government industries, where data accuracy is 5. _____.

Any corruption or unauthorized modification of data could have 6. _____ consequences, including financial losses, legal 7. _____ , or threats to public safety.

Exercise 6. Compose a story on one of the topics (up to 100 words):

1. Common Threats to Integrity
2. Common Threats to Availability

Lesson 6

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

BASIC PRINCIPLES OF INFORMATION PROTECTION

General Observations. As computers become better understood and more economical, every day brings new applications. Many of these new applications involve both storing information and simultaneous use by several individuals. The key concern in this paper is multiple use. For those applications in which all users should not have identical authority, some scheme is needed to ensure that the computer system implements the desired authority structure.

For example, in an airline seat reservation system, a reservation agent might have authority to make reservations and to cancel reservations for people whose names he can supply. A flight boarding agent might have the additional authority to print out the list of all passengers who hold reservations on the flights for which he is responsible. The airline might wish to withhold from the reservation agent the authority to print out a list of reservations, so as to be sure that a request for a passenger list from a law enforcement agency is reviewed by the correct level of management.

The airline example is one of protection of corporate information for corporate self-protection (or public interest, depending on one's view). A different kind of example is an online warehouse inventory management system that generates reports about the current status of the inventory. These reports not only represent corporate information that must be protected from release outside the company, but also may indicate the quality of the job being done by the warehouse manager. In order to preserve his personal privacy, it may be appropriate to restrict the access to such reports, even within the company, to those who have a legitimate reason to be judging the quality of the warehouse manager's work.

Many other examples of systems requiring protection of information are encountered every day: credit bureau data banks; law enforcement information systems; time-sharing service bureaus; on-line medical information systems; and government social service data processing systems. These examples span a wide range of needs for organizational and personal privacy. All have in common controlled sharing of information among multiple users. All, therefore, require some plan to ensure that the computer system helps implement the correct authority structure. Of course, in some applications no special provisions in the computer system are necessary. It may be, for instance, that an externally administered code of ethics or a lack of knowledge about computers adequately protects the stored information. Although there are situations in which the computer need provide no aids to ensure protection of information, often it is appropriate to have the computer enforce a desired authority structure.

The words "privacy," "security," and "protection" are frequently used in connection with information-storing systems. Not all authors use these terms in the same way. This paper uses definitions commonly encountered in computer science literature.

The term "privacy" denotes a socially defined ability of an individual (or organization) to determine whether, when, and to whom personal (or organizational) information is to be released.

This paper will not be explicitly concerned with privacy, but instead with the mechanisms used to help achieve it.

Exercise 1. Read and memorize using a dictionary:

authority, key concern, simultaneous, application, multiple use, to implement, to withhold, to preserve, privacy, security, to restrict the access, processing systems, provision, to denote, to encounter

Exercise 2. Make up 5 sentences with new words.

Exercise 3. Answer the questions:

1) What do many of new applications involve?
2) What examples of protection of information are there in the text?
3) What do all these examples have in common?
4) What words are frequently used in connection with information-storing systems?
5) What does the term “privacy” denote?

Exercise 4. Match the left part with the right:

1 The words "privacy," "security," and "protection" are frequently	a) a socially defined ability of an individual (or organization) to determine whether, when, and to whom personal (or organizational) information is to be released.
2. The term "privacy" denotes	b) definitions commonly encountered in computer science literature.
3. This paper uses	c) used in connection with information-storing systems.
4. Not all authors use these terms	d) in the same way.

Exercise 5. Fill in the gaps with the suggested words:

authority, ensure, which, several , involve, become, new

As computers_____ better understood and more economical, every day brings _____applications. Many of these new applications_____ both storing information and simultaneous use by_____ individuals. The key concern in this paper is multiple use. For those applications in_____ all users should not have identical authority, some scheme is needed to_____ that the computer system implements the desired_____ structure.

Exercise 6. Compose a story on one of the topics (up to 100 words):

1. Principles of information protection
2. Concept of “Privacy”

Lesson 7

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

Foundations of Computer Security

The term "security" describes techniques that control who may use or modify the computer or the information contained in it.

Security specialists have found it useful to place potential security violations in three categories.

1) Unauthorized information release: an unauthorized person is able to read and take advantage of information stored in the computer. This category of concern sometimes extends to "traffic analysis," in which the intruder observes only the patterns of information use and from those patterns can infer some information content. It also includes unauthorized use of a proprietary program.

2) Unauthorized information modification: an unauthorized person is able to make changes in stored information - a form of sabotage. Note that this kind of violation does not require that the intruder see the information he has changed.

3) Unauthorized denial of use: an intruder can prevent an authorized user from referring to or modifying information, even though the intruder may not be able to refer to or modify the information. Causing a system "crash," disrupting a scheduling algorithm, or firing a bullet into a computer are examples of denial of use. This is another form of sabotage.

The term "unauthorized" in the three categories listed above means that release, modification, or denial of use occurs contrary to the desire of the person who controls the information, possibly even contrary to the constraints supposedly enforced by the system. The biggest complication in a general-purpose remote-accessed computer system is that the "intruder" in these definitions may be an otherwise legitimate user of the computer system.

