

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ



Державний університет
інтелектуальних технологій і зв'язку

кафедра лінгводидактики та іноземних мов

КУЗЬМЕНКО ЮЛІЯ
ДЯКУН КАТЕРИНА

ПРАКТИКУМ

для аудиторної та самостійної роботи
з англійської мови
для здобувачів 2 курсу ВК
«Англійська для ІТ та кібербезпеки»
першого (бакалаврський) рівня вищої освіти
спеціальності F5 «Кібербезпека та захист інформації»

Частина I



СУЧАСНА
ОСВІТА



КІБЕРБЕЗПЕКА



ІНТЕЛЕКТУАЛЬНІ
ТЕХНОЛОГІЇ

Одеса 2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Державний університет інтелектуальних технологій і зв'язку
кафедра лінгводидактики та іноземних мов

КУЗЬМЕНКО ЮЛІЯ
ДЯКУН КАТЕРИНА

ПРАКТИКУМ

для аудиторної та самостійної роботи з англійської мови

ЧАСТИНА 1

для здобувачів 2 курсу ВК «Англійська для ІТ та кібербезпеки»
першого (бакалаврський) рівня вищої освіти
спеціальностей F2, F3, F5, F6, F7

УДК 811.111:004(075.8)

Автори:

Кузьменко Ю.О., доцент кафедри лінгводидактики та іноземних мов Державного університету інтелектуальних технологій і зв'язку, кандидат педагогічних наук, доцент

Дякун К.О., старший викладач кафедри лінгводидактики та іноземних мов Державного університету інтелектуальних технологій і зв'язку

Рецензенти:

Трубіцина О.М., кандидат педагогічних наук, доцент, завідувачка кафедри романської філології та методики викладання іноземних мов, ДЗ "Південноукраїнський національний педагогічний університет імені К.Д.Ушинського

Фогель Т.М., кандидат педагогічних наук, доцент, доцент кафедри германських і східних мов та методики їх навчання, ДЗ "Південноукраїнський національний педагогічний університет імені К.Д.Ушинського

*Рекомендовано до друку Навчально-методичною радою
Державного університету інтелектуальних технологій і зв'язку
(Протокол №4 від 19 червня 2026 року)*

Кузьменко Ю.О., Дякун К.О. **Практикум для аудиторної та самостійної роботи з англійської мови, Частина 1** [для здобувачів 2 курсу ВК «Англійська для ІТ та кібербезпеки» першого (бакалаврський) рівня вищої освіти для спеціальностей F2, F3, F5, F6, F7]. Одеса : ДУІТ3, 2026. 114 с. URL: <https://metod.suitt.edu.ua>

Практикум «Англійська для ІТ та кібербезпеки» Частина І є складовою навчально-методичного забезпечення підготовки здобувачів 2 курсу першого (бакалаврського) рівня вищої освіти спеціальностей F2, F3, F5, F6, F7. Видання розроблено для освітнього компонента ВК «Англійська для ІТ та кібербезпеки» на основі автентичних англомовних текстів фахового спрямування та орієнтовано на формування й удосконалення навичок роботи з професійно-орієнтованими матеріалами у сфері інформаційних технологій та кібербезпеки.

Структура практикуму відповідає змісту освітнього компонента та охоплює завдання для аудиторної й самостійної роботи, вправи для розвитку навичок читання, перекладу, усного та писемного мовлення, а також завдання, спрямовані на активне засвоєння професійної термінології у сфері ІТ та кібербезпеки. Практикум сприяє розвитку комунікативних компетентностей здобувачів вищої освіти та формуванню навичок використання англійської мови у професійній діяльності.

ПЕРЕДМОВА

Пропонований практикум для аудиторної та самостійної роботи з англійської мови призначений для здобувачів 2 курсу першого (бакалаврського) рівня вищої освіти спеціальностей F2, F3, F5, F6 та F7, які вивчають англійську мову за професійним спрямуванням у сфері ІТ та кібербезпеки.

Метою даного практикума є розвиток умінь і навичок роботи з автентичними англомовними текстами професійної тематики, формування практичних комунікативних компетенцій, а також оволодіння і активне використання фахової англійської термінології. Практикум спрямований на розширення словникового запасу здобувачів професійною лексикою та розвиток навичок професійного спілкування англійською мовою.

Практикум структурований у три модулі, кожен з яких включає по три уроки. У кожному уроці подано автентичні тексти професійного характеру, тематичний словник та післятекстові завдання лексичного, граматичного та комунікативного спрямування. Для ефективного засвоєння матеріалу посібник пропонує систему вправ, що дозволяє:

- опановувати тематичний словник;
- закріплювати лексику через читання та аналіз текстів;
- відпрацьовувати граматичні конструкції у професійному контексті;
- розвивати навички усного та письмового спілкування у сфері ІТ та кібербезпеки.

Всі завдання у практикумі відповідають рівню B2 (Upper-Intermediate) і дозволяють здобувачам як самостійно, так і під керівництвом викладача ефективно опанувати матеріал. В кінці практикуму подано відповіді.

CONTENTS

Module 1. Introduction to IT and Cybersecurity.	
<i>Lesson 1. Computer Systems & Networks.</i>	6
<i>Lesson 2. Operating Systems and Software.</i>	15
<i>Lesson 3. Cloud Computing & Security</i>	23
Module 2. Cybersecurity and Modern Threats	
<i>Lesson 1. Cyber Threats & Attacks</i>	32
<i>Lesson 2. Internet Security & Encryption</i>	41
<i>Lesson 3. Network Security & Firewalls</i>	52
Module 3. Cybersecurity Policies & Regulations	
<i>Lesson 1. Ethical Hacking & Penetration Testing</i>	61
<i>Lesson 2. Cybersecurity in Business</i>	71
<i>Lesson 3. Artificial Intelligence & Cybersecurity</i>	81
Answer Keys	
Module 1. Introduction to IT and Cybersecurity	90
Module 2. Cybersecurity and Modern Threats	96
Module 3. Cybersecurity Policies & Regulations	103

Module 1. Introduction to IT and Cybersecurity

Lesson 1. Computer Systems & Networks

WORDBANK

Term	Translation
1. hardware architecture	апаратна архітектура
2. system resources	системні ресурси
3. network infrastructure	мережева інфраструктура
4. data transmission	передача даних
5. bandwidth capacity	пропускна здатність
6. communication protocol	протокол зв'язку
7. client-server model	клієнт-серверна модель
8. packet switching	пакетна комутація
9. network latency	затримка мережі
10.routing mechanism	механізм маршрутизації
11.scalability	масштабованість
12.system reliability	надійність системи
13.fault tolerance	відмовостійкість
14.network topology	мережева топологія
15.secure connectivity	захищене з'єднання

Task 1. Match the concepts with their definitions.

Terms	Definitions
1. hardware architecture	A. Protection of data during transmission from unauthorized access
2. network infrastructure	B. The capability of a system to grow without performance degradation
3. client-server model	C. A structured model in which clients request services from centralized systems
4. communication protocol	D. Time delay experienced during data transmission across a network
5. packet switching	E. A method of transmitting data in discrete units across networks
6. network latency	F. A collection of hardware, software, and communication links
7. routing mechanism	G. The process of selecting optimal paths for data transfer
8. scalability	H. A set of formal rules governing data exchange between devices
9. fault tolerance	I. The ability of a system to continue operating when failures occur
10. secure connectivity	J. The physical and logical organization of computing components

Task 2. Match the term with the correct Ukrainian translation and make the sentences.

Terms	Ukrainian translation
1. hardware architecture	A. пакетна комутація
2. network infrastructure	B. захищене з'єднання
3. client-server model	C. відмовостійкість
4. communication protocol	D. клієнт-серверна модель
5. packet switching	E. фізична та логічна організація компонентів
6. network latency	F. масштабованість
7. routing mechanism	G. затримка мережі
8. scalability	H. механізм маршрутизації
9. fault tolerance	I. протокол зв'язку
10. secure connectivity	J. мережева інфраструктура

Task 3. Complete the sentences using words from the wordbank.

model-server client, capacity bandwidth, architecture hardware, infrastructure network, connectivity secure, latency network, protocol communication, mechanism routing, switching packet, scalability

1. Modern computer systems depend on advanced _____ to ensure efficient processing and coordination of components.
2. A well-designed _____ is essential for stable enterprise-level communication.
3. In distributed systems, the _____ enables centralized management of resources.
4. Every _____ defines how data is formatted, transmitted, and verified.
5. High _____ significantly improves the performance of cloud-based services.

6. _____ allows large volumes of data to be transmitted efficiently across global networks.
7. Increased _____ may negatively affect real-time applications such as video conferencing.
8. An effective _____ minimizes congestion and data loss.
9. _____ ensures that systems can grow without performance degradation.
10. _____ is critical for protecting sensitive information during transmission.

Task 4. Reading

Computer Systems & Network

Computer systems and networks are the technological backbone of contemporary digital environments. A modern computer system is based on a defined hardware architecture, which integrates processors, memory units, and storage devices in order to manage system resources efficiently. Software layers interact with hardware to ensure reliability, scalability, and operational stability.

A network infrastructure connects multiple systems and enables data transmission between geographically distributed devices. Most enterprise environments rely on the client-server model, where clients request services and centralized servers process, store, and manage information. This model supports system scalability and simplifies security management.

Data exchange across networks is governed by communication protocols, which establish standardized rules for addressing, routing, and error detection. Using packet switching, data is divided into small units that travel independently across the network. This approach improves fault tolerance and optimizes bandwidth usage. However, excessive network latency can reduce system responsiveness, particularly in time-sensitive applications.

Network devices such as routers implement complex routing mechanisms to select efficient paths for data packets. Proper network design, including appropriate network topology, directly influences performance, reliability, and security. Furthermore, secure connectivity is essential in cybersecurity contexts, as it protects transmitted data from interception and manipulation.

In the context of cybersecurity, resilient network architectures enhance system reliability and reduce vulnerabilities. Without secure and scalable networks, cloud computing, remote work environments, and critical digital services would be impossible to maintain effectively.

Task 5. Decide whether the statements are True (T) or False (F).

- 1. Hardware architecture defines both physical and logical system organization.
- 2. Client-server systems eliminate the need for centralized data storage.
- 3. Communication protocols standardize data exchange processes.
- 4. Packet switching improves fault tolerance.
- 5. Network latency has no effect on real-time services.
- 6. Routing mechanisms influence network efficiency.
- 7. Network topology impacts cybersecurity.
- 8. Secure connectivity is optional in enterprise systems.
- 9. Scalability supports long-term system growth.
- 10. Network reliability is unrelated to cybersecurity.

Task 6. For each word, fill in the missing verb, noun, adjective, or adverb.

Verb	Noun	Adjective	Adverb
1. protect			protectively
2.	security		
3. monitor		monitored	
4. select			selectively

Verb	Noun	Adjective	Adverb
5.	efficiency		
6. interact		interactive	
7.	resilience		resiliently
8. optimize		optimal	
9. secure			securely
10.enhance	enhancement		
11.	reliability	reliable	
12.allocate		allocated	dynamically
13.transmit	transmission		
14.	connectivity	secure	
15.process		processed	

Grammar Focus: Passive Voice & Complex Present Simple

Task 7. Rewrite the sentences using the Passive Voice.

- Engineers design network infrastructures **regularly** to ensure reliability.
- Protocols regulate data transmission **currently**.
- Routers select optimal transmission paths **at the moment**.
- Network administrators monitor traffic **continuously**.
- Systems allocate resources **dynamically every time**.
- Security mechanisms protect transmitted data **always**.
- Servers process client requests **yesterday**.
- Network topology affects performance **usually**.
- Engineers implement fault tolerance mechanisms **last week**.
- Networks support cloud services **constantly**.
- Engineers will upgrade the network infrastructures **next month**.
- Security teams will monitor cyber threats **tomorrow**.

Task 8. Replace the highlighted terms in the sentences with suitable synonyms or equivalent expressions.

computer framework, network delay, system stability, client-server architecture, data segmentation, networking rules, protected connection, computing resources, path selection methods, data transfer, network framework

1. A modern **hardware architecture** integrates processors, memory units, and storage devices to support computing tasks.
2. Efficient management of **system resources** is essential for optimal performance of a computer system.
3. A robust **network infrastructure** connects multiple devices and ensures smooth communication.
4. High-speed **data transmission** is critical for cloud computing and online services.
5. Most enterprise applications operate on a **client-server model**, where clients request services from central servers.
6. Digital communication relies on standardized **communication protocols** for addressing and error detection.
7. Large files are often sent using **packet switching**, which divides data into smaller units.
8. Excessive **network latency** can cause delays and reduce performance in time-sensitive applications.
9. Routers implement **routing mechanisms** to determine the most efficient paths for data packets.
10. **Secure connectivity** protects transmitted data from interception and unauthorized access.
11. Redundant systems and failover solutions improve overall **system reliability** in IT networks.

Task 9. Open the brackets using Present Simple Active or Passive.

1. Data packets _____ (route) dynamically across multiple nodes to ensure efficient data transmission in complex network environments.
2. Network engineers _____ (monitor) system performance continuously to detect potential issues before they affect users.
3. Secure connections _____ (establish) using advanced encryption protocols to protect sensitive information from unauthorized access.
4. Users _____ (access) cloud-based services through secure gateways that provide authentication and data protection.
5. Network latency _____ (increase) significantly when the available bandwidth is insufficient to handle large volumes of data traffic.
6. IT specialists _____ (configure) network devices regularly to maintain optimal performance and prevent system failures.
7. Fault tolerance _____ (achieve) through redundancy mechanisms that allow systems to continue operating even in case of hardware failure.
8. System administrators _____ (update) security policies frequently to respond to emerging cybersecurity threats and vulnerabilities.
9. Routing decisions _____ (optimize) continuously by algorithms that analyze network conditions in real time.
10. Companies _____ (reduce) cybersecurity risks by implementing secure connectivity solutions and educating employees about safe online practices.

Task 10. Choose a topic from the given below prepare a presentation (5-7 slides).

1. Client-server vs peer-to-peer networking models
2. Role of protocols in cybersecurity
3. Packet switching and network efficiency
4. Network latency and real-time applications

5. Scalability challenges in cloud networks
6. Secure connectivity in enterprise environments
7. Network topology and system reliability
8. Fault tolerance in critical infrastructures
9. Importance of network design in cybersecurity

Task 11. Watch the videos and tick the sentences True (T) or False (F).

Video 1 <https://www.youtube.com/watch?v=wFjn2Nr7yIU>

Video 2 <https://www.youtube.com/watch?v=wqC0JJ-qC30>

1. Both videos discuss the impact of human behaviour on modern life.
2. The speakers suggest that people always make rational decisions.
3. One of the videos explains how emotions influence our choices.
4. The videos show that habits can affect everyday actions.
5. According to the videos, social influence has no effect on people's decisions.
6. One speaker mentions that modern technologies make certain behaviours easier.
7. The videos suggest that people are always aware of their actions.
8. Both videos include examples from real life.
9. The speakers agree that changing behaviour is impossible.
10. The videos encourage viewers to think more critically about their actions.

Lesson 2. Operating Systems and Software

WORDBANK

Term	Translation
1. operating system (OS)	операційна система
2. kernel	ядро
3. system call	системний виклик
4. user interface	інтерфейс користувача
5. resource allocation	розподіл ресурсів
6. multitasking	багатозадачність
7. process scheduling	планування процесів
8. access control	контроль доступу
9. system vulnerability	системна вразливість
10. software patch	програмне оновлення
11. open-source software	ПЗ з відкритим кодом
12. proprietary software	пропрієтарне ПЗ
13. execution environment	середовище виконання
14. privilege escalation	підвищення привілеїв
15. system stability	стабільність системи

Task 1. Match the word/phrase with the correct definition.

