

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх справ
Кафедра мовної підготовки

Кочина В. В.
Статівка О.О.

CyberPol English
Англійська мова для фахівців кіберполіції

Навчальний посібник з англійської мови для здобувачів вищої освіти
першого (бакалаврського) рівня за спеціальністю
F5 Кібербезпека та захист інформації

Кам'янець-Подільський
2026

УДК 811.111'276.6:004.056(075.8)
К75

*Рекомендовано до друку Вченою радою
Харківського національного університету внутрішніх справ
(протокол № 1 від 18.08.2026 року)*

Автори:

Кочина Валентина Василівна, кандидат педагогічних наук, доцент, доцент кафедри мовної підготовки Харківського національного університету внутрішніх справ

Статівка Олена Олександрівна, кандидат педагогічних наук, доцент, завідувач кафедри мовної підготовки Харківського національного університету внутрішніх справ

Рецензенти:

Березнева Ірина Миколаївна, доцент кафедри іноземних мов центру мовної підготовки Національної академії Національної гвардії України,

Ірина Леонідівна Кравець, кандидат педагогічних наук, доцент кафедри мовної підготовки Харківського національного університету внутрішніх справ

- К75** **CyberPol English. Англійська мова для фахівців кіберполіції:** навч. посіб. / В. В. Кочина, О. О. Статівка; Харків. нац. ун-т внутр. справ. — Кам'янець-Подільський: ХНУВС, 2026. 256 с.
- Навчальний посібник «**CyberPol English. Англійська мова для фахівців кіберполіції**» призначений для курсантів, студентів і слухачів закладів вищої освіти системи МВС України, працівників підрозділів кіберполіції, а також фахівців у сфері кібербезпеки, інформаційних технологій та цифрових розслідувань.
- Метою посібника є формування та розвиток професійної англомовної комунікативної компетентності, необхідної для ефективного спілкування у сфері протидії кіберзлочинності, кібербезпеки та цифрових розслідувань. Тематичний матеріал охоплює актуальну професійну лексику з кіберзлочинності, цифрової криміналістики, мережових технологій, захисту інформації, кіберінцидентів, цифрових доказів, міжнародного співробітництва правоохоронних органів та сучасних кіберзагроз.

ПЕРЕДМОВА

Сучасна кіберзлочинність є одним із найбільш динамічних і транскордонних викликів для правоохоронних органів усього світу. Розслідування кіберінцидентів, обмін цифровими доказами, взаємодія з іноземними правоохоронними органами, міжнародними організаціями та представниками ІТ-сектору потребують не лише ґрунтовної фахової підготовки, а й належного рівня володіння англійською мовою. Саме англійська сьогодні є одним із ключових інструментів професійної комунікації у сфері кібербезпеки, цифрової криміналістики та протидії кіберзлочинності.

Навчальний посібник **«CyberPol English. Англійська мова для фахівців кіберполіції»**, підготовлений для здобувачів освіти та фахівців Харківського національного університету внутрішніх справ, спрямований на формування й розвиток професійної англійської комунікативної компетентності у сфері кібербезпеки, кіберполіції та цифрових розслідувань.

Посібник призначений для курсантів, студентів і слухачів закладів вищої освіти системи МВС України, працівників підрозділів кіберполіції, а також фахівців у галузі кібербезпеки, інформаційних технологій, цифрової криміналістики та правоохоронної діяльності, які прагнуть удосконалити навички професійного спілкування англійською мовою.

Концепція посібника ґрунтується на поетапному формуванні мовної та професійно-комунікативної компетентності. Матеріал кожного наступного юніту поступово ускладнюється: від базового рівня А2 до рівня В2 відповідно до Загальноєвропейських рекомендацій з мовної освіти. Такий підхід дає змогу послідовно розширювати словниковий запас здобувачів освіти, ускладнювати граматичний і синтаксичний матеріал, переходити від опрацювання загальнонавчальної професійної лексики до роботи зі спеціалізованими англійськими текстами та ситуаціями професійного спілкування.

Розподіл і обсяг навчального матеріалу та вправ у кожному юніті визначено з урахуванням кількості аудиторних і самостійних годин, передбачених освітньою програмою. Це забезпечує можливість гнучкого використання посібника залежно від рівня підготовки здобувачів освіти, навчального навантаження та організації освітнього процесу. Завдання, призначені для самостійного опрацювання, позначено символом*.