Examples of security techniques sometimes applied to computer systems are the following:

1. labeling files with lists of authorized users,
2. verifying the identity of a prospective user by demanding a password,
3. shielding the computer to prevent interception and subsequent interpretation of electromagnetic radiation,
4. enciphering information sent over telephone lines,
5. locking the room containing the computer,
6. controlling who is allowed to make changes to the computer system (both its hardware and software),
7. using redundant circuits or programmed cross-checks that maintain security in the face of hardware or software failures,
8. certifying that the hardware and software are actually implemented as intended.

It is apparent that a wide range of considerations are pertinent to the engineering of security of information. Historically, the literature of computer systems has more narrowly defined the term *protection* to be just those security techniques that control the access of executing programs to stored information. An example of a protection technique is labeling of computer-stored files with lists of authorized users. Similarly, the term *authentication* is used for those security techniques that verify the identity of a person (or another external agent) making a request of a computer system. An example of an authentication technique is demanding a password. This paper concentrates on protection and authentication mechanisms, with only occasional reference to the other equally necessary security mechanisms. One should recognize that concentration on

protection and authentication mechanisms provides a narrow view of information security, and that a narrow view is dangerous. The objective of a secure system is to prevent all unauthorized use of information, a negative kind of requirement. It is hard to prove that this negative requirement has been achieved, for one must demonstrate that every possible threat has been anticipated. Thus, an expansive view of the problem is most appropriate to help ensure that no gaps appear in the strategy. In contrast, a narrow concentration on protection mechanisms, especially those logically impossible to defeat, may lead to false confidence in the system as a whole.

Exercise 1. Read and memorize using a dictionary:

Technique, to modify, security violation, unauthorized, to take advantage of, intruder, to infer, proprietary program, to prevent, denial, contrary to, supposedly, to verify, to shield, to encipher, redundant, circuit, objective, authentication, threat, remote-access system

Exercise 2. Answer the questions:

1) What categories of potential security violations are there?
2) What does the term “security describe”?
3) What is “traffic analysis”?
4) What does the term “unauthorized” mean?
5) What examples of security techniques are listed in the text?

Exercise 3. Match the left part with the right:

1 An example of an authentication technique is	a) labeling of computer-stored files with lists of authorized users.
2. The objective of a secure system is	b) those security techniques that verify the identity of a person (or other external agent) making a request of a computer system.
3. An example of a protection technique is	c) demanding a password.
4. Similarly, the term *authentication* is used for	d) to prevent all unauthorized use of information, a negative kind of requirement.

Exercise 4. Fill in the gaps with the suggested words:

infer, analysis, unauthorized, stored, person

Unauthorized information release: an unauthorized_____ is able to read and take advantage of information _____in the computer. This category of concern sometimes extends to "traffic_____," in which the intruder observes only the patterns of information use and from those patterns can_____ some information content. It also includes_____ use of a proprietary program.

Exercise 5. Compose a story on one of the topics (up to 100 words):

1) Potential security violations

2) Various security techniques

Lesson 8

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

Functional Levels of Information Protection

Many different designs have been proposed and mechanisms implemented for protecting information in computer systems. One reason for differences among protection schemes is their different functional properties - the kinds of access control that can be expressed naturally and enforced. It is convenient to divide protection schemes according to their functional properties. A rough categorization is the following.

a) Unprotected systems: Some systems have no provision for preventing a determined user from having access to every piece of information stored in the system. Although these systems are not directly of interest here, they are worth mentioning since, as of 1975, many of the most widely used, commercially available batch data processing systems fall into this category - for example, the Disk Operating System for the IBM System 370. Our definition of protection, which excludes features usable only for mistake prevention, is important here since it is common for unprotected systems to contain a variety of mistake-prevention features. These may provide just enough control that any breach of control is likely to be the result of a deliberate act rather than an accident. Nevertheless, it would be a mistake to claim that such systems provide any security.

b) All-or-nothing systems: These are systems that provide isolation of users, sometimes moderated by total sharing of some pieces of information. If only isolation is provided, the user of such a system might just as well be using his own private computer, as far as protection and sharing of information are concerned. More commonly, such systems also have public libraries to which every user may have access. In some cases, the public library mechanism may be extended to accept user contributions, but still on the basis that all users have equal access. Most of the first generation of commercial timesharing systems provide a protection scheme with this level of function. Examples include the Dartmouth Time-Sharing System (DTSS) and IBM's VM/370 system. There are innumerable others.

c) Controlled sharing: Significantly more complex machinery is required to control explicitly who may access each data item stored in the system. For example, such a system might provide each file with a list of authorized users and allow an owner to distinguish several common patterns of use, such as reading, writing, or executing the contents of the file as a program. Although conceptually straightforward, actual implementation is surprisingly intricate, and only a few complete examples exist. These include M.l.T.'s Compatible Time-Sharing System (CTSS), Digital Equipment Corporation's DECsystem/10, System Development Corporation's Advanced Development Prototype (ADEPT) System, and Bolt, Beranek, and Newman's TENEX.

d) User-programmed sharing controls: A user may want to restrict access to a file in a way not provided in the standard facilities for controlling sharing. For example, he may wish to permit access only on weekdays between 9:00 A.M. and 4:00 P.M. Possibly, he may wish to permit access to only the average value of the data in a file. Maybe he wishes to require that a file be modified only if two users agree. For such cases, and a myriad of others, a general escape is to provide for user-defined *protected objects* and *subsystems*. A *protected subsystem* is a collection of programs and data with the property that only the programs of the subsystem have direct access to the data (that is, the protected objects). Access to those programs is limited to calling specified entry points. Thus the programs of the subsystem completely control the operations

performed on the data. By constructing a protected subsystem, a user can develop any programmable form of access control to the objects he creates.