Terms	Definitions
1. operating system	A. The unauthorized gain of higher system permissions
2. kernel	B. Software with publicly available source code
3. resource allocation	C. Restriction of system access based on defined permissions
4. multitasking	D. A core component that controls low-level system operations
5. process scheduling	E. The ability to run multiple processes simultaneously
6. access control	F. Software that manages hardware and application execution
7. system vulnerability	G. An update designed to fix security or functionality issues
8. software patch	H. A weakness in a system that can be exploited by attackers
9. open-source software	I. A mechanism that determines the execution order of processes
10. privilege escalation	J. The regulated distribution of system resources

Task 2. Match the word/phrase with the correct Ukrainian translation and make your own sentences.

Terms	Ukrainian translation
1. operating system	A. ядро
2. kernel	B. багатозадачність
3. resource allocation	C. контроль доступу
4. multitasking	D. операційна система
5. process scheduling	E. планування процесів
6. access control	F. підвищення привілеїв

Terms	Ukrainian translation
7. system vulnerability	Г. програмне оновлення
8. software patch	Н. ПЗ з відкритим кодом
9. open-source software	І. системна вразливість
10. privilege escalation	Ж. розподіл ресурсів

Task 3. Complete the sentences using words from the wordbank.

system stability, kernel, access control, system vulnerability, operating system (OS), software patch, open-source software, process scheduling, multitasking, privilege escalation

1. The _____ manages hardware resources and provides services for applications.
2. The _____ operates at the lowest level of the system.
3. Efficient _____ ensures fair CPU usage.
4. Modern systems rely on _____ to improve productivity.
5. Strict _____ prevents unauthorized access.
6. A _____ may expose systems to cyberattacks.
7. Installing a _____ reduces security risks.
8. _____ allows community-driven development.
9. Improper _____ can lead to serious security breaches.
10. _____ ensures reliable long-term operation.

Task 4. Reading

Operating Systems and Software

An operating system (OS) is a fundamental component of modern computer systems, acting as an intermediary between hardware and software applications. Its primary function is to manage resource allocation, ensuring that processing power, memory, and storage are distributed efficiently among running programs. At the core of every OS lies the kernel, which controls low-

level operations and enables communication between hardware and software through system calls.

Modern operating systems support multitasking, allowing multiple processes to execute concurrently. This is achieved through advanced process scheduling mechanisms that determine which process receives CPU time at any given moment. The user interface, whether graphical or command-line based, enables interaction between users and the system.

From a cybersecurity perspective, operating systems are frequent targets of attacks due to potential system vulnerabilities. Weak access policies or software flaws may allow privilege escalation, enabling attackers to gain unauthorized control over the system. To mitigate such risks, developers regularly release software patches that address known vulnerabilities and improve system stability.

Operating systems can be classified as open-source software or proprietary software. Open-source systems provide transparency and flexibility, allowing experts to examine and modify source code. Proprietary systems, while closed, often offer centralized support and controlled development environments. In cybersecurity-focused environments, secure operating system configuration and continuous updates are essential. Without proper access control and patch management, even advanced security tools cannot guarantee system protection.

Task 5. Decide whether the statements are True (T) or False (F).

1. The operating system directly manages hardware resources.
2. The kernel operates at the application level.
3. Multitasking improves system efficiency.
4. Process scheduling controls CPU usage.
5. System vulnerabilities can be exploited.
6. Software patches increase vulnerabilities.
7. Open-source software allows code inspection.

8. Privilege escalation increases system security.
9. Access control restricts unauthorized users.
10. OS security is critical for cybersecurity.

Grammar Focus: Passive Voice & Causative Structures

Task 6. Rewrite sentences using the Passive Voice.

1. The operating system **allocates** system resources to active applications.
2. Developers **released** a critical security patch last week.
3. Administrators **are configuring** access control settings now.
4. The kernel **has managed** system calls efficiently for many years.
5. The system **will schedule** processes automatically.
6. Attackers **can exploit** software vulnerabilities remotely.
7. Engineers **are improving** system stability at the moment.
8. The operating system **must enforce** strict security policies.
9. Users **have installed** the latest software updates.
10. Administrators **were monitoring** system performance during the failure.

Task 7. Give synonyms to the words in bold.

1. The OS **controls** hardware operations and coordinates the interaction between physical devices and system software.
2. The kernel **handles** critical system tasks and ensures stable communication between different components.
3. The OS **allows** multitasking and enables users to run multiple applications at the same time.
4. System administrators **fix** vulnerabilities to protect the network from potential cyber threats.

5. The graphical interface **shows** important system information, including performance statistics and error messages.
6. Attackers **use** system weaknesses to gain unauthorized access to confidential data.
7. The OS **keeps** system resources organized and distributes them efficiently among running programs.
8. Regular software patches **improve** system stability and reduce the risk of technical failures.
9. Modern security systems **stop** unauthorized access by implementing strong authentication mechanisms.
10. Software developers **build** secure environments to ensure data protection and reliable system performance.

Task 8. Open the brackets using the correct form of the verb.

1. The OS _____ (allocate) resources dynamically every time new applications are launched.
2. IT specialists _____ (identify) multiple system vulnerabilities last week while they _____ (perform) a security audit.
3. Administrators _____ (manage) access rights carefully since the company _____ (implement) the new security policy.
4. The IT department _____ (maintain) overall system stability while upgrading servers yesterday.
5. Strict access control policies _____ (prevent) privilege escalation, and administrators _____ (review) them continuously this month.
6. Developers _____ (release) software patches regularly, and by the end of the day, they _____ (deploy) all critical updates.
7. The kernel _____ (execute) core operations constantly, and last night it _____ (process) more than 1,500 requests without errors.
8. The OS _____ (schedule) processes automatically, while the IT team _____ (record) any delays that have occurred this week.

9. Security teams _____ (monitor) user activity continuously, and they _____ (flag) all suspicious attempts that occurred yesterday.
10. Software developers and cybersecurity experts _____ (enhance) OS security gradually over the years, and by 2026 they _____ (introduce) several advanced protocols.

Task 9. Choose a topic from the given below prepare a presentation (5-7 slides).

1. The Strategic Role of Operating Systems in Modern Cybersecurity Frameworks (Focus on OS as a security layer, threat surface, integration with security tools.)
2. Kernel Architecture Design and Its Impact on System Security and Isolation Mechanisms (Monolithic vs microkernel, attack surface, memory protection.)
3. Security Implications of Open-Source and Proprietary Operating Systems: A Comparative Analysis (Transparency, vulnerability disclosure, update models, trust models.)
4. Advanced Access Control Mechanisms in Operating Systems: Models, Policies, and Implementation (DAC, MAC, RBAC, zero-trust principles.)
5. Privilege Escalation Attacks: Techniques, Exploitation Methods, and Prevention Strategies (Vertical vs horizontal escalation, real-world attack vectors.)
6. Patch Management as a Critical Component of Organizational Cybersecurity Strategy (Update cycles, vulnerability windows, risk management.)
7. Multitasking and Process Scheduling: Performance Optimization vs Security Risks (Race conditions, resource starvation, isolation failures.)
8. Operating System Vulnerabilities: Detection, Exploitation, and Mitigation Techniques (Zero-day exploits, sandboxing, hardening techniques.)

9. Ensuring System Stability and Security in Enterprise-Level IT Infrastructures (High availability, redundancy, monitoring, compliance.)
10. The Future of Operating System Security: AI Integration, Virtualization, and Zero-Trust Architectures (Cloud OS, containerization, predictive threat detection.)

Task 10. Watch the video and decide whether the statements are True (T) or False (F) .

Video: <https://www.youtube.com/watch?v=aw15lx56Cfg>

1. An operating system manages both hardware resources and software applications on a computer.
2. Utility programs are designed primarily to entertain users and provide multimedia content.
3. The operating system controls processes such as memory management, file handling, and device coordination.
4. Antivirus software is an example of a utility program that helps protect the system from threats.
5. Operating systems do not interact directly with computer hardware components.
6. Disk cleanup and file compression tools are commonly classified as utility programs.
7. A user cannot run application software without an operating system installed on the computer.
8. Utility programs are responsible for managing the central processing unit (CPU) during program execution.
9. Operating systems provide a user interface that allows people to interact with the computer system.
10. Backup utilities help users prevent data loss by creating copies of important files.

Lesson 3. Cloud Computing & Security

WORDBANK

Term	Translation
1. cloud computing	хмарні обчислення
2. virtualized environment	віртуалізоване середовище
3. scalability	масштабованість
4. cloud service provider	постачальник хмарних послуг
5. data encryption	шифрування даних
6. access management	управління доступом
7. shared responsibility model	модель спільної відповідальності
8. data breach	витік даних
9. redundancy	надмірність
10.availability	доступність
11.infrastructure as a service (IaaS)	інфраструктура як сервіс
12.platform as a service (PaaS)	платформа як сервіс
13.software as a service (SaaS)	програмне забезпечення як сервіс
14.compliance requirements	вимоги відповідності
15.risk mitigation	зменшення ризиків

Task 1. Match the term with the correct definition.

Terms	Definitions
1. cloud computing	A. unauthorized exposure of sensitive information
2. virtualized environment	B. protection of data through cryptographic methods
3. cloud service provider	C. ensuring systems remain operational despite failures
4. shared responsibility model	D. a model defining security responsibilities between providers and users
5. data encryption	E. techniques used to reduce security threats
6. access management	F. a computing model providing on-demand resources
7. data breach	G. an environment created using virtualization technologies
8. redundancy	H. an organization delivering cloud-based services
9. availability	I. the degree to which systems are accessible and operational
10. risk mitigation	J. management of user identities and permissions

Task 2. Match the term with the correct Ukrainian translation.

Terms	Translation
1. cloud computing	A. модель спільної відповідальності
2. virtualized environment	B. шифрування даних
3. cloud service provider	C. доступність
4. shared responsibility model	D. управління доступом
5. data encryption	E. надмірність
6. access management	F. витік даних
7. data breach	G. хмарні обчислення
8. redundancy	H. віртуалізоване середовище

Terms	Translation
9. availability	I. постачальник хмарних послуг
10. risk mitigation	J. зменшення ризиків

Task 3. Complete the sentences with the correct word from the box

computing cloud, environment virtualized, provider cloud service, model responsibility, shared encryption data, management access, breach data, redundancy, availability, mitigation risk

- Many companies are migrating their servers to _____ to reduce infrastructure costs.
- A _____ allows multiple virtual machines to run on a single physical server.
- Organizations must choose a reliable _____ to ensure high-quality cloud services.
- In the _____, both the provider and the client share security responsibilities.
- Sensitive data must always be protected using _____.
- _____ ensures that only authorized users can access cloud resources.
- A _____ can cause severe financial and reputational damage to a business.
- _____ mechanisms ensure services remain available even if one component fails.
- _____ measures ensure systems are accessible when users need them.
- Companies implement _____ to identify and reduce potential security threats.

Task 4. Reading

Cloud Computing & Security

Cloud computing has transformed the way organizations deploy and manage information systems by providing on-demand access to computing resources within a virtualized environment. Instead of maintaining physical infrastructure, organizations rely on a cloud service provider to deliver services such as IaaS, PaaS, and SaaS. This model offers significant advantages, including cost efficiency, flexibility, and scalability.

However, cloud environments introduce complex cybersecurity challenges. The shared responsibility model defines security obligations between providers and customers. While providers secure the underlying infrastructure, customers are responsible for data protection, access management, and compliance with regulatory standards. Failure to implement strong security controls may result in a data breach, exposing sensitive information.

To reduce risks, cloud systems employ data encryption, both during transmission and storage. Redundancy mechanisms ensure high availability, even in the event of hardware failure. Additionally, cloud platforms must comply with strict compliance requirements, particularly in sectors handling personal or financial data.

Effective risk mitigation strategies include continuous monitoring, identity management, and regular security audits. When properly implemented, cloud computing can provide secure and resilient infrastructures suitable for modern business and cybersecurity operations.

Task 5. Decide whether each statement is True or False.

1. Cloud computing allows organizations to scale resources on demand.
2. A virtualized environment always eliminates the need for physical servers.
3. Data breaches only happen due to weak passwords.

4. The shared responsibility model clarifies which security tasks are the provider's and which are the user's.
5. Data encryption ensures that data cannot be lost.
6. Redundancy improves system availability by duplicating critical resources.
7. Access management controls who can access which cloud resources.
8. Risk mitigation is only necessary in large enterprises.
9. Availability refers to the uptime and accessibility of cloud services.
10. Cloud service providers are always responsible for user mistakes.

Grammar: Present Perfect vs Past Simple

Task 6. Complete the sentences with the correct form of the verb in brackets (Present Perfect or Past Simple).

1. Companies _____ (migrate) their data to the cloud last year.
2. Engineers _____ (monitor) the virtualized environment continuously since Monday.
3. The IT department _____ (apply) the latest security patch yesterday.
4. Providers _____ (deliver) cloud services to clients for over 10 years.
5. Hackers _____ (exploit) several system vulnerabilities in the past month.
6. The company _____ (implement) redundancy systems to improve availability last quarter.
7. Sensitive data _____ (encrypt) before being uploaded to the cloud.
8. The security team _____ (detect) unusual activity on the server last night.
9. Cloud computing _____ (become) a standard solution for enterprises in the last decade.

10. Administrators _____ (update) access permissions many times this week.

Task 7. Replace the underlined word/phrase with an appropriate synonym.

1. Cloud computing **provides** on-demand resources. → _____
2. Sensitive data must be **protected** with encryption. → _____
3. Access management **controls** permissions. → _____
4. Redundancy **ensures** service continuity. → _____
5. A data breach **occurs** when information is exposed. → _____
6. Virtualized environments **allow** multiple OS instances. → _____
7. Risk mitigation **reduces** potential threats. → _____
8. Providers **deliver** cloud services globally. → _____
9. Availability **refers** to system uptime. → _____
10. Shared responsibility **defines** security duties. → _____

Task 8. Complete the sentences using the correct form of the verb in brackets and make First or Second Conditional as appropriate.

1. If a company _____ (neglect) regular software updates, it _____ (risk) a serious data breach.
2. If hackers _____ (find) a vulnerability in the system, they _____ (exploit) it immediately.
3. Cloud services _____ (fail) if the provider _____ (not maintain) redundancy systems.
4. If sensitive data _____ (encrypt) properly, unauthorized users _____ (not access) it.
5. If the IT team _____ (monitor) the network continuously, threats _____ (be detected) faster.
6. The company would save costs if it _____ (migrate) more applications to the cloud.

7. If users _____ (follow) security protocols, phishing attacks _____ (be less successful).
8. Providers _____ (improve) service availability if they _____ (increase) server capacity.
9. If a system administrator _____ (grant) too many permissions, the network _____ (become) vulnerable.
10. Organizations would avoid downtime if they _____ (implement) proper backup strategies.

Task 9. Choose a topic from the given below prepare a presentation (5-7 slides).