Тематика посібника охоплює актуальні професійні сфери, зокрема кібербезпеку, кіберзлочинність, цифрову криміналістику, мережеві технології, захист інформації, шкідливе програмне забезпечення, фішинг та соціальну інженерію, криптографію, цифрові докази, розслідування кіберінцидентів, OSINT, аналіз кіберзагроз, міжнародне співробітництво правоохоронних органів та сучасні виклики у сфері цифрової безпеки.

Структура посібника передбачає системне поєднання мовної та професійної підготовки. Кожен тематичний блок містить глосарій ключових термінів, професійно орієнтовані тексти та комплекс вправ, спрямованих на розвиток основних видів мовленнєвої діяльності — читання, аудіювання,

говоріння та письма. Практичні завдання моделюють типові ситуації професійної комунікації, що можуть виникати під час виконання службових обов'язків: обговорення кіберінциденту, опис цифрових доказів, підготовка службового повідомлення, аналіз технічної інформації, проведення брифінгу, комунікація з іноземними колегами та підготовка професійної документації.

Окреме місце в посібнику посідають практичні кейси, наближені до реальних завдань фахівців кіберполіції. Їх використання сприяє розвитку не лише мовних навичок, а й уміння аналізувати професійну ситуацію, формулювати висновки, аргументувати власну позицію, ставити уточнювальні запитання та приймати рішення англійською мовою.

Особливу увагу приділено формуванню навичок роботи з англійською професійною документацією: повідомленнями про кіберінциденти, технічними описами, звітами, електронним листуванням, аналітичними матеріалами та іншими видами документів, з якими фахівець у сфері кібербезпеки може працювати у професійній діяльності. Передбачено також завдання на підготовку професійних повідомлень, звітів, описів інцидентів і ділового листування.

Важливою складовою посібника є комплекс завдань, орієнтованих на підготовку до єдиного вступного іспиту (ЄВІ) з іноземної мови. Такі завдання спрямовані на вдосконалення навичок читання, розуміння англійського тексту, роботи з лексикою та граматикою, визначення правильної відповіді на основі контексту й виконання інших типів завдань, необхідних для успішного складання іспиту. Поєднання загальної підготовки з професійною тематикою дає змогу одночасно розвивати мовну компетентність і готувати здобувачів освіти до виконання стандартизованих тестових завдань.

Посібник може використовуватися під час аудиторної та самостійної роботи, у процесі професійної підготовки, перепідготовки та підвищення кваліфікації працівників правоохоронних органів і фахівців у сфері кібербезпеки. Запропонована структура також дає змогу викладачеві адаптувати навчальний матеріал до конкретного рівня мовної підготовки та потреб навчальної групи.

Автори посібника прагнули поєднати сучасну англійську мову, професійну термінологію та практичну спрямованість навчання. Адже для сучасного фахівця кіберполіції володіння англійською мовою є не лише академічною компетентністю, а й необхідною умовою ефективної професійної діяльності, міжнародної взаємодії та доступу до світового інформаційного й професійного простору.

ЗМІСТ

Передмова	3
Unit 1. Kharkiv National University of Internal Affairs and the cyber police in the cybersecurity system	6
Final Test Unit 1	21
Unit 2. Network security. The basics of cybersecurity	25
Final Test Unit 2	50
Unit 3. Collecting and analysing data methods in computer networks	62
Final Test Unit 3	79
Unit 4. Modern information systems and networks protection	83
Final Test Unit 4	113
Unit 5. Cyberattacks and network security	116
Final Test Unit 5	138
Unit 6. The basics of cryptography and steganography	141
Final Test Unit 6	162
Unit 7. Introduction to Digital Forensics and Cyber Investigations	166
Final Test Unit 7	205
Unit 8. Digital Forensics in Modern Technologies	209
Final Test Unit 8	250
References	254



Unit 1

Kharkiv National University of Internal Affairs and the cyber police in the cybersecurity system

Texts:

1. The Role of Kharkiv National University of Internal Affairs and the Cyber Police in Ensuring Cybersecurity
2. Training of specialists in information and analytical support and cyber security for the National Police of Ukraine