Exercise 1. Read and memorize using a dictionary:

convenient, property, according to, to exclude, isolation, to moderate, to share, intricate, to distinguish, data, entry

Exercise 2. Answer the questions:

1) How are protection schemes divided?
2) What systems of information protection are there?
3) What examples of each system are given?
4) What is a protected subsystem?
5) What do the programs of the subsystem protect?

Exercise 3. Match the left part with the right:

1 A user may want to restrict	a) permit access to only the average value of the data in a file.
2. For example, he may wish to permit access only on	b) that a file be modified only if two users agree.
3. Possibly, he may wish to	c) access to a file in a way not provided in the standard facilities for controlling sharing.
4. Maybe he wishes to require	d) weekdays between 9:00 A.M. and 4:00 P.M.

Exercise 4. Define the terms using the suggested words and expressions as in example:

Information science	**Subsystem**	**Data**	**File**
discipline, deals with, processes, storing, transferring, information	self-contained system within larger system	facts statistics collected together reference analysis	set related data

EXAMPLE: Information science is a discipline that deals with the processes of storing and transferring information.

Exercise 5. Fill in the gaps with the suggested words:

sharing, own pieces, such, provide

These are systems that _____isolation of users, sometimes moderated by total sharing of some_____ of information. If only isolation is provided, the user of _____a system might just as well be using his_____ private computer, as far as protection and _____of information are concerned.

Exercise 6. Compose a story on one of the topics (up to 100 words):

1) Information protection systems
2) Protection schemes

Lesson 9

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

Passwords

Passwords as a general technique have some notorious defects. The most often mentioned defect lies in choice of password - if a person chooses his own password, he may choose something easily guessed by someone else who knows his habits. In one recent study of some 300 self-chosen passwords on a typical time-sharing system, more than 50 percent were found to be short enough to guess by exhaustion, derived from the owner's name, or something closely associated with the owner, such as his telephone number or birth date. For this reason, some systems have programs that generate random sequences of letters for use as passwords. They may even require that all passwords be system-generated and changed frequently. On the other hand, frequently changed random sequences of letters are hard to memorize, so such systems tend to cause users to make written copies of their passwords, inviting compromise. One solution to this problem is to provide a generator of "pronounceable" random passwords based on digraph or higher order frequency statistics to make memorization easier.

A second significant defect is that the password must be exposed to be used. In systems where the terminal is distant from the computer, the password must be sent through some communication system, during which passage a wiretapper may be able to intercept it.

An alternative approach to secrecy is unforgeability. The user is given a key, or magnetically striped plastic card, or some other unique and relatively difficult-to-fabricate object. The terminal has an input device that examines the object and transmits its unique identifying code to the computer system, which treats the code as a password that need not be kept secret. Proposals have been made for fingerprint readers and dynamic signature readers in order to increase the effort required for forgery.

The primary weakness of such schemes is that the hard-to-fabricate object, after being examined by the specialized input device, is reduced to a stream of bits to be transmitted to the computer. Unless the terminal, its object reader, and its communication lines to the computer are physically secured against tampering, it is relatively easy for an intruder to modify the terminal to transmit any sequence of bits he chooses. It may be necessary to make the acceptable bit sequences a secret after all. On the other hand, the scheme is convenient, resists casual misuse, and provides a conventional form of accountability through the physical objects used as keys.

A problem common to both the password and the unforgeable object approach is that they are "one-way" authentication schemes. They authenticate the user to the computer system, but not vice versa. An easy way for an intruder to penetrate a password system, for example, is to intercept all communications to and from the terminal and direct them to another computer--one that is under the interceptor's control. This computer can be programmed to "masquerade," that is, to act just like the system the caller intended to use, up to the point of requesting him to type his password. After receiving the password, the masquerader gracefully terminates the communication with some unsurprising error message, and the caller may be unaware that his password has been stolen. The same attack can be used on the unforgeable object system as well.

Exercise 1. Read and memorize using a dictionary:

Unforgeable, technique, to derive, random sequence, to memorize, digraph, wiretapper, to intercept, forgery, tampering, approach, vice versa

Exercise 2. Answer the questions:

1) What defects do passwords have as a general technique?
2) Why do some systems have programs that generate random sequences of letters for use as passwords?
3) What alternative approach to secrecy it there?
4) What common problem do password and the unforgeable object approaches have?
5) What easy way for an intruder to penetrate a password system is there?

Exercise 3. Match the left part with the right:

1 The primary weakness of such schemes is that the hard-to-fabricate object is reduced to	a) sequences a secret after all.
2. It is relatively easy for an intruder to	b) a stream of bits to be transmitted to the computer.
3. It may be necessary to make the acceptable bit	c) modify the terminal to transmit any sequence of bits he chooses.
4. A second significant defect is that	d) the password must be exposed to be used.