1. Evaluating the Advantages and Disadvantages of Cloud Computing in IT Security (Analyze benefits like scalability and remote access vs risks such as data leakage and compliance issues.)
2. Optimizing Resource Utilization Through Virtualized Environments (Explore how virtualization enhances server efficiency, reduces costs, and introduces security challenges.)
3. The Strategic Role of Cloud Service Providers in Ensuring Cybersecurity (Examine responsibilities, SLAs, security tools, and incident response management.)
4. Deep Dive into the Shared Responsibility Model in Cloud Security (Clarify which security tasks are handled by providers vs customers, and real-world implications.)
5. Data Encryption Techniques and Their Real-World Applications (Compare symmetric, asymmetric, and homomorphic encryption with practical enterprise examples.)
6. Access Management Best Practices for Enterprise Cloud Systems (Focus on identity management, multi-factor authentication, role-based access control, and monitoring.)

7. Case Studies of Major Data Breaches: Analysis and Lessons Learned
(Study high-profile breaches to understand attack vectors, prevention strategies, and regulatory consequences.)
8. Redundancy and Failover Strategies to Maximize Cloud Service Availability
(Discuss backup solutions, load balancing, disaster recovery, and minimizing downtime.)
9. Implementing Risk Mitigation Frameworks in Cloud Cybersecurity
(Explore NIST, ISO 27001, and CIS controls to reduce vulnerabilities and manage threats.)
10. Emerging Trends in Cloud Computing and Next-Generation Security Technologies
(Look at AI-driven security, zero-trust architectures, container security, and hybrid/multi-cloud strategies.)

Task 10. Watch the video and decide whether the statements are True (T) or False (F).

Video: <https://www.youtube.com/watch?v=PT-saj5qGkk>

1. Cloud computing means storing and running data or applications on remote servers accessed via the internet instead of on a local computer.
2. In cloud computing, users must always own the physical servers where their data is stored.
3. Cloud services allow access to computing resources such as storage, servers, and software on demand.
4. One major benefit of cloud computing is that it can reduce upfront investment in physical infrastructure.
5. The cloud only works when applications are installed directly on the user's device.
6. Cloud computing can be organized into different service models such as SaaS, PaaS, and IaaS.

7. Security concerns can arise in the cloud because data is stored and processed outside the end user's direct control.
8. Cloud computing offers no flexibility in scaling resources according to changing needs.
9. Cloud security requires measures such as encryption and access controls to protect cloud-based assets.
10. Cloud computing does not support businesses and individuals in accessing applications from different devices over the internet.

Module 2. Cybersecurity and Modern Threats

Lesson 1. Cyber Threats & Attacks

WORDBANK

Term	Translation
1. exponential growth	експоненційне зростання
2. unauthorized access	несанкціонований доступ
3. disrupt services	порушення роботи сервісів
4. demand financial ransom	вимагати фінансову винагороду
5. malware	шкідливе програмне забезпечення
6. ransomware	програмне забезпечення-вимагач
7. compromise system integrity	порушити цілісність системи
8. human psychology exploitation	використання психології людини
9. multi-layered defense strategy	багаторівнева стратегія захисту
10.intrusion detection systems	системи виявлення вторгнень
11.potential vulnerabilities	потенційні вразливості
12.operational efficiency	ефективність роботи
13.critical digital assets	критично важливі цифрові активи
14.emerging threats	нові/виникаючі загрози
15.ongoing vigilance	постійна пильність
16.exploit software vulnerabilities	використання вразливостей ПЗ
17.remove malicious programs	видаляти шкідливі програми

Task 1. Match the term with the correct definition.

English Term / Phrase	Definition
1. exponential growth	A) Convincing people to ignore security rules by manipulating their behavior
2. unauthorized access	B) Using weaknesses in software to attack a system
3. disrupt services	C) Gaining access to a system or data without permission
4. demand financial ransom	D) Interrupting normal operation of services or applications
5. malware	E) Demanding money in exchange for restoring access or data
6. human psychology exploitation	F) Rapid increase in size, number, or importance
7. multi-layered defense strategy	G) Weak points in a system that could be exploited by attackers
8. intrusion detection systems	H) Software designed to harm, damage, or gain unauthorized access to a system
9. potential vulnerabilities	I) Systems that monitor networks for suspicious or unusual activity
10. exploit software vulnerabilities	J) A structured approach using multiple security measures to protect systems

Task 2. Match the term with the correct Ukrainian translation.

Term	Ukrainian Translation
1. multi-layered defense strategy	A) хмарні обчислення
2. intrusion detection systems	B) системи безпеки на базі штучного інтелекту
3. disrupt services	C) порушити цілісність системи
4. exponential growth	D) нові/виникаючі загрози
5. potential vulnerabilities	E) видаляти шкідливі програми
6. remove malicious programs	F) експоненційне зростання
7. critical digital assets	G) кіберзагрози
8. exploit software vulnerabilities	H) фішингові атаки
9. human psychology exploitation	I) багаторівнева стратегія захисту
10.demand financial ransom	J) використання психології людини
11.malware	K) вимагати фінансову винагороду
12.ransomware	L) критично важливі цифрові активи
13.compromise system integrity	M)потенційні вразливості
14.cyber threats	N) системи виявлення вторгнень
15.operational efficiency	O) ефективність роботи
16.emerging threats	P) порушення роботи сервісів
17.ongoing vigilance	Q) програмне забезпечення-вимагач
18.phishing attacks	R) шкідливе програмне забезпечення
19.AI-driven security systems	S) використання вразливостей ПЗ
20.cloud computing	T) багаторівнева стратегія захисту

Task 3. Fill the gaps using words from the box

multi-layered defense strategy, intrusion detection systems, disrupt services, exponential growth, potential vulnerabilities, removes malicious programs, critical digital assets, exploit software vulnerabilities, human psychology exploitation, demand financial ransom

1. The Internet has grown so fast that the _____ of connected devices is creating new challenges.
2. Last year, cybercriminals _____ several companies' systems to steal confidential data.
3. Many organizations are implementing a _____ to protect their networks from multiple threats.
4. Firewalls and antivirus software _____ before malware can damage important files.
5. Social engineers often use _____ to trick employees into revealing sensitive information.
6. If security rules are ignored, it can lead to _____, stopping important business operations.
7. The company had to pay because hackers _____ after encrypting all the files.
8. Advanced AI systems will soon be able to predict _____ in real time.
9. Protecting _____ is a top priority for all modern organizations.
10. Cybersecurity teams are constantly monitoring networks with _____ to detect suspicious behavior.

Task 4. Reading

Cybersecurity and Modern Threats

In today's digital world, cybersecurity has become one of the most important concerns for individuals, organizations, and governments. The rapid exponential growth of the internet, cloud computing, and connected devices has created an environment where cyber threats are increasingly sophisticated and widespread. Cybercriminals exploit software vulnerabilities, human mistakes, and organizational weaknesses to gain unauthorized access, steal sensitive information, disrupt services, or demand financial ransom.

One of the most common threats is malware, which includes viruses, worms, spyware, and trojans designed to compromise system integrity. Phishing attacks often use fake emails or websites to trick users into revealing login credentials or bank details. Ransomware is a particularly serious type of malware that encrypts files and demands a ransom, leaving victims with few options. Social engineering, on the other hand, targets human psychology exploitation rather than technical vulnerabilities, convincing employees to ignore security policies or share confidential information.

To counter these threats, organizations must adopt a multi-layered defense strategy. Firewalls control incoming and outgoing network traffic, antivirus software removes malicious programs, and intrusion detection systems monitor for unusual behavior. Additional measures include strong password policies, two-factor authentication, regular system updates, and encryption of sensitive data. Employee training is also crucial, as staff who recognize phishing attempts, suspicious links, or abnormal network activity act as a key line of defense.

Advanced technologies such as artificial intelligence (AI) and machine learning (ML) offer both opportunities and challenges. AI-driven security systems can automatically detect threats, analyze patterns of suspicious activity, and predict potential vulnerabilities. However, cybercriminals can use these same technologies to develop adaptive malware capable of evading traditional

defenses. Cloud computing has improved operational efficiency and accessibility, but it requires strict data protection policies, secure authentication, and continuous monitoring.

Overall, cybersecurity is a dynamic and constantly evolving field. Protecting critical digital assets demands proactive strategies, ongoing vigilance, and collaboration between technical experts, policymakers, and users to stay ahead of emerging threats.

Task 5. Decide whether each statement is True (T) or False (F).

1. Cybersecurity is mainly a concern for large corporations.
2. Malware includes viruses, spyware, and worms.
3. Phishing attacks target system vulnerabilities rather than human behavior.
4. Ransomware typically encrypts files and demands payment.
5. Social engineering relies on manipulating human psychology.
6. Firewalls prevent unauthorized network traffic.
7. Employee training is optional if advanced software is installed.
8. AI can be used to detect patterns of suspicious activity.
9. Cybercriminals cannot exploit AI for malicious purposes.
10. Cloud computing increases efficiency but requires strong security policies.

Task 6. Multiple Choice (choose the correct answer).

1. What is the primary goal of cybercriminals?
 - a) Improve security
 - b) Access, steal, or disrupt data
 - c) Train employees
 - d) Update firewalls
2. Which technology can detect patterns of suspicious activity?
 - a) Cloud storage
 - b) Machine learning

c) Email filters

d) Password managers

3. Why is social engineering dangerous?

a) It can bypass firewalls

b) It exploits human behavior

c) It encrypts data

d) It blocks network traffic

4. Ransomware attacks usually result in:

a) loss of access to files

b) detection of malware

c) password protection

d) human error

5. Employee awareness helps in:

a) reducing system updates

b) preventing phishing and human errors

c) encrypting all data automatically

d) replacing firewalls

6. Which is NOT a type of malware?

a) Trojan

b) Worm

c) Firewall

d) Spyware

7. Cloud computing requires:

a) no security measures

b) strong authentication and monitoring

c) only firewalls

d) only antivirus

8. AI in cybersecurity can:

a) only automate updates

b) predict potential vulnerabilities

- c) eliminate the need for employees
 - d) replace all traditional software
9. Human error is considered:
- a) an irrelevant factor
 - b) a major exploited vulnerability
 - c) a software weakness
 - d) always avoidable
10. A multi-layered defense combines:
- a) technical tools and human vigilance
 - b) only AI-based tools
 - c) only employee training
 - d) only firewalls

Task 7. Complete the sentences using words from the text

cybercriminals, malware, phishing, ransomware, social engineering, AI, cloud, encryption, firewall, vulnerability

1. _____ often exploits weaknesses in human behavior, manipulating employees or users to bypass security protocols and reveal sensitive information.
2. _____ is a method of converting data into unreadable code, ensuring that even if unauthorized parties access it, they cannot read the information.
3. _____ attacks are carefully designed to trick users into revealing passwords, credit card numbers, or other personal information through fake emails or websites.
4. _____ encrypts important files on a user's system and demands a ransom for their release, often causing major operational disruption.
5. _____ are continually developing more sophisticated cyber threats, combining technical skills and creativity to bypass traditional security measures.
6. Advanced _____ technologies can analyze patterns in network traffic and predict suspicious activity before it causes damage.

7. Many organizations store their data on the _____ to improve scalability, accessibility, and operational efficiency across multiple locations.
8. A _____ monitors and filters incoming and outgoing network traffic, blocking malicious activity and protecting the system from attacks.
9. _____ includes viruses, trojans, worms, and spyware, all designed to compromise the integrity and security of computer systems.
10. Any weakness in a system that can be exploited by attackers is a _____, and identifying it is essential for maintaining cybersecurity.

Task 8. Replace the underlined words with suitable synonyms from the text.

1. Cybercriminals are **continuously creating** new malware.
2. Employees should be **aware** of phishing attempts.
3. AI systems can **forecast** potential threats.
4. Firewalls **control** network traffic.
5. Ransomware **locks** files until payment is made.
6. Social engineering **uses** human psychology to attack systems.
7. Organizations implement **many-layered** defense strategies.
8. Vulnerabilities are **weak points** in systems.
9. Training helps employees **understand** cyber risks.
10. Cloud computing improves **effectiveness** but requires security.

Speaking

Task 9. – Critical Thinking / Discussion (10 prompts)

1. How might AI both improve and threaten cybersecurity?
2. Should organizations prioritize technology over training? Why or why not?
3. Which is more dangerous: human error or malware?
4. How can phishing attacks be prevented?
5. Why is social engineering so effective despite technological defenses?
6. What role do firewalls play in multi-layered defense?

7. How can organizations balance cloud efficiency and security?
8. Can ransomware attacks be completely prevented?
9. What skills should cybersecurity experts have?
10. How can constant vigilance be implemented practically?

Task 10. Watch 2 videos and decide if sentences are True (T) or False (F)

Video 1: <https://www.youtube.com/watch?v=ey4dXseAODE>

Video 2: <https://www.youtube.com/watch?v=inWWhr5tnEA>

1. Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
2. Cybersecurity is only important for large companies and governments, not individuals.
3. Malware refers to harmful software such as viruses, worms, and Trojan horses that can damage systems.
4. Phishing is a type of attack that tries to trick users into revealing personal information.
5. Ransomware encrypts files and demands payment to restore access.
6. Strong passwords and regular software updates can help improve cybersecurity.
7. Denial-of-service attacks aim to overwhelm a system so that legitimate users can't access it.
8. Cybersecurity only involves technical tools and does not include training users about safe behavior.
9. Protecting data integrity means preventing unauthorized modification or deletion of data.
10. A multi-layered defense with firewalls, antivirus software, and access controls is a key principle of cybersecurity.

Lesson 2. Internet Security & Encryption

WORDBANK

Term	Translation
1. confidentiality	конфіденційність
2. integrity	цілісність
3. availability	доступність
4. encryption	шифрування
5. decryption key	ключ дешифрування
6. AES (Advanced Encryption Standard)	СПШ (Стандарт передового шифрування)
7. RSA	АШ (Алгоритм шифрування)
8. VPN (Virtual Private Network)	віртуальна приватна мережа
9. HTTPS websites	вебсайти з HTTPS
10. firewalls	брандмауери
11. antivirus software	антивірусне програмне забезпечення
12. multi-factor authentication	багатофакторна автентифікація
13. phishing	фішинг
14. ransomware	вимагач (програма-вимагач)
15. denial-of-service attacks	атаки відмови в обслуговуванні
16. software updates	оновлення програмного забезпечення
17. cloud security	хмарна безпека
18. data encryption	шифрування даних
19. access control	контроль доступу
20. network monitoring	моніторинг мережі
21. security policies	політики безпеки

Task 1. Match the term with the correct definition.

Term	Definition
1. confidentiality, integrity, availability	A) A set of rules and procedures designed to protect information and systems
2. encryption	B) Online systems used to store and manage data on remote servers
3. firewalls	C) A method of converting data into a coded form to prevent unauthorized access
4. antivirus software	D) Principles that ensure data is secure, accurate, and accessible
5. multi-factor authentication	E) Software that detects and removes malicious programs
6. phishing	F) Security system that monitors and controls incoming and outgoing traffic
7. ransomware	G) A cyberattack that tricks users into revealing sensitive information
8. denial-of-service attacks	H) Malicious software that blocks access to data until a payment is made
9. cloud platforms	I) An attack that overloads a system to make it unavailable
10. security policy	J) A method of verifying identity using multiple forms of authentication

Task 2. Match the term with the correct Ukrainian translation.

Term	Ukrainian Translation
1. Internet security	A) шифрування
2. encryption	B) брандмауер
3. unauthorized access	C) інтернет-безпека
4. cyberattacks	D) несанкціонований доступ
5. malware	E) кібератаки
6. firewall	F) шкідливе програмне забезпечення
7. antivirus software	G) антивірусне програмне забезпечення
8. multi-factor authentication	H) багатофакторна автентифікація
9. phishing	I) фішинг
10.ransomware	J) програма-вимагач
11.cloud security	K) хмарна безпека
12.access control	L) контроль доступу
13.network monitoring	M)моніторинг мережі

Task 3. Fill the gaps using words from the box.

ransomware, integrity, cloud platforms, phishing, firewall, security policy, encryption, availability, multi-factor authentication, antivirus software, denial-of-service attacks, confidentiality

1. Ensuring the _____ of data means that information is only accessible to authorized users.
2. The company uses _____ to convert sensitive data into a secure coded format.
3. A _____ helps protect a network by controlling incoming and outgoing traffic.
4. Installing _____ is essential to detect and remove malicious programs from a computer.

5. _____ requires users to verify their identity using more than one method.
6. Many cybercriminals use _____ emails to trick people into sharing personal information.
7. _____ can block access to important files until a ransom is paid.
8. Websites may crash due to _____ that overload servers with excessive traffic.
9. More businesses are storing their data on _____ to ensure flexibility and remote access.
10. Every organization should implement a strong _____ to protect its digital resources.

Task 4. Reading.

Internet Security & Encryption

Internet security is a critical aspect of modern information technology that protects data, devices, and networks from unauthorized access, cyberattacks, and malware. As more personal and business activities are conducted online, ensuring the confidentiality, integrity, and availability of digital information has become essential. One of the main tools used to secure online communications is encryption. Encryption is the process of converting readable data into a coded format to prevent unauthorized access, ensuring that only someone with the correct decryption key can read or use the information. This ensures that even if data is intercepted during transmission, it remains unreadable to unauthorized users. Common encryption methods include AES (Advanced Encryption Standard) and RSA, which are widely implemented in VPNs (Virtual Private Networks), HTTPS websites, and email communications.

Effective internet security also requires the use of firewalls, antivirus software, and multi-factor authentication to prevent unauthorized access and reduce the risk of cyber threats such as phishing, ransomware, and denial-of-

service attacks. In addition, regular software updates and user awareness play a significant role in maintaining a secure digital environment.

Furthermore, organizations increasingly adopt cloud security measures to protect data stored in remote servers. Data encryption, access control, and network monitoring are essential to prevent breaches in cloud platforms.

Implementing security policies and educating employees about potential risks strengthens overall cybersecurity. By combining advanced encryption techniques, proactive monitoring, and strong organizational practices, both individuals and businesses can maintain a safe and trustworthy online presence.

Task 5. Decide whether each statement is True (T) or False (F).

1. Internet security protects only computers from cyber threats.
2. Confidentiality, integrity, and availability are essential principles of internet security.
3. Encryption converts coded data into readable information.
4. Encrypted data cannot be read without the correct decryption key.
5. AES and RSA are examples of encryption methods.
6. Firewalls and antivirus software are not necessary for internet security.
7. Phishing and ransomware are types of cyber threats.
8. Multi-factor authentication uses only one method to verify identity.
9. Cloud platforms store data on remote servers.
10. Security policies and employee education help improve cybersecurity.

Grammar Focus: Modal Verbs

Task 6. Complete the sentences using the correct modal verb: must, should, might, can't, could.

1. Users _____ update their passwords regularly to prevent unauthorized access.
2. Emails from unknown sources _____ be phishing attempts.
3. You _____ ignore security warnings on your device.

4. Sensitive data _____ be encrypted before being sent online.
5. Firewalls _____ protect networks from external threats.
6. Hackers _____ gain access if a system is not properly secured.
7. Employees _____ follow the company's security policies at all times.
8. Multi-factor authentication _____ make accounts safer than passwords alone.
9. Malware _____ cause serious damage to your files.
10. Cloud platforms _____ store sensitive data safely if proper security measures are used.

Task 7. Translate into English using Modal verbs in correct tense (can, must, should, may).

1. Користувачі повинні регулярно оновлювати антивірусне програмне забезпечення, щоб захистити свої пристрої.
2. Дані повинні бути зашифровані перед передачею через Інтернет.
3. Електронні листи від незнайомих джерел можуть бути фішинговими атаками.
4. Брандмауер може захищати мережу від несанкціонованого доступу.
5. Співробітники повинні дотримуватися політики безпеки компанії.
6. Хакери можуть отримати доступ до даних, якщо система недостатньо захищена.
7. Багатофакторна автентифікація може робити облікові записи більш безпечними.
8. Хмарні платформи можуть зберігати дані безпечно, якщо застосовані належні заходи безпеки.
9. Програми-вимагачі можуть завдати серйозної шкоди файлам користувача.
10. Якщо користувачі не будуть уважні, вони можуть стати жертвами кібератаки.

Task 8. Combine the sentences using relative pronouns(who, which, that) and correct IT/cybersecurity vocabulary.

1. Encryption protects data. Encryption is used in VPNs.
2. The hacker stole personal information. The hacker was arrested last week.
3. Firewalls block malicious traffic. Firewalls are installed on all company servers.
4. Antivirus software detects malware. Antivirus software is installed on all computers.
5. Multi-factor authentication improves security. Multi-factor authentication requires multiple verification methods.
6. Ransomware encrypted files. Ransomware caused serious damage to the company.
7. Cloud platforms store sensitive data. Cloud platforms are managed by trusted providers.
8. Cybersecurity policies protect organizations. Cybersecurity policies are followed by all employees.
9. Data is transmitted online. Data must be encrypted to remain secure.
10. Phishing emails target users. Phishing emails try to steal passwords and personal information.

Task 9. Replace the underlined words with suitable synonyms.

cyber threats, deployed, encrypted format, maintaining, secure, online security framework, safeguarding, applied, access, digital assets, protect, decrypt, secure digital footprint, security, ensuring

1. Internet security safeguards **data, devices, and networks** from unauthorized access.
2. Ensuring the **protection** of digital information is critical.
3. Encryption transforms readable data into a **coded format** to prevent unauthorized access.

4. Only someone with the correct decryption key can **interpret** the information.
5. Common encryption standards such as AES and RSA are widely **implemented** in VPNs, HTTPS websites, and email systems.
6. Firewalls, antivirus software, and multi-factor authentication minimize the risk of **cyberattacks**.
7. Regular software updates and user awareness are crucial for **sustaining** a secure digital environment.
8. Organizations adopt cloud security measures to **safeguard** data stored in remote servers.
9. Applying comprehensive security policies strengthens overall **cybersecurity posture**.
10. Combining advanced encryption methods, proactive monitoring, and robust practices allows individuals and businesses to maintain a **trustworthy online presence**.

Task 10. Speaking Task – Dialogue: Cybersecurity in the Workplace.

Characters: IT Manager (Alex) & Employee (Maria)

Fill the dialogue with these words:

cyber threats, deployed, encrypted format, maintaining, secure, online security framework, safeguarding, applied, access, digital assets, protect, decrypt, secure digital footprint, security, ensuring

Maria: Hi Alex, I wanted to ask about our company's data. How do we make sure our _____ are safe?

Alex: That's a good question. First, we have a strong _____ in place. All sensitive files are stored in _____, so even if someone intercepts them, they cannot _____ the data without the key.

Maria: That sounds reassuring. But what about the employees? How do we control _____ to this information?

Alex: We use multi-factor authentication and strict permission policies. This helps in _____ sensitive information. Only authorized personnel can _____ certain files.

Maria: And the firewalls and antivirus?

Alex: They have already been _____ across all servers and workstations. These tools help in _____ our network from _____ like phishing or ransomware.

Maria: I see. So, maintaining these systems is also important, right?

Alex: Absolutely. _____ and regularly updating software is crucial. It's also about _____ that all employees follow best practices for _____.

Maria: What about our online presence? Can our actions affect security outside the company?

Alex: Definitely. We all need to manage a _____. Careless online behavior can expose the company to risks. By following policies and good habits, we _____ both personal and corporate data.

Maria: This makes sense. So, by combining technical tools and employee awareness, we are really _____ our information and _____ our operations.

Alex: Exactly. Cybersecurity is not just about technology—it's about people, processes, and _____ that our _____ remain safe from all _____.

Task 11. Choose a topic from the given below prepare a presentation (5-7 slides).

1. The Role of Encryption in Protecting Online Communications
– Explore how AES, RSA, and other encryption standards secure data.
2. Cyber Threats and How to Prevent Them
– Discuss phishing, ransomware, denial-of-service attacks, and countermeasures.

3. Firewalls, Antivirus Software, and Multi-Factor Authentication: Tools for Internet Security – Examine how these technologies protect networks and devices.
4. The Importance of Data Confidentiality, Integrity, and Availability – Explain the CIA triad and its application in real-world cybersecurity.
5. Cloud Security: Protecting Data on Remote Servers – Focus on encryption, access control, and monitoring in cloud platforms.
6. Maintaining a Secure Digital Footprint in the Age of Social Media – Discuss personal cybersecurity practices and online privacy.
7. Cybersecurity Policies: Creating a Safe Online Environment for Organizations – Explore policy implementation, employee training, and compliance.
8. The Evolution of Encryption Techniques and Standards – Trace the development from classical ciphers to modern encryption algorithms.
9. What steps individuals and organizations should take to stay safe online – Analyze steps individuals and organizations should take to stay safe online.
10. Future Trends in Internet Security and Encryption – Discuss AI in cybersecurity, quantum encryption, and emerging threats.

Lesson 3. Network Security & Firewalls

WORDBANK

Term	Translation
1. network security	мережева безпека
2. firewall protection	захист міжмережевим екраном
3. unauthorized access	несанкціонований доступ
4. inbound traffic	вхідний трафік
5. outbound traffic	вихідний трафік
6. security policy	політика безпеки
7. packet filtering	фільтрація пакетів даних
8. Intrusion Prevention System (IPS)	Система Запобігання Вторгненням (СЗВ)
9. access control rules	правила контролю доступу
10. malware	шкідливе програмне забезпечення
11. data breach	витік даних
12. authentication process	процес автентифікації
13. Virtual Private Network (VPN)	Віртуальна Приватна Мережа (ВПМ)
14. threat detection	виявлення загроз
15. real-time monitoring	моніторинг у реальному часі

Task 1. Match the term with the correct definition.

Term	Definition
1. Malware	A) A secure encrypted connection that allows users to access a private network over the internet
2. Network security	B) Protection of computer networks from cyber threats, attacks, and unauthorized access
3. Authentication process	C) Software designed to damage, disrupt, or gain unauthorized access to computer systems
4. Data breach	D) A system that monitors network activity and automatically blocks or prevents suspicious behavior
5. Security policy	E) A set of rules and procedures designed to protect information and systems
6. Packet filtering	F) A method of inspecting data packets and deciding whether they should be allowed or blocked
7. Unauthorized access	G) Access to a system or data without permission or legal authorization
8. Firewall protection	H) The process of verifying the identity of a user before granting access to a system
9. Intrusion Prevention System (IPS)	I) An incident where sensitive or protected data is exposed to unauthorized users
10. Virtual Private Network (VPN)	J) A security mechanism that monitors and filters incoming and outgoing network traffic based on rules

Task 2. Match the term with the correct Ukrainian Translation.

Term	Ukrainian Translation
1. Network security	A) система, що перевіряє особу користувача перед наданням доступу
2. Malware	B) захист комп'ютерних мереж від кібератак і несанкціонованого доступу
3. Firewall protection	C) віртуальна приватна мережа, що забезпечує захищене з'єднання через інтернет
4. Authentication process	D) програмне забезпечення, призначене для шкоди або несанкціонованого доступу
5. Data breach	E) метод перевірки пакетів даних для їх дозволу або блокування
6. Security policy	F) інцидент, під час якого дані стають доступними неавторизованим користувачам
7. Packet filtering	G) система правил і процедур для захисту інформації та систем
8. Unauthorized access	H) механізм безпеки, що контролює мережевий трафік і блокує підозрілу активність
9. Intrusion Prevention System (IPS)	I) доступ до системи без дозволу або авторизації
10. Virtual Private Network (VPN)	J) система безпеки, що контролює та фільтрує вхідний і вихідний трафік

Task 3. Reading.

Network Security & Firewalls

Network security is a fundamental component of modern cybersecurity infrastructure, designed to protect computer systems, networks, and sensitive data from unauthorized access and cyber threats. One of the most important tools used in this area is a firewall, which acts as a security layer between a trusted internal network and untrusted external networks such as the Internet.

A firewall monitors and controls inbound and outbound traffic based on predefined security policies. It uses packet filtering techniques and access control rules to determine whether data packets should be allowed or blocked. By analyzing traffic patterns, firewalls help prevent malicious software from entering the system and reduce the risk of data breaches.

Modern firewalls are often integrated with intrusion prevention systems (IPS), which provide real-time monitoring and threat detection. These systems can identify suspicious activity and automatically respond to potential attacks. In addition, encrypted communication and virtual private networks (VPNs) enhance security by protecting data during transmission.

Effective network security also depends on proper authentication processes, ensuring that only authorized users can access sensitive resources. Organizations must regularly update their security policies to address system vulnerabilities and emerging cyber threats.

In conclusion, firewalls play a critical role in maintaining secure digital environments. They act as the first line of defense in cybersecurity, helping organizations protect their data, systems, and users from constantly evolving cyber risks.

Answer the questions according to the text.

1. What is the main purpose of network security in modern cybersecurity systems?
2. How does a firewall protect a computer network from external threats?

3. What is the difference between inbound and outbound traffic in a network?
4. How do packet filtering techniques work in firewall systems?
5. What role does an Intrusion Prevention System (IPS) play in network security?
6. Why is authentication important in controlling access to network resources?
7. How do VPNs and encrypted communication improve data protection?

Task 4. Decide whether each statement is True (T) or False (F).

1. Network security protects computer systems and data from cyber threats and unauthorized access.
2. Firewalls only allow incoming traffic and block all outgoing traffic.
3. A firewall acts as a security layer between internal and external networks.
4. Packet filtering is used to automatically create malware inside a system.
5. Firewalls use predefined security policies and access control rules.
6. Intrusion Prevention Systems (IPS) provide real-time monitoring and threat detection.
7. VPNs increase security by encrypting data during transmission.
8. Authentication processes allow any user to access sensitive resources without restrictions.

Task 5. Read the text and fill it with the correct prepositions.

*for (4), from (2), on (3), between (1), by (2), into (1), of (1), in (2), to (4),
via (1), over (1)*

Network security is essential ____ protecting modern IT systems ____ cyber threats and unauthorized access. Organizations rely ____ firewalls to control traffic ____ internal and external networks. A firewall works ____ filtering data packets and applying strict security rules ____ each connection attempt. It helps

prevent malicious software from entering ____ the system and reduces the risk ____ data breaches.

In addition, intrusion prevention systems operate ____ real time to detect suspicious activity ____ the network. These systems respond ____ potential attacks automatically. Users often connect ____ remote systems ____ virtual private networks (VPNs), which ensure encrypted communication ____ the internet. Authentication processes are also important ____ granting access ____ sensitive resources only ____ authorized users. Overall, network security depends ____ multiple layers of protection working together ____ ensure data integrity and system safety.

Grammar Focus: Passive Voice

Task 6. Fill in the gaps with the correct Passive Voice form (Present Perfect, Future Simple, Present Continuous, Past Continuous, Past Perfect, Modals).

Network security systems have significantly improved in recent years. Today, most corporate networks ____ already ____ (protect) by multi-layered firewalls and intrusion prevention systems.