Exercise 4. Define the terms using the suggested words and expressions as in example:

Information science	**Forgery**	**Bit**	**Sequence**
discipline, deals with, processes, storing, transferring, information	producing, copy, document, signature, banknote, work of art	smallest, unit, information, computer's, memory	Particular, order, which, things, happen, are arranged

EXAMPLE: Information science is a discipline that deals with the processes of storing and transferring information.

Exercise 5. Fill in the gaps with the suggested words:

plastic ,approach, transmits, given, input, code

An alternative_____ to secrecy is unforgeability. The user is _____a key, or magnetically striped _____card, or some other unique and relatively difficult-to-fabricate object. The terminal has an _____device that examines the object and _____its unique identifying code to the computer system, which treats the_____ as a password that need not be kept secret.

Exercise 6. Compose a story on one of the topics (up to 100 words):

1) Password as a general technique of secrecy
2) Different approaches to secrecy and their defects

Lesson 10

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

Development of technical basis of information protection

1) The Development Plan: At this point we begin a development of the technical basis of information protection in modern computer systems. There are two ways to approach the subject: from the top down, emphasizing the abstract concepts involved, or from the bottom up, identifying insights by, studying example systems. We shall follow the bottom-up approach, introducing a series of models of systems as they are, (or could be) built in real life.

Our first model is of a multiuser system that completely isolates its users from one another. We shall then see how the logically perfect walls of that system can be lowered in a controlled way to allow limited sharing of information between users. Section II of this paper generalizes the mechanics of sharing using two different models: the capability system and the access control list system. It then extends these two models to handle the dynamic situation in which authorizations can change under control of the programs running inside the system. Further extensions to the models control the dynamics. The final model (only superficially explored) is of protected objects and protected subsystems, which allow arbitrary modes of sharing that are unanticipated by the system designer. These models are not intended so much to explain the particular systems as they are to explain the underlying concepts of information protection.

Our emphasis throughout the development is on direct access to information (for example, using LOAD and STORE instructions) rather than acquiring information indirectly (as when calling a data base management system to request the average value of a set of numbers supposedly not directly accessible). Control of such access is the function of the protected subsystems developed near the end of the paper. Herein lies perhaps the chief defect of the bottom-up approach, since conceptually there seems to be no reason to distinguish direct and indirect access, yet the detailed mechanics are typically quite different. The beginnings of a top-down approach based on a message model that avoids distinguishing between direct and indirect information access may be found in a paper by Lampson.

2) The Essentials of Information Protection*:* For purposes of discussing protection, the information stored in a computer system is not a single object. When one is considering direct access, the information is divided into mutually exclusive partitions, as specified by its various creators. Each partition contains a collection of information, all of which is intended to be protected uniformly. The uniformity of protection is the same kind of uniformity that applies to all of the diamonds stored in the same vault: any person who has a copy of the combination can obtain any of the diamonds. Thus, the collections of information in the partitions are the fundamental objects to be protected.

Conceptually, then, it is necessary to build an impenetrable wall around each distinct object that warrants separate protection, construct a door in the wall through which access can be obtained, and post a guard at the door to control its use. Control of use, however, requires that the guard have some way of knowing which users are authorized to have access, and that each user have some reliable way of identifying himself to the guard. This authority check is usually implemented by having the guard demand a match between something he knows and something the prospective user possesses. Both protection and authentication mechanisms can be viewed in terms of this general model.

Exercise 1. Read and memorize using a dictionary:

Insight, multiuser system, access control list system, to handle the situation, to extend, superficially explored, arbitrary, to acquire information, emphasis, indirect, partition, mutually, uniformity, to demand, authority check

Exercise 2. Answer the questions:

1) What does a multiuser system do?
2) What does a model of protected subsystems allow?
3) What is information divided into?
4) What are the fundamental objects to be protected?
5) How authority check is usually implemented?

Exercise 3. Match the left part with the right:

1 Our first model is of a multiuser	a) be lowered in a controlled way to allow limited sharing of information between users.
2. We shall then see how the logically perfect walls of that system can	b) system that completely isolates its users from one another.
3. Section II of this paper generalizes the mechanics of	c) dynamic situation in which authorizations can change under control of the programs running inside the system.
4. It then extends these two models to handle the	d) sharing using two different models: the capability system and the access control list system.

Exercise 4. Define the terms using the suggested words and expressions as in example:

Information science	**Database management system**	**Operating system**	**CPU**
discipline, deals with, processes, storing, transferring, information	system quick search retrieval information from database	software, keeps track, files, controls, processing computer programs	principal, component, composed control unit, instruction-decoding unit, arithmetic-logic unit

EXAMPLE: Information science is a discipline that deals with the processes of storing and transferring information.

Exercise 5. Fill in the gaps with the suggested words:

Real, protection, concepts, ways, begin, approach

At this point we _____a development of the technical basis of information_____ in modern computer systems. There are two____ to approach the subject: from the top down, emphasizing the abstract _____involved, or from the bottom up, identifying insights by, studying example systems. We shall follow the bottom-up____, introducing a series of models of systems as they are, (or could be) built in_____ life.

Exercise 6. Compose a story on one of the topics (up to 100 words):

1) The Essentials of Information Protection
2) Technical basis of information protection in modern computer systems

Lesson 11

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

Isolation Mechanisms in Multiprogramming Systems

Before extending this model, we pause to consider two concrete examples, the multiplexing of a single computer system among several users and the authentication of a user's claimed identity. These initial examples are complete isolation systems--no sharing of information can happen. Later we will extend our model of guards and walls in the discussion of shared information.