Currently, all inbound and outbound traffic ____ continuously ____ (monitor) to ensure real-time threat detection. Sensitive data ____ always ____ (encrypt) before transmission, especially in cloud-based environments.

At the same time, new security policies ____ regularly ____ (update) by administrators to respond to emerging cyber risks. If suspicious behavior is identified, it ____ immediately ____ (detect) and analyzed by security systems.

During a recent attack, several network segments ____ actively ____ (configure) to isolate the affected areas, while the incident ____ thoroughly ____ (investigate) by cybersecurity experts.

In the future, all critical infrastructure ____ (must / protect) by AI-driven security systems, and cyber threats ____ automatically ____ (block) before they reach internal networks. By the time administrators responded, the system logs ____ already ____ (analyze) to determine the origin of the breach.

Task 7. Replace the underlined phrases with suitable synonyms.

monitor, firewall protection, encrypt, data breach, authentication process, detect, traffic inspection, unauthorized access, block, network security

1. Modern **protection of computer networks against cyber threats and attacks** is a fundamental requirement for all organisations operating in the digital environment.
2. A properly configured **system that filters and controls incoming and outgoing network traffic** acts as the first defensive barrier between internal systems and external threats.
3. Security tools continuously **observe and analyse data flow across the network infrastructure** to ensure compliance with organisational security policies.
4. Intrusion prevention systems are designed to **identify suspicious activities and cyberattack patterns in real time** within complex digital environments.
5. All sensitive information must be **converted into a secure coded format** before being transmitted over public or unsecured communication channels.
6. Cybersecurity mechanisms are capable of instantly **preventing harmful data packets from entering protected systems** during potential attack attempts.
7. A severe **incident involving the exposure of confidential or sensitive data to unauthorised users** can seriously damage organisational reputation and trust.

8. Strong **procedures for verifying the identity of users before granting system access** are essential in protecting critical resources.
9. Continuous **systematic analysis of network communication and data flow** helps administrators identify vulnerabilities and prevent cyber threats.
10. Hackers often attempt **illegal entry into secure systems without permission or authorisation** in order to exploit or steal valuable data.

Speaking

Task 8. Watch the video and decide whether the statements are True (T) or False (F).

Video: <https://www.youtube.com/watch?v=kDEX1HXybrU>

1. A firewall is used to prevent unauthorized access to a private network.
2. Firewalls allow all incoming traffic without any restrictions.
3. A firewall works by filtering network traffic based on security rules.
4. Firewalls can block unwanted or malicious traffic from entering a system.
5. The main purpose of a firewall is to increase internet speed.
6. Firewalls act as a barrier between a trusted internal network and the internet.
7. Firewalls cannot control outgoing traffic from a network.
8. Network administrators define rules that determine what traffic is allowed or denied.
9. Firewalls are only used in small personal computers, not in organizations.
10. A firewall helps protect a network from hackers and cyber threats.

Task 9. Fill in the gaps in a dialogue using wordbank.

*system, network security, traffic, allow, monitor, encrypt, cyber threats,
firewall, internal network, detect, external network, rules, block,
unauthorized access*

Alex: I've been studying cybersecurity, but I still don't fully understand how a ____ actually protects a computer ____.

Maria: A firewall is a key tool in ____ _____. It creates a barrier between an ____ _____ and an ____ _____.

Alex: So it controls everything that enters and leaves the system?

Maria: Exactly. It can ____ or ____ network ____ based on predefined security _____. It also helps ____ suspicious activity and ____ potential cyber threats in real time.

Alex: What happens if the data is sensitive?

Maria: Then it can be ____ before transmission to ensure safety. Firewalls also help prevent ____ _____ from gaining access to protected resources.

Alex: So it's like a digital security guard?

Maria: Yes, it constantly ____ the system and decides what is safe or dangerous for the ____.

Task 10. Choose a topic from the given below prepare a presentation (5-7 slides).

1. Fundamentals of Network Security in Modern IT Systems
2. How Firewalls Work: Principles and Mechanisms
3. Types of Firewalls: Hardware vs Software Solutions
4. Packet Filtering and Traffic Inspection Techniques
5. Intrusion Detection and Intrusion Prevention Systems (IDS/IPS)
6. Common Cyber Threats and How Firewalls Defend Against Them
7. Role of Encryption in Secure Network Communication
8. Authentication and Access Control in Network Security
9. Virtual Private Networks (VPNs) and Secure Remote Access
10. Real-World Cyberattacks and Firewall Protection Strategies

Module 3. Cybersecurity Policies & Regulations

Lesson 1. Ethical Hacking & Penetration Testing

WORDBANK

Term	Translation
1. penetration testing	тестування на проникнення
2. cybersecurity posture	рівень кіберзахищеності
3. vulnerability remediation	усунення вразливостей
4. post-exploitation analysis	аналіз після експлуатації
5. regulatory compliance	відповідність нормативним вимогам
6. reconnaissance phase	етап розвідки
7. system resilience	стійкість системи
8. incident response capabilities	можливості реагування на інциденти
9.unauthorized access prevention	запобігання несанкціонованому доступу
10. secure software development	безпечна розробка програмного забезпечення
11. cyberattack mitigation	пом'якшення наслідків кібератак
12. vulnerability assessment	оцінка вразливостей

Task 1. Match the term with the correct definition.

Term	Definition
1. penetration testing	A) the process of gathering information about a target system before launching an attack.
2. cybersecurity posture	B) measures and controls implemented to stop intruders from gaining access to systems or data.
3. vulnerability remediation	C) the overall strength and effectiveness of an organization's security measures.
4. post-exploitation analysis	D) the process of fixing or eliminating identified security weaknesses.
5. regulatory compliance	E) the ability of a system to continue operating and recover quickly after a cyber incident or failure.
6. reconnaissance phase	F) a simulated cyberattack performed to evaluate the security of a system.
7. system resilience	G) activities conducted after gaining access to a system to understand impact and improve defenses.
8. incident response capabilities	H) adherence to laws, regulations, and standards related to cybersecurity.
9. unauthorized access prevention	I) actions and strategies used to identify, contain, and recover from security breaches or attacks.
10. secure software development	J) the practice of designing and coding applications in a way that minimizes security risks.

Task 2. Match the term with the correct Ukrainian Translation.

Term	Ukrainian Translation
1. ethical hacking	A) оцінка вразливостей
2. penetration testing	B) реагування на інциденти
3. vulnerability assessment	C) кібербезпекова позиція
4. system resilience	D) етичний хакінг
5. reconnaissance	E) проникне тестування
6. exploitation phase	F) стійкість системи
7. cybersecurity posture	G) розвідка (збір інформації)
8. incident response	H) фаза експлуатації
9. unauthorized access	I) несанкціонований доступ
10. secure software development	J) безпечна розробка програмного забезпечення

Task 3. Reading.**Ethical Hacking & Penetration Testing**

Ethical hacking and penetration testing are essential practices in modern cybersecurity aimed at identifying and mitigating vulnerabilities in information systems. They are conducted by certified security professionals who simulate malicious attacks in a controlled and authorized environment to evaluate system resilience. Penetration testers use a variety of tools and methodologies to discover weaknesses such as misconfigurations, outdated software, and insecure network protocols. The process typically includes reconnaissance, scanning, exploitation, and post-exploitation phases to assess the overall security posture of an organization. Results are documented in detailed reports that provide risk ratings, evidence of vulnerabilities, and recommendations for remediation.

Ethical hacking supports proactive defense strategies, helping organizations strengthen their cybersecurity posture and comply with regulatory

standards. It plays a crucial role in protecting sensitive data, preventing unauthorized access, and reducing the risk of cyberattacks in critical infrastructure. Penetration testing can be performed as black box, white box, or grey box testing depending on the level of prior knowledge available to the tester.

Organizations increasingly integrate ethical hacking into their cybersecurity lifecycle to continuously monitor risks, improve incident response capabilities, and ensure long-term resilience against evolving threats. Proper authorization and adherence to legal frameworks are fundamental principles of ethical hacking, ensuring that all testing activities remain compliant and do not harm real systems. Pen testers also collaborate with development and security teams to fix vulnerabilities and enhance secure software development practices.

Continuous learning and up-to-date knowledge of attack techniques are necessary for professionals working in ethical hacking domains and cybersecurity industry standards. These skills ensure accurate assessment, responsible disclosure, and stronger protection of digital infrastructures worldwide in modern environments today.

Answer the questions according to the text.

1. What is the purpose of ethical hacking and penetration testing?
2. Who conducts penetration testing and under what conditions?
3. What types of vulnerabilities can be identified during penetration testing?
4. What are the main stages of the penetration testing process?
5. What kind of information is included in penetration testing reports?
6. How does ethical hacking help organizations improve cybersecurity?
7. Why are continuous learning and up-to-date knowledge important for cybersecurity professionals?

Task 4. Decide whether each statement is True (T) or False (F).

1. Ethical hacking is used to perform real cyberattacks without permission.
2. Penetration testing helps identify weaknesses in systems.
3. Reconnaissance is the final phase of penetration testing.
4. Ethical hacking contributes to preventing unauthorized access.
5. Reports from penetration testing include recommendations for fixing vulnerabilities.
6. Ethical hacking is not related to regulatory compliance.
7. Penetration testing can be conducted in different formats such as black box and white box testing.
8. Cybersecurity posture refers to physical security of buildings only.
9. Continuous monitoring and learning are important in cybersecurity.
10. Ethical hacking may harm real systems during testing.

Grammar Focus: Tenses**Task 5. Complete the table with the correct forms (Noun – Verb – Adjective – Adverb).**

	Noun	Verb	Adjective	Adverb
1	_____	secure	_____	securely
2	protection	_____	protective	_____
3	_____	assess	_____	_____
4	_____	_____	authorized	_____
5	_____	comply	compliant	_____
6	prevention	_____	_____	preventively
7	development	_____	_____	_____
8	_____	_____	vulnerable	_____
9	_____	resile	resilient	_____
10	analysis	_____	analytical	_____

Note for students:

* Some verb forms (e.g., *vulnerate*, *resile*) are rare in modern usage; more common expressions are:

- “be vulnerable” , “show resilience”

Task 6. Order the words to make sentences.

(Use Present Simple, Present Continuous, Present Perfect, Past Simple, Past Continuous, Past Perfect, Future Simple, and be going to forms)

1. ethical / cybersecurity / is / a / essential / discipline / in / modern
2. researchers / are / currently / conducting / penetration / testing / in / controlled / environments
3. ethical / hacking / has / significantly / improved / organizational / cybersecurity / posture
4. did / last / year / penetration / testing / not / detect / all / system / vulnerabilities
5. security / incidents / were / sometimes / being / simulated / in / academic / environments
6. organizations / have / recently / strengthened / their / incident / response / capabilities
7. ethical / hacking / will / play / an / important / role / in / future / cybersecurity / strategies
8. cybersecurity / teams / are / going / to / implement / advanced / monitoring / tools / soon
9. the / penetration / testing / process / typically / includes / reconnaissance / and / exploitation / phases
10. professionals / were / analyzing / system / logs / while / attacks / were / occurring
11. the / researchers / had / already / completed / vulnerability / assessment / before / the / audit

12. professionals / are / going / to / continuously / develop / their / cybersecurity / competencies

Task 7. Read the text and fill it with the correct prepositions:

in (4), on, at, for (2), to (2), of, with, from, about

Ethical hacking plays a crucial role ___ modern cybersecurity practices. It is used to identify vulnerabilities ___ information systems and to strengthen protection ___ cyberattacks. Penetration testers work ___ controlled environments and simulate real-world attacks ___ order to evaluate system security.

The process usually begins ___ reconnaissance, when professionals collect information ___ the target system. After that, they move ___ scanning and exploitation phases. All findings are recorded ___ detailed reports, which include evidence ___ vulnerabilities and recommendations ___ improvement.

Organizations rely ___ ethical hacking to improve their cybersecurity posture and comply ___ international security standards. Continuous monitoring and analysis are essential ___ maintaining system resilience and preventing unauthorized access ___ critical data.

Task 8. Replace the underlined phrases with suitable synonyms.

ethical hacking, penetration testing, cybersecurity posture, vulnerability assessment, reconnaissance phase, incident response capabilities, unauthorized access prevention, secure software development, system resilience, cyberattack mitigation

1. Ethical hackers help improve **the overall strength of an organization's security measures**.
2. Penetration testers perform **a simulated cyberattack to evaluate system security**.
3. The team conducted a detailed **analysis of system weaknesses** before the audit.

4. Professionals begin their work with the **information-gathering stage before an attack.**
5. Organizations aim to enhance **their ability to react to and recover from security incidents.**
6. Security teams focus on **stopping intruders from entering systems or data.**
7. Developers follow principles of **building applications with minimal security risks.**

Task 9. Writing. Watch two videos and write short summaries.

<https://www.youtube.com/watch?v=YXO6he3vbMI>

<https://www.youtube.com/watch?v=kyxanedlP0>

Speaking

Useful language for speaking tasks

1. Introducing ideas

- In our opinion, the main issue is...
- The situation shows that...
- From a cybersecurity perspective, it is clear that...
- One possible explanation is that...
- We should first consider...

2. Suggesting actions (Problem-Solving)

- The first step should be to...
- It is necessary to immediately...
- We recommend conducting...
- A possible solution would be to...
- The system should be checked for...
- It might be useful to implement...

3. Giving opinions (Debate)

- I strongly believe that...
- I partly agree, but...
- I disagree because...
- In my view, ethical hacking...
- There is a risk that...
- However, it is also true that...

4. Agreeing / Disagreeing

- I completely agree with that point.
- That's a valid argument.
- I see your point, but...
- I'm not convinced that...
- I have a different opinion.
- That may be true, however...

5. Justifying ideas

- This is important because...
- The main reason is that...
- It helps organizations to...
- This reduces the risk of...
- This improves system security by...

Concluding ideas

- To conclude, we believe that...
- Overall, the most effective solution is...
- In summary, cybersecurity should focus on...
- Finally, we recommend that...

Task 10. Problem-Solving Scenario.

“Cybersecurity Incident”

Task:

Your university has detected unusual activity in its network. Work in groups and decide:

- What steps should be taken immediately?
- Should penetration testing be used? Why?
- Who should be responsible for the investigation?
- How can similar incidents be prevented in the future?

Output:

Present your group solution in 1–2 minutes.

Task 11. Debate “*Ethical Hacking: Good or Risky Practice?*”

Team A: Ethical hacking is essential and fully beneficial.

Team B: Ethical hacking can create risks and should be limited.

Structure:

- Introduction of argument
- 2–3 supporting points
- Rebuttal
- Conclusion

Task 12. Role Play “*Penetration Tester vs. Company Manager*”.

Roles:

- Penetration tester
- IT manager / company director

Situation:

The tester presents security vulnerabilities found during testing.

Tasks:

- Explain vulnerabilities clearly
- Suggest improvements
- Discuss budget and urgency
- Agree on next steps

Lesson 2. Cybersecurity in Business**WORDBANK**

	Term	Translation
1	cyber threat intelligence	розвідка кіберзагроз
2	information security management	управління інформаційною безпекою
3	encryption key management	управління ключами шифрування
4	vulnerability assessment	оцінка вразливостей
5	incident response plan	план реагування на інциденти
6	zero-day vulnerability	вразливість нульового дня
7	malware analysis	аналіз шкідливого програмного забезпечення
8	threat mitigation strategy	стратегія зниження кіберзагроз
9	network segmentation	сегментація мережі
10	secure software development lifecycle (SDLC)	життєвий цикл безпечної розробки програмного забезпечення

Task 1. Match the term with the correct definition.