3) An Isolated Virtual Machine*:* A typical computer consists of a processor, a linearly addressed memory system, and some collection of input/output devices associated with the processor. It is relatively easy to use a single computer to simulate several, each of which is completely unaware of the existence of the others, except that each runs more slowly than usual. Such a simulation is of interest, since during the intervals when one of the simulated (commonly called *virtual*) processors is waiting for an input or output operation to finish, another virtual processor may be able to progress at its normal rate. Thus, a single processor may be able to take the place of several. Such a scheme is the essence of a multiprogramming system.

To allow each virtual processor to be unaware of the existence of the others, it is essential that some isolation mechanism be provided. One such mechanism is a special hardware register called a *descriptor register*. All memory references by the processor are checked by an extra piece of hardware that is interposed in the path to the memory. The descriptor register controls exactly which part of memory is accessible. The descriptor register contains two components: a *base* value and a *bound* value. The base is the lowest numbered address the program may use, and the bound is the number of locations beyond the base that may be used. We will call the value in the descriptor register a *descriptor*, as it describes an object (in this case, one program) stored in memory. The program controlling the processor has full access to everything in the base-bound range, by virtue of possession of its one descriptor. As we go on, we shall embellish the concept of a descriptor: it is central to most implementations of protection and of sharing of information.

So far, we have not provided for the dynamics of a complete protection scheme: we have not discussed who loads the descriptor register. If any running program could load it with any arbitrary value, there would be no protection. The instruction that loads the descriptor register with a new descriptor must have some special controls - either on the values it will load or on who may use it. It is easier to control who may use the descriptor, and a common scheme is to introduce an additional bit in the processor state. This bit is called the *privileged state* bit. All attempts to load the descriptor register are checked against the value of the privileged state bit; the privileged state bit must be ON for the register to be changed. One program (named the *supervisor*) runs with the privileged state bit ON, and controls the simulation of the virtual processors for the other programs. All that is needed to make the scheme complete is to ensure that the privileged state bit cannot be changed by the user programs except, perhaps, by an instruction that simultaneously transfers control to the supervisor program at a planned entry location. (In most implementations, the descriptor register is not used in the privileged state.)

Exercise 1. Read and memorize using a dictionary:

Multiplexing, several, claimed identity, initial, linearly addressed memory system, associated, unaware, rate, descriptor register, interposed, a base value, a bound value, embellish, supervisor program, privileged state bit

Exercise 2. Answer the questions:

1) What is an example of a complete isolation system?
2) What does a typical computer consist of?
3) What is the essence of a multiprogramming system?
4) What is a descriptor register?
5) What is the privileged state bit?

Exercise 3. Match the left part with the right:

1 It is relatively easy to use a single computer to	a) simulate several, each of which is completely unaware of the existence of the others, except that each runs more slowly than usual.
2. Such a simulation is of interest, since during	b) a multiprogramming system.
3. Thus a single processor may be able to	c) the intervals when one of the simulated (commonly called *virtual*) processors is waiting for an input or output operation to finish, another virtual processor may be able to progress at its normal rate.
4. Such a scheme is the essence of	d) take the place of several.

Exercise 4. Define the terms using the suggested words and expressions as in example:

Information science	**Computer science**	**Data processing**	**Multiplexing**
discipline, deals with, processes, storing, transferring, information	study, computers, computation, systems control, development, hardware, software, programming	conversion, raw, data, machine-read able form	process, transmitting, multiple, signals, simultaneously, single, channel,

EXAMPLE: Information science is a discipline that deals with the processes of storing and transferring information.

Exercise 5. Fill in the gaps with the suggested words:

Will, load, additional, to, state, with

The instruction that loads the descriptor register ____a new descriptor must have some special controls--either on the values it ____load or on who may use it. It is easier ____control who may use the descriptor, and a common scheme is to introduce an _____bit in the processor state. This bit is called the *privileged state* bit. All attempts to_____ the descriptor register are checked against the value of the privileged state bit; the privileged _____bit must be ON for the register to be changed.

Exercise 6. Compose a story on one of the topics (up to 100 words):

1) The multiplexing of a single computer system among several users
2) The authentication of a user's claimed identity
3) An isolated virtual machine

Lesson 12

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

Protection Architecture for Virtual Processors

One might expect the supervisor program to maintain a table of values of descriptors, one for each virtual processor. When the privileged state bit is OFF, the index in this table of the program currently in control identifies exactly which program and thus which virtual processor is accountable for the activity of the real processor. For protection to be complete, a virtual processor must not be able to change arbitrarily the values in the table of descriptors. If we suppose the table to be stored inside the supervisor program, it will be inaccessible to the virtual processors. We have here an example of a common strategy and sometime cause of confusion: the protection mechanisms not only protect one user from another, they may also protect their own implementation. We shall encounter this strategy again.

So far, this virtual processor implementation contains three protection mechanisms that we can associate with our abstractions. For the first, the information being protected is the distinct programs. The guard is represented by the extra piece of hardware that enforces the descriptor restriction. The impenetrable wall with a door is the hardware that forces all references to memory through the descriptor mechanism. The authority checks on a request to access memory is very simple. The requesting virtual processor is identified by the base and bound values in the descriptor register, and the guard checks that the memory location to which access is requested lies within the indicated area of memory.