Term	Definition
1. cyber threat intelligence	A) a strategy designed to reduce the impact or likelihood of cyberattacks.
2. information security management	B) the process of collecting and analyzing information about current or potential cyber threats.
3. encryption key management	C) the practice of detecting, analyzing, and understanding malicious software behavior.
4. vulnerability assessment	D) a structured approach to identifying, responding to, and recovering from cybersecurity incidents.
5. incident response plan	E) a security weakness that is unknown to the vendor and has no available patch.
6. zero-day vulnerability	F) the process of managing cryptographic keys to ensure secure data encryption and access control.
7. malware analysis	G) the process of dividing a computer network into smaller isolated parts to improve security.
8. threat mitigation strategy	H) a systematic evaluation of systems to identify security weaknesses and risks.
9. network segmentation	I) a framework for developing software with integrated security practices at every stage.
10. secure software development lifecycle (SDLC)	J) the overall coordination and management of policies and procedures to protect information

Term	Definition
	systems.

Task 2. Fill the gaps using words from the box.

cyber threat intelligence, secure software development lifecycle (SDLC), information security management, encryption key management, vulnerability assessment, incident response plan, zero-day vulnerability, malware analysis, threat mitigation strategy, network segmentation,

1. A serious risk in cybersecurity is a _____, which refers to an unknown software flaw that attackers can exploit before it is fixed.
2. Companies also rely on _____ to ensure that all policies and procedures are properly applied to protect digital assets and sensitive information.
3. To reduce the impact of cyberattacks, companies develop a _____ that helps minimize damage and control threats.
4. Security teams also perform _____ to study how malicious software behaves and spreads within systems.
5. Cybersecurity in modern organizations requires _____, which helps organizations understand emerging attacks and identify potential risks in advance.
6. Before launching systems into production, organizations perform _____ to detect weaknesses and reduce possible security risks.
7. Large networks are often protected using _____, which divides systems into smaller isolated segments to improve security.
8. In case of a cyber incident, a well-developed _____ is necessary to ensure fast and effective reaction to attacks.
9. To protect encrypted data, specialists use _____, which ensures that cryptographic keys are securely created, stored, and managed.

10. Finally, modern companies apply the _____ to integrate security into every stage of software development.

Task 3. Reading.

Cybersecurity in Business

Cybersecurity has become a critical component of modern business operations due to the rapid growth of digital technologies and the increasing number of cyber threats. Organizations of all sizes rely on information systems to store, process, and transmit sensitive data, including financial records, personal information, and intellectual property. As a result, protecting these systems is essential for maintaining trust, ensuring business continuity, and avoiding financial losses.

One of the key elements of cybersecurity in business is risk management. Companies must identify potential vulnerabilities in their systems and apply appropriate security measures to reduce the likelihood of cyberattacks. Common practices include ethical hacking and penetration testing, which help simulate real-world attacks in a controlled environment. These methods allow security professionals to detect weaknesses before they can be exploited by malicious actors.

Large technology companies are good examples of how cybersecurity is applied in practice. For instance, **Google** uses artificial intelligence to detect cyber threats in real time and works with ethical hackers through bug bounty programs. **Microsoft** integrates cybersecurity into all its products and uses vulnerability assessments, secure software development practices, and incident response teams. **Amazon Web Services (AWS)** protects cloud systems through encryption, access control, and continuous monitoring, while also providing security tools for its customers. **Apple** focuses strongly on privacy and uses encryption and strict ecosystem control to prevent unauthorized access. **Meta (Facebook)** applies artificial intelligence to detect fake accounts and cyberattacks across its platforms.

In addition, businesses must ensure compliance with international security standards and regulations. This includes implementing policies for data protection, access control, and incident response. Strong cybersecurity posture also depends on employee awareness, as human error is often a major cause of security breaches. Modern organizations are increasingly investing in advanced technologies such as artificial intelligence, intrusion detection systems, and secure software development practices. These tools improve system resilience and support faster response to cyber incidents.

In conclusion, cybersecurity is no longer optional for businesses; it is a fundamental requirement in the digital age. Companies that invest in strong security strategies are better prepared to prevent cyberattacks, protect their data, and maintain long-term stability in a highly connected world.

Task 4. Decide whether each statement is True (T) or False (F).

1. Cyber threat intelligence helps organizations predict and understand possible cyberattacks.
2. Information security management focuses only on technical tools and ignores policies.
3. Encryption key management ensures secure handling of cryptographic keys.
4. Vulnerability assessment is used to identify weaknesses in systems before attackers do.
5. Incident response plan is unnecessary if a company has strong antivirus software.
6. A zero-day vulnerability is a known security flaw that already has a patch.
7. Malware analysis studies how malicious software behaves and spreads.
8. Threat mitigation strategy is used to increase the impact of cyberattacks.
9. Network segmentation improves security by dividing a network into isolated parts.

10. Secure software development lifecycle (SDLC) integrates security into every stage of software creation

Grammar Focus: Linking words

Present Perfect (for results & experience)

Task 5. Complete each sentence with the correct linking word.

however (2), in addition (2), consequently (1), therefore (3), as a result (2)

1. Cybersecurity threats are increasing rapidly; _____, organizations must strengthen their defenses.
2. Ethical hacking is widely used in companies; _____, it helps identify system vulnerabilities before attacks occur.
3. Penetration testing is effective; _____, it does not guarantee complete system security.
4. Many businesses invest in encryption technologies; _____, they improve the protection of sensitive data.
5. The system was not updated regularly; _____, it became vulnerable to cyberattacks.
6. Security teams detected unusual activity; _____, they immediately activated the incident response plan.
7. Cloud services are convenient; _____, they require strong access control mechanisms.
8. The company improved its cybersecurity posture; _____, the number of incidents decreased significantly.
9. Malware analysis is essential for security; _____, it helps understand how attacks spread.
10. Organizations use advanced monitoring tools; _____, they can respond faster to threats.

Task 6. Complete the sentences (Present Perfect: positive, negative, questions).

1. Companies _____ (improve) their cybersecurity systems in recent years.
2. Ethical hackers _____ not _____ (find) all system vulnerabilities yet.
3. _____ security teams _____ (respond) to recent cyberattacks?
4. Researchers _____ (discover) new malware analysis methods.
5. Organizations _____ not _____ (implement) strong encryption key management.
6. _____ IT specialists _____ (conduct) vulnerability assessments this year?
7. The company _____ (strengthen) its incident response plan recently.
8. Attackers _____ not _____ (exploit) all system weaknesses.
9. _____ cybersecurity experts _____ (develop) advanced tools for threat detection?
10. Companies _____ (gain) experience from previous cyberattacks.

Task 7. Translate the sentences into English using the Present Perfect Tense.

1. За останні роки великі технологічні компанії значно покращили свої системи кібербезпеки для захисту конфіденційних даних користувачів.
2. Етичні хакери вже виявили критичні вразливості в корпоративних інформаційних системах і повідомили про них організаціям.
3. Команда кібербезпеки вже відреагувала на кілька складних інцидентів, використовуючи сучасні інструменти аналізу загроз.

4. Дослідники розробили нові методи аналізу шкідливого програмного забезпечення, які дозволяють швидше визначати тип атак.
5. Багато організацій ще не впровадили ефективне управління ключами шифрування, що підвищує ризик витоку даних.
6. IT-спеціалісти провели численні оцінки вразливостей у складних мережових інфраструктурах великих компаній.
7. Компанія вже суттєво посилила свій план реагування на інциденти після кількох недавніх кібератак.
8. Зловмисники використали раніше невідомі вразливості нульового дня для атаки на критичні системи.
9. Експерти з кібербезпеки розробили інноваційні інструменти для виявлення та зниження кіберзагроз у реальному часі.
10. Компанії накопили значний практичний досвід у сфері захисту інформаційних систем після серії попередніх кіберінцидентів.

Task 8. Replace the underlined phrases with suitable synonyms.

cyber threat intelligence, information security management, encryption key management, vulnerability assessment, incident response plan, zero-day vulnerability, malware analysis, threat mitigation strategy, network segmentation, secure software development lifecycle (SDLC)

1. Organizations must regularly conduct a **systematic evaluation of weaknesses** in their IT systems to reduce cyber risks.
2. Security teams rely on a **structured plan** for reacting to and recovering from cyber incidents.
3. Experts use **methods for studying malicious software behavior and its spread in systems**.
4. Companies implement **strategies aimed at reducing the impact of cyberattacks**.

5. A **previously unknown software flaw without an available patch** can be extremely dangerous for critical infrastructure.
6. Large organizations apply **a process for managing cryptographic keys** used in encryption systems.
7. Modern companies follow a framework that **integrates security into every stage of software development**.
8. IT departments use **the process of dividing a network into isolated segments** for better protection.
9. Businesses depend on **the overall coordination of policies and procedures** to protect information systems.
10. Analysts study **information about current and potential cyber threats to predict attacks**.

Speaking Task: Continue the Ideas.

Task 9. Complete each sentence orally by adding 2–3 sentences with your own ideas, explanations, or examples.

1. Cybersecurity is essential for modern businesses because...
2. Ethical hacking helps organizations improve security by...
3. Penetration testing is important in business environments because...
4. One major cyber threat for companies today is...
5. Companies should invest in cybersecurity tools such as...
6. A strong cybersecurity posture is necessary because...
7. If a company does not protect its systems properly,...
8. Incident response plans are useful when...
9. Network segmentation improves security because...
10. In the future, cybersecurity will become even more important because...

Task 10. Watch the video and decide if the statements are True (T) or False (F).

Video: <https://www.youtube.com/watch?v=OyvpBydEVeQ>

1. Cybersecurity is important only for large international companies, not for small businesses.
2. One of the main risks for businesses is phishing attacks that try to steal sensitive information.
3. Strong passwords and regular updates are recommended as basic cybersecurity practices.
4. Multi-factor authentication makes accounts less secure and should be avoided.
5. Employee training plays an important role in preventing cyberattacks.
6. Cybersecurity threats can only come from outside the organization.
7. Regular data backups help companies recover after cyber incidents.

Lesson 3. Artificial Intelligence & Cybersecurity

WORDBANK

Term	Ukrainian Translation
1. threat detection mechanisms	механізми виявлення загроз
2. data exfiltration	несанкціоноване вилучення даних
3. anomalous behavioral patterns	аномальні поведінкові патерни
4. machine learning algorithms	алгоритми машинного навчання
5. predictive threat modeling	прогностичне моделювання загроз
6. system vulnerabilities	вразливості системи
7. deep neural networks	глибокі нейронні мережі
8. incident response framework	структура реагування на інциденти
9. algorithmic decision-making processes	процеси алгоритмічного прийняття рішень
10.intelligent automation systems	інтелектуальні автоматизовані системи

Task 1. Match words with definitions.

Term	Definition
1. anomaly	A) a weakness in a system that can be exploited by attackers
2. vulnerability	B) the process of converting data into a secure format
3. encryption	C) something that deviates from the normal or expected pattern
4. data exfiltration	D) the unauthorized transfer of data from a computer system
5. predictive analysis	E) a method of forecasting future events based on data analysis
6. neural network	F) a computing model inspired by the human brain used for pattern recognition
7. intrusion detection	G) a system designed to detect unauthorized access to networks
8. authentication	H) a process of verifying the identity of a user or system
9. algorithm	I) a step-by-step procedure used to solve a problem or perform a task
10. firewall	J) a security system that monitors and controls network traffic

Task 2. Complete the table with correct word forms.

	Noun	Verb	Adjective	Adverb
1.	optimization	_____	_____	optimally
2.	_____	encrypt	_____	_____
3.	_____	_____	_____	authentically
4.	_____	infiltrate	infiltrative	_____
5.	detection	_____	detectable	_____
6.	_____	_____	_____	resiliently
7.	governance	govern	_____	_____

Task 3. Reading.**Artificial Intelligence & Cybersecurity**

Artificial Intelligence (AI) is revolutionizing the domain of cybersecurity by introducing sophisticated mechanisms for threat detection and prevention. Contemporary organizations are increasingly exposed to a wide range of cyber threats, including malware infiltration, phishing schemes, and large-scale data breaches. Conventional security frameworks often fail to respond promptly to these evolving and highly complex attacks, which necessitates the integration of AI-driven solutions.

A key advantage of AI lies in its capacity to process vast datasets in real time and identify anomalous patterns of behavior. Advanced machine learning algorithms enable predictive threat analysis, allowing systems to mitigate risks before they escalate into critical incidents. For instance, AI-powered systems can detect irregular network traffic, unauthorized access attempts, and potential system vulnerabilities.

Leading technology corporations such as Google, Microsoft, IBM, and OpenAI are at the forefront of developing cutting-edge AI technologies for cybersecurity. These organizations invest substantial resources in enhancing automated threat detection, strengthening data encryption protocols, and optimizing incident response strategies.

Looking toward the next decade, AI is expected to become increasingly autonomous, adaptive, and precise. Nevertheless, the growing reliance on AI introduces new challenges, as cybercriminals also exploit these technologies to orchestrate more sophisticated and targeted attacks. Consequently, the future of cybersecurity will depend on the synergy between advanced technological solutions and human expertise to ensure resilient and robust protection systems.

Multiple Choice (choose the correct answer).

1. What is the primary function of AI in cybersecurity?
 - a) Threat detection and prevention
 - b) Data storage
 - c) Website design
2. What does “anomalous patterns” refer to?
 - a) Normal activity
 - b) Planned actions
 - c) Unusual behavior
3. What do machine learning algorithms enable?
 - a) Manual control
 - b) Predictive threat analysis
 - c) Data deletion
4. What is “malware infiltration”?
 - a) Data protection
 - b) Unauthorized harmful software entering a system
 - c) Safe internet usage

5. What do leading companies invest in?
 - a) Entertainment technologies
 - b) Social media platforms
 - c) Automated threat detection and encryption
6. What is expected from AI in the future?
 - a) Greater autonomy and precision
 - b) Decreased efficiency
 - c) Limited usage
7. What is a major cybersecurity challenge mentioned?
 - a) Lack of internet access
 - b) Low data volume
 - c) Use of AI by cybercriminals

Task 5. Use words from the text to fill the gaps.

mitigate, schemes, vulnerabilities, cutting-edge, synergy, anomalies, en

ryption, algorithms, frameworks, automation

1. AI systems can _____ potential risks before they escalate into serious incidents.
2. Cybercriminals often use phishing _____ to deceive users.
3. AI helps identify system _____ before they are exploited.
4. Leading companies develop _____ AI technologies to improve security.
5. Effective cybersecurity depends on the _____ between humans and AI.
6. Machine learning tools can _____ the impact of cyberattacks.
7. Many employees are trained to recognize fraudulent _____.
8. Weak passwords create serious _____ in digital systems.
9. _____ innovations play a key role in modern cybersecurity strategies.
10. The _____ of human expertise and automation improves decision-making.

Task 6. Replace the underlined phrases with suitable synonyms.

synergy, vulnerabilities, cutting-edge, anomalous behavioral patterns, mitigate, automated threat detection, vast datasets, potential security threat

1. AI systems can **reduce cyber risks** before they escalate into serious incidents.
2. Cybersecurity experts analyze **very large amounts of data** in real time.
3. Machine learning algorithms can detect **unusual behavior patterns** in network traffic.
4. Companies invest in **modern and highly advanced technologies** to strengthen digital protection.
5. Hackers often exploit **weak points in computer systems** to gain unauthorized access.
6. AI enables organizations to perform **automatic threat detection and response**.
7. The system identified **a possible security problem** in the database.
8. Cybersecurity requires **cooperation between humans and artificial intelligence systems**.