The second mechanism protects the contents of the descriptor register. The wall, door, and guard are implemented in hardware, as with the first mechanism. An executing program requesting to load the descriptor register is identified by the privileged state bit. If this bit is OFF, indicating that the requester is a user program, then the guard does not allow the register to be loaded. If this bit is ON, indicating that the requester is the supervisor program, then the guard does allow it.

The third mechanism protects the privileged state bit. It allows an executing program identified by the privileged state bit being OFF (a user program) to perform the single operation "turn privileged state bit ON and transfer to the supervisor program." An executing program identified by the privileged state bit being ON is allowed to turn the bit OFF. This third mechanism is an embryonic form of the sophisticated protection mechanisms required to implement protected subsystems. The supervisor program is an example of a protected subsystem, of which more will be said later.

The supervisor program is part of all three protection mechanisms, for it is responsible for maintaining the integrity of the identifications manifest in the descriptor register and the privileged state bit. If the supervisor does not do its job correctly, virtual processors could become labeled with the wrong base and bound values, or user programs could become labeled with a privileged state bit that is ON. The supervisor protects itself from the user programs with the same isolation hardware that separates users, an example of the "economy of mechanism" design principle.

Exercise 1. Read and memorize using a dictionary:

Currently, accountable for, confusion, extra piece of hardware, impenetrable, contents, executing program, integrity, responsible, to perform, to load, requester

Exercise 2. Answer the questions:

1) What might one expect the supervisor program to maintain?
2) What does virtual processor implementation contain?
3) What protection mechanisms are described in the text?
4) What does each mechanism protect?
5) What program is part of all three protection mechanisms?

Exercise 3. Match the left part with the right:

1 So far, this virtual processor implementation contains	a) three protection mechanisms that we can associate with our abstractions.
2. For the first, the information being protected is the	b) forces all references to memory through the descriptor mechanism.
3. The guard is represented by the extra	c) distinct programs of Fig. 1.
4. The impenetrable wall with a door is the hardware that	d) piece of hardware that enforces the descriptor restriction.

Exercise 4. Define the terms using the suggested words and expressions as in example:

Information science	**Descriptor**	**Code**	**Binary code**
discipline, deals with, processes, storing, transferring, information	piece stored data indicates how data stored	system, symbols, rules, used, expressing, information	code, digital, computers, based, binary, number, system, there are, two, possible, states, off and on, usually, symbolized, 0 and 1

EXAMPLE: Information science is a discipline that deals with the processes of storing and transferring information.

Exercise 5. Fill in the gaps with the suggested words:

requester, not, first, identified, mechanism

The second _____protects the contents of the descriptor register. The wall, door, and guard are implemented in hardware, as with the _____mechanism. An executing program requesting to load the descriptor register is_____ by the privileged state bit. If this bit is OFF, indicating that the requester is a user program, then the guard does _____allow the register to be loaded. If this bit is ON, indicating that the_____ is the supervisor program, then the guard does allow it.

Exercise 6. Compose a story on one of the topics (up to 100 words):

1) Different protection mechanisms
2) Authority check

Lesson 13

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

From Virtual Machine Isolation to User Authentication

With an appropriately sophisticated and careful supervisor program, we now have an example of a system that completely isolates its users from one another. Similarly isolated permanent storage can be added to such a system by attaching some long-term storage device (e.g., magnetic disk) and developing a similar descriptor scheme for its use. Since long-term storage is accessed less frequently than primary memory, it is common to implement its descriptor scheme with the supervisor programs rather than hardware, but the principle is the same. Data streams to input or output devices can be controlled similarly. The combination of a virtual processor, a memory area, some data streams, and an isolated region of long-term storage is known as a virtual machine.

Long-term storage does, however, force us to face one further issue. Suppose that the virtual machine communicates with its user through a typewriter terminal. If a new user approaches a previously unused terminal and requests to use a virtual machine, which virtual machine (and, therefore, which set of long-term stored information) should he be allowed to use? We may solve this problem outside the system, by having the supervisor permanently associate a single virtual machine and its long-term storage area with a single terminal. Then, for example, padlocks can control access to the terminal. If, on the other hand, a more flexible system is desired, the supervisor program must be prepared to associate any terminal with any virtual machine and, as a result, must be able to verify the identity of the user at a terminal. Schemes for performing this authentication are the subject of our next example.

4) Authentication Mechanisms: Our second example is of an authentication mechanism: a system that verifies a user's claimed identity. The mechanics of this authentication mechanism differ from those of the protection mechanisms for implementing virtual machines mainly because not all of the components of the system are under uniform physical control. In particular, the user himself and the communication system connecting his terminal to the computer are components to be viewed with suspicion. Conversely, the user needs to verify that he is in communication with the expected computer system and the intended virtual machine. Such systems follow our abstract model of a guard who demands a match between something he knows and something the requester possesses. The objects being protected by the authentication mechanism are the virtual machines. In this case, however, the requester is a computer system user rather than an executing program, and because of the lack of physical control over the user and the communication system, the security of the computer system must depend on either the secrecy or the unforgeability of the user's identification.

In time-sharing systems, the most common scheme depends on secrecy. The user begins by typing the name of the person he claims to be, and then the system demands that the user type a password, presumably known only to that person.

There are, of course, many possible elaborations and embellishments of this basic strategy. In cases where the typing of the password may be observed, passwords may be good for only one use, and the user carries a list of passwords, crossing each one off the list as he uses it. Passwords may have an expiration date, or usage count, to limit the length of usefulness of a compromised one.

The list of acceptable passwords is a piece of information that must be carefully guarded by the system. In some systems, all passwords are passed through a hard-to-invert transformation before being stored, an idea suggested by R. Needham. When the user types his password, the system transforms it also and compares the transformed versions. Since the transform is supposed to be hard to invert (even if the transform itself is well known), if the stored version of a password is compromised, it may be very difficult to determine what original password is involved. It should be noted, however, that "hardness of inversion" is difficult to measure. The attacker of such a system does not need to discern the general inversion, only the particular one applying to some transformed password he has available.

Exercise 1. Read and memorize using a dictionary:

Appropriately, sophisticated, permanent, long-term storage device, rather than, since, primary memory, issue, to face, previously, on the other hand, flexible, authentication, in particular, conversely, to match, presumably, expiration date, usage count, to invert, to discern, data stream

Exercise 2. Answer the questions:

1) What is a virtual machine?
2) What issue does log-term storage force us to face?
3) What is an authentication mechanism?
4) What are passwords passed through in some systems?
5) Who suggested the idea of a hard-to-invert transformation?

Exercise 3. Match the left part with the right:

1 In particular, the user himself and the communication system connecting his terminal to the computer are	a) components to be viewed with suspicion.
2. Conversely, the user needs to verify that he	b) demands a match between something he knows and something the requester possesses.
3. Such systems follow our abstract model of a guard who	c) the virtual machines.
4. The objects being protected by the authentication mechanism are	d) is in communication with the expected computer system and the intended virtual machine.

Exercise 4. Define the terms using the suggested words and expressions as in example:

Information science	**Memory**	**Data processing**	**Storage**
discipline, deals with, processes, storing,	physical, device, to store, information,	manipulation, data, by, computer	process, storing, data, computer

transferring, information	data, programs, temporary, permanent, basis		

EXAMPLE: Information science is a discipline that deals with the processes of storing and transferring information.

Exercise 5. Fill in the gaps with the suggested words:

use, communicates, allowed, user, face

Long-term storage does, however, force us to____ one further issue. Suppose that the virtual machine _____with its user through a typewriter terminal. If a new_____ approaches a previously unused terminal and requests to_____ a virtual machine, which virtual machine (and, therefore, which set of long-term stored information) should he be_____ to use?

Exercise 6. Compose a story on one of the topics (up to 100 words):

1) Passwords and their drawbacks
2) Authentication mechanisms

Lesson 14

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

The Differences and Features of Hardware & Software Firewalls

A firewall is a protective system that lies, in essence, between your computer network and the Internet. When used correctly, a firewall prevents unauthorized use and access to your network. The job of a firewall is to carefully analyze data entering and exiting the network based on your configuration. It ignores information that comes from an unsecured, unknown or suspicious location. A firewall plays an important role on any network as it provides a protective barrier against most forms of attack coming from the outside world.

Firewalls can be either hardware or software. The ideal firewall configuration will consist of both. In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificates and logins. While many people do not completely understand the importance and necessity of a firewall, or consider it to be a product for businesses only, if your network or computer has access to the outside world via the Internet then you need have a firewall to protect your network, individual computer and data therein.

Hardware Firewalls

Hardware firewalls can be purchased as a stand-alone product but more recently hardware firewalls are typically found in broadband routers, and should be considered an important part of your system and network set-up, especially for anyone on a broadband connection. Hardware firewalls can be effective with little or no configuration, and they can protect every machine on a local network. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.

A hardware firewall uses packet filtering to examine the header of a packet to determine its source and destination. This information is compared to a set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped.

As with any electronic equipment, a computer user with general computer knowledge can plug in a firewall, adjust a few settings and have it work. To ensure that your firewall is configured for optimal security and protect however, consumers will no doubt need to learn the specific features of their hardware firewall, how to enable them, and how to test the firewall to ensure it"s doing a good job of protecting your network.

Not all firewalls are created equal, and to this end it is important to read the manual and documentation that comes with your product. Additionally, the manufacturer's Web site will usually provide a knowledgebase or FAQ to help you get started.

To test your hardware firewall security, you can purchase third-party test software or search the Internet for a free online-based firewall testing service. Firewall testing is an important part of maintenance to ensure your system is always configured for optimal protection.

Exercise 1. Read and memorize using a dictionary:

firewall, to prevent, suspicious, in addition to, remote access, authentication, via, broadband router, packet filtering, to forward, knowledgebase, maintenance

Exercise 2. Answer the questions:

1) What are the functions of a firewall?

2) What will the ideal firewall configuration consist of?
3) What does a hardware firewall use?
4) How can you test your firewall security?
5) What can protect every machine on a local network?

Exercise 3. Match the left part with the right:

1 A firewall is a	a) unauthorized use and access to your network.
2.When used correctly, a firewall prevents	b) protective system that lies, in essence, between your computer network and the Internet.
3. The job of a firewall is	c) information that comes from an unsecured, unknown or suspicious location.
4. Firewall ignores	d) to carefully analyze data entering and exiting the network based on your configuration.