Grammar Focus: Infinitive&Gerund

Task 7. Choose the correct option in brackets.

1. AI systems help prevent (to detect / detecting) cyber threats in real time.
2. Cybersecurity experts are responsible for (to analyze / analyzing) suspicious network activity.
3. Companies aim (to improve / improving) their data protection strategies.
4. Hackers try (to exploit / exploiting) system vulnerabilities.
5. Machine learning enables computers (to recognize / recognizing) unusual behavior patterns.
6. Organizations avoid (to expose / exposing) sensitive data to external risks.
7. Researchers continue (to develop / developing) advanced encryption methods.

8. The system began (to process / processing) large volumes of data automatically.
9. Governments consider (to introduce / introducing) stricter cybersecurity regulations.
10. AI assists in (to identify / identifying) potential security breaches.

Task 8. Complete with Gerund or Infinitive.

1. Cybersecurity specialists need _____ (monitor) network traffic continuously.
2. AI tools are designed _____ (detect) malicious software.
3. Companies risk _____ (lose) sensitive information without proper protection.
4. The system is capable of _____ (analyze) complex datasets.
5. Experts recommend _____ (update) security software regularly.
6. Hackers attempt _____ (gain) unauthorized access to systems.
7. Organizations should avoid _____ (ignore) security alerts.
8. Machine learning helps _____ (improve) threat detection accuracy.
9. Students are learning _____ (use) AI in cybersecurity applications.
10. The software started _____ (block) suspicious connections automatically.

Task 9. Find and correct the mistakes in the sentences (one sentence is correct).

1. Artificial intelligence helps to detecting cyber threats in complex and constantly changing digital environments.
2. Cybersecurity specialists avoid to ignore automated system alerts generated by AI-based monitoring tools.
3. The company decided improving its encryption infrastructure in order to strengthen data protection across all departments.
4. Hackers attempted accessing highly secure databases containing sensitive financial and personal information.

5. The system began to analyzing large volumes of user behavior data immediately after the software update.
6. Researchers continue to develop advanced artificial intelligence models capable of predicting cyberattacks.
7. Employees are responsible for to protect confidential information stored within organizational networks.
8. AI enables modern security systems recognizing unusual activity patterns in real time.
9. Governments plan introducing stricter cybersecurity regulations to reduce the risk of large-scale cyber incidents.
10. It is important to securing digital infrastructure effectively in order to prevent unauthorized access and data breaches.

Speaking

Task 10: Problem-Solving Situation.

Discuss and decide on the best solution.

Situation:

A large company has experienced a cyberattack that exposed sensitive customer data. The system is still vulnerable, and operations are partially disrupted.

Tasks:

- Identify possible causes of the attack
- Suggest immediate actions to stop further damage
- Propose long-term cybersecurity improvements
- Decide whether AI-based systems should be introduced or improved
- Explain your final recommendation

Task 11. Choose a topic from the given below prepare the final presentation (5-7 slides).

Module 1. Introduction to IT and Cybersecurity

1. Fundamentals of Computer Systems and Their Components
2. How Computer Networks Work: Structure and Communication Models
3. Types of Networks: LAN, WAN, and the Internet
4. Operating Systems: Functions, Types, and Security Features
5. Software Categories: System Software vs Application Software
6. Cloud Computing Models: IaaS, PaaS, SaaS
7. Security Challenges in Cloud Computing Environments

Module 2. Cybersecurity and Modern Threats

1. Overview of Modern Cyber Threats and Attack Vectors
2. Malware Types: Viruses, Worms, Trojans, and Ransomware
3. Social Engineering and Phishing Attacks in Cybersecurity
4. Principles of Internet Security and Safe Online Behavior
5. Encryption Methods and Data Protection Techniques
6. Network Security Fundamentals and Defense Strategies
7. Firewalls: Types, Functions, and Real-World Applications

Module 3. Cybersecurity Policies & Regulations

1. Ethical Hacking: Purpose, Methods, and Legal Boundaries
2. Penetration Testing in Modern Cybersecurity Practice
3. Cybersecurity Policies in Organizations: Structure and Importance
4. Data Protection Regulations (GDPR and Global Standards)
5. Cybersecurity in Business: Risk Management and Strategy
6. Artificial Intelligence in Cybersecurity: Opportunities and Threats

ANSWER KEYS

Module 1. Introduction to IT and Cybersecurity

Lesson 1. Computer Systems & Networks

Task 1.

1–J, 2–F, 3–C, 4–H, 5–E, 6–D, 7–G, 8–B, 9–I, 10–A

Task 2.

1–E, 2–J, 3–D, 4–I, 5–A, 6–G, 7–H, 8–F, 9–C, 10–B

Task 3.

1. architecture hardware, 2. infrastructure network, 3. model-server client, 4. protocol communication, 5. capacity bandwidth, 6. switching packet, 7. latency network, 8. mechanism routing, scalability, 9. connectivity secure

Task 5. True / False

1-T, 2-F, 3-T, 4-T, 5-F, 6-T, 7-T, 8-F, 9-T, 10-F

Task 6.

	Verb	Noun	Adjective	Adverb
1.	protect	protection	protective	protectively
2.	secure	security	secure	securely
3.	monitor	monitoring	monitored	continuously
4.	select	selection	selective	selectively
5.	optimize	optimization	optimal	optimally
6.	enhance	enhancement	enhanced	
7.	interact	interaction	interactive	interactively
8.	allocate	allocation	allocated	dynamically
9.	transmit	transmission	transmissible	
10.	process	processing	processed	

	Verb	Noun	Adjective	Adverb
11.	analyze	analysis	analytical	analytically
12.	evaluate	evaluation	evaluative	evaluatively
13.	detect	detection	detectable	detectably
14.	resilient	resilience	resilient	resiliently
15.	reliable	reliability	reliable	reliably

Task 7. Passive Voice (*Other grammatically correct passive forms are acceptable.*)

1. Network infrastructures **are designed** to ensure reliability.
2. Data transmission **is regulated** by protocols.
3. Optimal transmission paths **are selected** by routers.
4. Network traffic **is monitored** continuously by administrators.
5. System resources **are allocated** dynamically.
6. Transmitted data **is protected** by security mechanisms.
7. Client requests **are processed** by servers.
8. Network performance **is affected** by topology.
9. Fault tolerance mechanisms **are implemented** by engineers.
10. Cloud services **are supported** by networks.

Task 8. (possible answers)

1) computer framework, 2) computing resources, 3) network framework, 4) data transfer, 5) client-server architecture, 6) networking rules, 7) data segmentation, 8) network delay, 9) path selection methods, 10) protected connection, 11) system stability

Task 9.

1. are routed (Passive)
2. monitor (Active)
3. are established (Passive)

4. access (Active)
5. increases (Active)
6. configure (Active)
7. is achieved (Passive)
8. update (Active)
9. are optimized (Passive)
10. reduce (Active)

Task 11.

1. **True**
2. **False** – The speakers explain that people are often influenced by emotions, habits, or biases, not just rational thinking.
3. **True**
4. **True**
5. **False** – Social influence is presented as a strong factor affecting people's choices.
6. **True**
7. **False** – The videos suggest that people are not always fully aware of their actions or decisions.
8. **True**
9. **False** – The speakers argue that behaviour **can** be changed, even if it is difficult.
10. **True**

Lesson 2. Operating Systems and Software

Task 1.

1-b, 2-d, 3-g, 4-e, 5-a, 6-j, 7-c, 8-h, 9-i, 10-f

Task 2.

1-F, 2-D, 3-J, 4-E, 5-I, 6-C, 7-H, 8-G, 9-B, 10-A

Task 3.

- 1 – **D** (operating system – операційна система)
- 2 – **A** (kernel – ядро)
- 3 – **J** (resource allocation – розподіл ресурсів)
- 4 – **B** (multitasking – багатозадачність)
- 5 – **E** (process scheduling – планування процесів)
- 6 – **C** (access control – контроль доступу)
- 7 – **I** (system vulnerability – системна вразливість)
- 8 – **G** (software patch – програмне оновлення)
- 9 – **H** (open-source software – ПЗ з відкритим кодом)
- 10 – **F** (privilege escalation – підвищення привілеїв)

Task 5.

- 1.T, 2. F, 3.T, 4.T, 5.T, 6.F, 7.T, 8.F, 9.T, 10. T.

Task 6.

- 1. System resources **are allocated** to active applications by the operating system.
- 2. A critical security patch **was released** last week by developers.
- 3. Access control settings **are being configured** now by administrators.
- 4. System calls **have been managed** efficiently for many years by the kernel.
- 5. Processes **will be scheduled** automatically by the system.
- 6. Software vulnerabilities **can be exploited** remotely by attackers.
- 7. System stability **is being improved** at the moment by engineers.
- 8. Strict security policies **must be enforced** by the operating system.
- 9. The latest software updates **have been installed** by users.
- 10. System performance **was being monitored** during the failure by administrators.

Task 7.

controls–manages; handles–processes; allows–enables; fix–remediate; shows–displays; use–exploit; keeps–maintains; improve–enhance; stop–prevent; build–develop

Task 8 (Mixed Tenses)

1. allocates (Present Simple)
2. identified / were performing (Past Simple / Past Continuous)
3. have managed / implemented (Present Perfect)
4. maintained (Past Simple)
5. prevent / have been reviewing (Present Simple / Present Perfect Continuous)
6. release / will have deployed (Present Simple / Future Perfect)
7. executes / processed (Present Simple / Past Simple)
8. schedules / has recorded (Present Simple / Present Perfect)
9. monitor / flagged (Present Simple / Past Simple)
10. have enhanced / will have introduced (Present Perfect / Future Perfect)

Task 9.

1. **True**
2. **False** – Utility programs perform maintenance and optimization tasks, not entertainment.
3. **True**
4. **True**
5. **False** – The OS directly interacts with hardware through drivers and system processes.
6. **True** – These tools are standard examples of utility software.
7. **True**
8. **False** – CPU management is a function of the operating system, not utility programs.

9. **True**
10. **True**

Lesson 3. Cloud Computing & Security

Task 1. 1–F, 2–G, 3–H, 4–D, 5–B, 6–J, 7–A, 8–C, 9–I, 10–E

Task 2. 1–G, 2–H, 3–I, 4–A, 5–B, 6–D, 7–F, 8–E, 9–C, 10–J

Task 3.

- 1–cloud computing
- 2–virtualized environment
- 3–cloud service provider
- 4–shared responsibility model
- 5–data encryption
- 6–access management
- 7–data breach
- 8–redundancy
- 9–availability
- 10–risk mitigation

Task 4.

1. T, 2. F, 3. T, 4. F, 5. T, 6. T, 7. F, 8. T, 9. F.

Task 5.

1. migrated (Past Simple)
2. have been monitoring (Present Perfect Continuous – continuous fits here)
3. applied (Past Simple)
4. have delivered (Present Perfect)
5. have exploited (Present Perfect)
6. implemented (Past Simple)
7. was encrypted (Past Simple – passive)
8. detected (Past Simple)

9. has become (Present Perfect)
10. have updated (Present Perfect)

Task 6.

1. offers, 2. secured, 3. regulates, 4. guarantees, 5. happens, 6. enable, 7. minimizes, 8. offer, 9. indicates, 10. specifies

Task 7.

1. neglect / will risk (First Conditional)
2. find / will exploit (First Conditional)
3. will fail / does not maintain (First Conditional)
4. is encrypted / will not access (First Conditional)
5. monitor / will be detected (First Conditional)
6. migrated / would save (Second Conditional)
7. follow / will be less successful (First Conditional)
8. will improve / increase (First Conditional)
9. grants / will become (First Conditional)
10. implemented / would avoid (Second Conditional)

Task 9.

1. **True**
2. **False** – Users do **not** need to own the physical servers; cloud providers manage the infrastructure.
3. **True**
4. **True**
5. **False** – The cloud works regardless of local installations; users access cloud services via internet connections.
6. **True**
7. **True**

8. **False** – One key benefit of cloud computing is *elasticity* and flexibility to scale resources up or down.
9. **True**
10. **False** – Cloud computing **does** support access to applications and data from multiple devices through the internet.

Module 2. Cybersecurity and Modern Threats

Lesson 1. Cyber Threats & Attacks

Task 1.

1-f, 2-c, 3-d, 4-e, 5-h, 6-a, 7-j, 8-i, 9-g, 10-b

Task 2. 1 – i, 2 – n, 3 – p, 4 – f, 5 – m, 6 – e, 7 – l, 8 – s, 9 – j, 10 – k, 11 – r, 12 – q, 13 – c, 14 – g, 15 – o, 16 – d, 17 – a, 18 – h, 19 – b, 20 – a

Task 3.

- 1 – exponential growth
- 2 – exploit software vulnerabilities
- 3 – multi-layered defense strategy
- 4 – removes malicious programs
- 5 – human psychology exploitation
- 6 – disrupt services
- 7 – demand financial ransom
- 8 – potential vulnerabilities
- 9 – critical digital assets
- 10 – intrusion detection systems

Task 5 – True/False

1. F – Cybersecurity is critical for individuals, businesses, and governments.
2. T – Text explicitly lists these as types of malware.

3. F – Phishing targets human behavior.
4. T – Ransomware encrypts files and demands ransom.
5. T – Social engineering exploits psychology.
6. T – Firewalls filter network traffic.
7. F – Human training is essential.
8. T – AI can detect suspicious patterns.
9. F – Cybercriminals may use AI adaptively.
10. T – Cloud requires strong security measures.

Task 6.

1–b, 2–b, 3–b, 4–a, 5–b, 6–c, 7–b, 8–b, 9–b, 10–a

Task 7.

1. Social engineering, 2. Encryption, 3. Phishing, 4. Ransomware, 5. Cybercriminals, 6. AI, 7. Cloud, 8. Firewall, 9. Malware, 10. Vulnerability

Task 8.

1. devising, 2. vigilance, 3. predict, 4. filter, 5. encrypts, 6. exploits, 7. multi-layered, 8. weaknesses, 9. recognize, 10. efficiency

Task 9.

1. **True**
2. **False** – Cybersecurity is important for everyone, including individuals, businesses, and governments.
3. **True**
4. **True**
5. **True** – Ransomware encrypts data and demands payment for decryption.
6. **True**
7. **True**
8. **False** – Cybersecurity also involves educating users and establishing safe practices, not just technical tools.
9. **True**
10. **True**

Lesson 2. Internet Security & Encryption

Task 1.

1–D, 2–C, 3–F, 4–E, 5–J, 6–G, 7–H, 8–I, 9–B, 10–A

Task 2.

1–C, 2–A, 3–D, 4–E, 5–F, 6–B, 7–G, 8–H, 9–I, 10–J, 11–K, 12–L, 13–M

Task 3.

Keys: 1–confidentiality, 2–encryption, 3–firewall, 4–antivirus software, 5–multi-factor authentication, 6–phishing, 7–ransomware, 8–denial-of-service attacks, 9–cloud platforms, 10–security policy

Task 4.

1. **False** – Internet security protects not only computers but also data, devices, and networks.
2. **True**
3. **False** – Encryption converts readable data into a coded format, not the other way around.
4. **True**
5. **True**
6. **False** – Firewalls and antivirus software are essential components of internet security.
7. **True**
8. **False** – Multi-factor authentication requires more than one method to verify identity.
9. **True**
10. **True**

Task 5. Grammar

1–should, 2–might, 3–must not / can't, 4–must, 5–can, 6–could, 7–must, 8–can, 9–can, 10–can

Task 6.