Exercise 4. Define the terms using the suggested words and expressions as in example:

Information science	**A firewall**	**FAQ**	**Router**
discipline, deals with, processes, storing, transferring, information	protective, system, lies, in essence, between, computer, network, Internet.	abbreviation frequently asked, questions	Piece, equipment, allows, access, computers, networks

EXAMPLE: Information science is a discipline that deals with the processes of storing and transferring information.

Exercise 5. Fill in the gaps with the suggested words:

to, useful, either, network, both

Firewalls can be _____hardware or software. The ideal firewall configuration will consist of_____. In addition to limiting access to your computer and network, a firewall is also_____ for allowing remote access ___a private_____ through secure authentication certificates and logins.

Exercise 6. Compose a story on one of the topics (up to 100 words):

1) Functions of firewalls
2) Hardware firewall

Lesson 15

Мета заняття: вміти використовувати іноземну мову, включаючи усну та письмову форми в обсязі програмних вимог в продуктивних та рецептивних видах мовленнєвої діяльності. здатність працювати з різними джерелами, розшукувати, обробляти, аналізувати і синтезувати отриману інформацію.

Software Firewalls

For individual home users, the most popular firewall choice is a software firewall. Software firewalls are installed on your computer (like any software) and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or e-mail worms. Many software firewalls have user defined controls for setting up safe file and printer sharing and to block unsafe applications from running on your system. Additionally, software firewalls may also incorporate privacy controls, web filtering and more. The downside to software firewalls is that they will only protect the computer they are installed on, not a network, so each computer will need to have a software firewall installed on it.

Like hardware firewalls there is a vast number of software firewalls to choose from. To get started you may wish to read reviews of software firewalls and search out the product Web site to glean some information first. Because your software firewall will always be running on your computer, you should make note of the system resources it will require to run and any incompatibilities with your operating system. A good software firewall will run in the background on your system and use only a small amount of system resources. It is important to monitor a software firewall once installed and to download any updates available from the developer.

The differences between a software and hardware firewall are vast, and the best protection for your computer and network is to use both, as each offers different but much-needed security features and benefits. Updating your firewall and your operating system is essential to maintaining optimal protection, as is testing your firewall to ensure it is connected and working correctly.

Exercise 1. Read and memorize using a dictionary:

software firewall, to customize, downside, incompatibility, to glean information, vast, benefit, essential

Exercise 2. Answer the questions:

6) What will software firewall protect your computer from?
7) What is the downside to software firewall?
8) What can software firewall incorporate?
9) What should you do before installing a software firewall?
10) What is essential to maintaining optimal protection of your computer?

Exercise 3. Match the left part with the right:

1 Like hardware firewalls there is	a) read reviews of software firewalls and search out the product Web site to glean some information first.
2. To get started you may wish to	b) the background on your system and use only a small amount of system resources.
3. A good software firewall will run in	c) a vast number of software firewalls to choose from.
4. It is important to monitor	d) a software firewall once installed and to download any updates available from the developer.

Exercise 4. Define the terms using the suggested words and expressions as in example:

Information science	**Download**	**Worm program**	**Access**
discipline, deals with, processes, storing, transferring, information	Copy, data, one computer, system, another, to a disk.	self-replicating, program, able to, propagate, itself, network, typically, having, detrimental, effect	Process, obtaining, retrieving, information, stored, computer's, memory

EXAMPLE: Information science is a discipline that deals with the processes of storing and transferring information.

Exercise 5. Fill in the gaps with the suggested words:

unsafe, incorporate, have, your, and

Many software firewalls ____user defined controls for setting up safe file and printer sharing and to block _____applications from running on____ system. Additionally, software firewalls may also _____privacy controls, web filtering____ more.

Exercise 6. Compose a story on one of the topics (up to 100 words):

1) Software firewall
2) The differences between a software and hardware firewall

References

https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

https://cybersecuritynews.com/cia-triad-confidentiality-integrity-availability/

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/

https://eligovoting.com/key-principles-of-data-protection-explained/

https://www.box.com/en-nl/resources/principles-and-fundamentals-information-security

https://cyberranges.com/whitepaper-download-understanding-cyber-ranges-from-hype-to-reality/?utm_source=google&utm_medium=search&utm_campaign=ecso-white-paper&utm_id=general-ecso&gad_source=1&gad_campaignid=22362881191&gbraid=0AAAACyrLDqzdTdeKdF9eg5b-tMdYCKHu&gclid=CjwKCAiAqprNBhB6EiwAMe3yhk2cQErePY5eDtPG3FFZ3c4Jm2LlfG6Luv8nlU4BOtD9S_oZQ3NbSRoCTK4QAvD_BwE

https://cybersecuritynews.com/cia-triad-confidentiality-integrity-availability/

https://web.mit.edu/saltzer/www/publications/protection/Basic.html

https://tech.rochester.edu/security/passwords-passphrases/

https://eng.libretexts.org/Bookshelves/Computer_Science/Operating_Systems/Think_OS_-_A_Brief_Introduction_to_Operating_Systems_(Downey)/02%3A_Processes/2.02%3A_Isolation

www.cse.iitd.ac.in/~srsarangi/advbook/chapters/secure-archs.pdf