1. Users should update their antivirus software regularly to protect their devices.
2. Data must be encrypted before being transmitted over the Internet.
3. Emails from unknown sources might be phishing attempts.
4. A firewall can protect the network from unauthorized access.
5. Employees must follow the company's security policy.
6. Hackers could gain access to data if the system is not properly secured.
7. Multi-factor authentication can make accounts safer.
8. Cloud platforms can store data safely if proper security measures are applied.
9. Ransomware can cause serious damage to a user's files.
10. If users are not careful, they might become victims of a cyberattack.

Task 7.

1. Encryption, **which is used in VPNs**, protects data.
2. The hacker **who stole personal information** was arrested last week.
3. Firewalls **that are installed on all company servers** block malicious traffic.
4. Antivirus software, **which is installed on all computers**, detects malware.
5. Multi-factor authentication, **which requires multiple verification methods**, improves security.
6. Ransomware, **which encrypted files**, caused serious damage to the company.
7. Cloud platforms, **which are managed by trusted providers**, store sensitive data.
8. Cybersecurity policies, **which are followed by all employees**, protect organizations.
9. Data, **which must be encrypted to remain secure**, is transmitted online.

10. Phishing emails, **which try to steal passwords and personal information**, target users.

Task 8.

- 1 – data, devices, and networks → **digital assets**
- 2 – protection → **security / safeguarding**
- 3 – coded format → **encrypted format**
- 4 – interpret → **decrypt / access**
- 5 – implemented → **applied / deployed**
- 6 – cyberattacks → **cyber threats**
- 7 – sustaining → **maintaining / ensuring**
- 8 – safeguard → **protect / secure**
- 9 – cybersecurity posture → **online security framework**
- 10 – trustworthy online presence → **secure digital footprint**

Task 9.

digital assets, online security framework, encrypted format, decrypt, access, safeguarding, applied, deployed, protect, cyber threats, maintaining, ensuring, security, secure digital footprint, secure.

Lesson 3. Network Security & Firewalls

Task 1. 1–C, 2–B, 3–H, 4–I, 5–E, 6–F, 7–G, 8–J, 9–D, 10–A

Task 2. 1–B, 2–D, 3–J, 4–A, 5–F, 6–G, 7–E, 8–I, 9–H, 10–C

Task 3. Possible answers

1. The main purpose of network security is to protect computer systems, networks, and sensitive data from unauthorized access and cyber threats.

2. A firewall protects a network by monitoring and controlling incoming and outgoing traffic based on security rules and blocking suspicious data.
3. Inbound traffic is data coming into a network, while outbound traffic is data leaving the network to external destinations.
4. Packet filtering works by inspecting data packets and allowing or blocking them based on predefined security rules.
5. An Intrusion Prevention System (IPS) detects suspicious activity in real time and automatically blocks or prevents potential attacks.
6. Authentication is important because it verifies the identity of users before granting access to sensitive systems and resources.
7. VPNs and encrypted communication improve data protection by securing transmitted data and preventing interception by unauthorized users.

Task 4.

- 1 – True.
- 2 – False (Firewalls control both inbound and outbound traffic, not only incoming traffic.)
- 3 – True.
- 4 – False (Packet filtering is used to inspect and filter data packets, not to create malware.)
- 5 – True.
- 6 – True.
- 7 – True.
- 8 – False (Authentication processes verify identity and restrict access to authorized users only.)

Task 5. 1–for, 2–from, 3–on, 4–between, 5–by, 6–for, 7–into, 8–of, 9–in, 10–on, 11–to, 12–via, 13–over, 14–for, 15–to, 16–for, 17–on, 18–to.

Task 6.

1. have already been protected
2. is being monitored
3. is always encrypted
4. are regularly updated
5. is immediately detected
6. were actively being configured
7. was thoroughly being investigated
8. must be protected
9. will be automatically blocked
10. had already been analyzed

Task 7.

- 1 – network security
- 2 – firewall protection
- 3 – monitor
- 4 – detect
- 5 – encrypt
- 6 – block
- 7 – data breach
- 8 – authentication process
- 9 – traffic inspection
- 10 – unauthorized access

Task 8.

- 1 – True
- 2 – False (Firewalls do not allow all incoming traffic; they filter it.)
- 3 – True
- 4 – True
- 5 – False (Their purpose is security, not increasing internet speed.)

6 – True

7 – False (Firewalls can control both inbound and outbound traffic.)

8 – True

9 – False (Firewalls are widely used in both organizations and personal devices.)

10 – True

Task 9. 1–firewall, 2–network, 3–network security, 4–internal network, 5–external network, 6–block, 7–allow, 8–traffic, 9–rules, 10–detect, 11–monitor, 12–encrypt, 13–unauthorized access, 14–monitor, 15–system.

Module 3. Cybersecurity Policies & Regulations

Lesson 1. Ethical Hacking & Penetration Testing

Task 1.

1–F, 2–C, 3–D, 4–G, 5–H, 6–A, 7–E, 8–I, 9–B, 10–J.

Task 2.

1–D, 2–E, 3–A, 4–F, 5–G, 6–H, 7–C, 8–B, 9–I, 10–J.

Task 4.

1. **False** – Ethical hacking is conducted legally and with permission in a controlled environment.

2. **True**

3. **False** – Reconnaissance is the initial phase, not the final one.

4. **True**

5. **True**

6. **False** – Ethical hacking supports regulatory compliance.

7. **True**

8. **False** – Cybersecurity posture refers to overall security, not physical security only.

9. **True**

10. **False** – Ethical hacking is designed not to harm real systems.

Task 5.

Nº	Noun	Verb	Adjective	Adverb
1	security	secure	secure	securely
2	protection	protect	protective	protectively
3	assessment	assess	assessable	assessably
4	authorization	authorize	authorized	authorizably
5	compliance	comply	compliant	compliantly
6	prevention	prevent	preventive	preventively
7	development	develop	developmental	developmentally
8	vulnerability	vulnerate*	vulnerable	vulnerably
9	resilience	resile*	resilient	resiliently
10	analysis	analyze	analytical	analytically

Task 6.

1. Ethical hacking is an essential discipline in modern cybersecurity. (*Present Simple*)
2. Researchers are currently conducting penetration testing in controlled environments. (*Present Continuous*)
3. Ethical hacking has significantly improved organizational cybersecurity posture. (*Present Perfect*)
4. Penetration testing did not detect all system vulnerabilities last year. (*Past Simple*)
5. Security incidents were sometimes being simulated in academic environments. (*Past Continuous*)
6. Organizations have recently strengthened their incident response capabilities. (*Present Perfect*)
7. Ethical hacking will play an important role in future cybersecurity strategies. (*Future Simple*)

8. Cybersecurity teams are going to implement advanced monitoring tools soon. (*be going to*)
9. The penetration testing process typically includes reconnaissance and exploitation phases. (*Present Simple*)
10. Professionals were analyzing system logs while attacks were occurring. (*Past Continuous*)
11. The researchers had already completed vulnerability assessment before the audit. (*Past Perfect*)
12. Professionals are going to continuously develop their cybersecurity competencies. (*be going to*)

Task 7.

in, in, against, in, in, with, about, to, in, of, for, on, with, for, to

Task 8.

1. cybersecurity posture
2. penetration testing
3. vulnerability assessment
4. reconnaissance phase
5. incident response capabilities
6. unauthorized access prevention
7. secure software development

Task 9. Students' own answers

Task 10-12.

Penetration Tester

- We have identified several vulnerabilities in your system.
- The testing results show that...
- There is a high/medium/low risk related to...

- We recommend fixing this issue as soon as possible.
- The system was tested using a controlled environment.

Manager / IT Director

- Could you explain the severity of the issue?
- How urgent is this problem?
- What would be the cost of fixing it?
- How can we prevent this in the future?
- Is our data currently at risk?

Lesson 2. Cybersecurity in Business

Task 1.

1–B, 2–J, 3–F, 4–H, 5–D, 6–E, 7–C, 8–A, 9–G, 10–I

Task 2.

1. zero-day vulnerability, 2. information security management, 3. threat mitigation strategy, 4. malware analysis, 5. cyber threat intelligence, 6. vulnerability assessment, 7. network segmentation, 8. incident response plan, 9. encryption key management, 10. secure software development lifecycle (SDLC)

Task 4.

1. **True**
2. **False** – Information security management includes both technical tools and organizational policies and procedures.
3. **True**
4. **True**
5. **False** – An incident response plan is essential even if antivirus software is used, as it guides reaction to attacks.

6. **False** – A zero-day vulnerability is an unknown security flaw that has no available patch.
7. **True**
8. **False** – Threat mitigation strategy is used to reduce or minimize the impact of cyberattacks, not increase them.
9. **True**
10. **True**

Task 5.

1. therefore, 2. as a result, 3. however, 4. in addition, 5. consequently, 6. therefore, 7. however, 8. as a result, 9. in addition

Task 6.

1. have improved, 2. have not found, 3. have responded, 4. have discovered, 5. have not implemented, 6. have conducted, 7. has strengthened, 8. have not exploited, 9. have developed, 10. have gained

Task 7.

1. Large technology companies have significantly improved their cybersecurity systems to protect users' sensitive data over recent years.
2. Ethical hackers have already identified critical vulnerabilities in corporate information systems and reported them to organizations.
3. The cybersecurity team has already responded to several complex incidents using advanced threat analysis tools.
4. Researchers have developed new malware analysis methods that allow faster identification of attack types.
5. Many organizations have not yet implemented effective encryption key management, which increases the risk of data leaks.
6. IT specialists have conducted numerous vulnerability assessments in complex network infrastructures of large companies.

7. The company has already significantly strengthened its incident response plan after several recent cyberattacks.
8. Attackers have exploited previously unknown zero-day vulnerabilities to target critical systems.
9. Cybersecurity experts have developed innovative tools for detecting and mitigating cyber threats in real time.
10. Companies have gained significant practical experience in protecting information systems after a series of previous cyber incidents.

Task 8.

1. vulnerability assessment, 2. incident response plan, 3. malware analysis, 4. threat mitigation strategy, 5. zero-day vulnerability, 6. encryption key management, 7. secure software development lifecycle (SDLC), 8. network segmentation, 9. information security management, 10. cyber threat intelligence.

Task 9.

1. Cybersecurity is essential for modern businesses *because it protects sensitive data, ensures business continuity, and helps maintain customer trust in a highly digital environment.*
2. Ethical hacking helps organizations improve security *by identifying system vulnerabilities before real attackers can exploit them and by simulating real-world cyberattacks in a controlled way.*
3. Penetration testing is important in business environments *because it allows companies to evaluate the strength of their security systems and discover weaknesses in networks, applications, and infrastructure.*
4. One major cyber threat for companies today *is phishing attacks, where attackers trick employees into revealing confidential information such as passwords or financial data.*

5. Companies should invest in cybersecurity tools *such as encryption systems, intrusion detection software, firewalls, and multi-factor authentication to strengthen their protection.*
6. A strong cybersecurity posture is necessary *because it reduces the risk of cyberattacks, improves resilience, and ensures compliance with international security standards.*
7. If a company does not protect its systems properly, *it may suffer data breaches, financial losses, reputational damage, and legal consequences.*
8. Incident response plans are useful when a cyberattack occurs *because they provide clear steps for detecting, containing, and recovering from security incidents.*
9. Network segmentation improves security *because it divides a network into smaller isolated parts, limiting the spread of attacks and protecting critical systems.*
10. In the future, cybersecurity will become even more important *because digital technologies will continue to grow and cyber threats will become more advanced and frequent.*

Task 10.

1. **False** – Cybersecurity is important for all businesses, including small and medium-sized companies, not only large ones.
2. **True**
3. **True**
4. **False** – Multi-factor authentication increases security by adding an extra layer of protection.
5. **True**
6. **False** – Cybersecurity threats can come from both outside and inside an organization.
7. **True**

Lesson 3. Artificial Intelligence & Cybersecurity

Task 1.

1–C, 2–A, 3–B, 4–D, 5–E, 6–F, 7–G, 8–H, 9–I, 10–J

Task 2.

Noun	Verb	Adjective	Adverb
algorithmic optimization	optimize	optimized	optimally
encryption	encrypt	encrypted	encryptedly*
authentication	authenticate	authentic authenticated	/ authentically
infiltration	infiltrate	infiltrative	infiltratively
anomaly detection	detect	detectable	detectably
computational resilience	enhance strengthen	/ resilient	resiliently
cybersecurity governance	govern	governed	governably*

Task 4. 1-a, 2-c, 3-b, 4-b, 5-c, 6-a, 7-c

Task 5.

1. mitigate, 2. schemes, 3. vulnerabilities, 4. cutting-edge, 5. synergy, 6. mitigate, 7. schemes, 8. vulnerabilities, 9. cutting-edge, 10. synergy

Task 6.

1. mitigate cyber risks, 2. vast datasets, 3. anomalous behavioral patterns, 4. cutting-edge technologies, 5. vulnerabilities, 6. automated threat detection, 7. potential security threat, 8. synergy .

Task 7.

1. detecting, 2. analyzing, 3. to improve, 4. to exploit, 5. to recognize, 6. exposing, 7. developing, 8. processing, 9. introducing, 10. identifying.

Task 8.

1. to monitor, 2. to detect, 3. losing, 4. analyzing, 5. updating, 6. to gain, 7. ignoring, 8. improve, 9. to use, 10. blocking.

Task 9.

1. detect, 2. ignoring, 3. to improve, 4. to access, 5. to analyze, 6. (correct), 7. protecting, 8. to recognize, 9. to introduce, 10. to secure.

Task 10. Speaking (possible answers)

The cyberattack may have been caused by weak authentication systems, poor password management, unpatched software vulnerabilities, phishing attacks, insufficient firewall protection, outdated security infrastructure, or lack of employee cybersecurity awareness. To stop further damage immediately, the company should isolate affected systems from the network, disable compromised accounts, activate the incident response plan, apply urgent security patches, monitor network activity for ongoing threats, and inform both cybersecurity specialists and relevant stakeholders.

For long-term improvement, the organization should implement multi-factor authentication, strengthen encryption for data storage and transmission, conduct regular security audits and vulnerability assessments, provide continuous employee training, upgrade firewalls and intrusion detection systems, and establish reliable backup and disaster recovery mechanisms. AI-based cybersecurity systems should be introduced or further improved because they enhance real-time threat detection, identify anomalous behavior patterns, and reduce response time through automation.

Overall, the best solution is a multi-layered cybersecurity strategy that combines immediate containment measures, long-term infrastructure improvements, continuous staff training, and AI-driven security technologies to ensure system resilience, scalability, and strong protection against future cyberattacks.

Навчальне видання

Кузьменко Юлія Олександрівна

кандидат педагогічних наук, доцент кафедри лінгводидактики та
іноземних мов ДУІТЗ

Дякун Катерина Олексіївна

старший викладач кафедри лінгводидактики та іноземних мов ДУІТЗ

ПРАКТИКУМ

для аудиторної та самостійної роботи з англійської мови

ЧАСТИНА 1

для здобувачів 2 курсу ВК «Англійська для ІТ та кібербезпеки»
першого (бакалаврський) рівня вищої освіти
спеціальностей спеціальностей F2, F3, F5, F6, F7

електронне видання

Одеса 2026