Glossary

Kharkiv National University of Internal Affairs – Харківський національний університет внутрішніх справ
кібербезпека — cybersecurity
кіберзлочинність — cybercrime
кіберзагроза — cyber threat
інформаційна безпека — information security
цифрові технології — digital technologies
правоохоронні органи — law enforcement agencies
курсант — cadet
студент — student
навчально-науковий інститут — educational and scientific institute
підготовка фахівців — training of specialists
інформаційно-аналітичне забезпечення — information and analytical support
розслідування кіберзлочинів — cybercrime investigation
повномасштабне вторгнення — full-scale invasion
релокація — relocation
практичний досвід — practical experience
співпраця — cooperation
підрозділ поліції — police unit
кіберполіція — cyber police
викрадення особистих даних — identity theft
онлайн-шахрайство — online fraud
кібератака — cyberattack
шкідливе програмне забезпечення — malicious software (malware)
запобігання злочинам — crime prevention
обробка інформації — information processing
захист інформаційних систем — protection of information systems
бакалаврський рівень — bachelor's level
спеціальне звання — special rank
лейтенант поліції — police lieutenant
слідчий — investigator

оперативний працівник — operative officer

Text

The Role of Kharkiv National University of Internal Affairs and the Cyber Police in Ensuring Cybersecurity

In the modern world, cybersecurity has become an essential part of national and personal safety. As people increasingly rely on digital technologies for communication, education, and business, the number of cyber threats continues to grow. Therefore, it is important for Ukraine to develop strong institutions that can effectively respond to these challenges.

Kharkiv National University of Internal Affairs plays a key role in preparing both students and cadets for work in the field of cybersecurity. The university provides professional education and practical training in areas such as information security, cybercrime investigation, and digital technologies. Both students and cadets gain the necessary knowledge and skills to understand modern cyber threats and to protect information systems.

It is important to understand the difference between students and cadets. Students usually study at the university as civilians and focus mainly on academic knowledge and professional skills. Cadets, in contrast, are members of law enforcement training programs. They combine their studies with practical police training, follow stricter discipline, and prepare for future service in the National Police.

A significant role in cybersecurity education belongs to Educational and Scientific Institute No. 4 of the university. This institute specializes in training professionals in information and analytical support and cybersecurity for the National Police of Ukraine. It has many years of experience in preparing law enforcement officers who have advanced knowledge and practical skills in the field of modern information technologies.

Since 2015, the institute has been training specialists for a new unit of the National Police — the cyber police. In 2022, due to the full-scale invasion of Russia and constant shelling in Kharkiv, the institute was relocated to a safer region of Ukraine. Despite these challenges, the educational process continued. In 2024, the faculty was reorganized into Educational and Scientific Institute No. 4, which reflects its growing importance and wider responsibilities.

Today, the institute trains specialists at the bachelor's level in several fields, including cybersecurity, law enforcement, and law. Graduates receive the rank of police lieutenant and can work in different departments of the National Police, such as the cyber police, criminal analysis units, migration police, and investigative divisions. They may work as оперативні офіцери (operative officers), investigators, analysts, engineers, or IT specialists.

The training at the institute combines theory and practice. Cadets often cooperate with real police units, which helps them gain professional experience. This

system also allows police departments to identify talented cadets and invite them to work in the future.

The cyber police of Ukraine is a specialized unit responsible for combating cybercrime. Its officers investigate hacking, online fraud, identity theft, and cyberattacks. They also work on prevention and educate citizens about safe behavior on the Internet.

Graduates of the institute are able to perform many important tasks. They can detect and prevent cybercrime, analyze information in digital systems, use modern technologies in police work, and build secure information systems. Their work helps improve the effectiveness of law enforcement and strengthens national cybersecurity.

In conclusion, Kharkiv National University of Internal Affairs and the cyber police play a crucial role in ensuring cybersecurity in Ukraine. Their cooperation, education, and practical training help create a safer digital environment and protect society from modern cyber threats.

Questions:

1. Why has cybersecurity become an essential part of modern life?
2. What risks are increasing with the development of digital technologies?
3. What role does Kharkiv National University of Internal Affairs play in cybersecurity?
4. What knowledge and skills do students and cadets gain at the university?
5. What is the main difference between students and cadets?
6. What is the purpose of Educational and Scientific Institute No. 4?
7. When did the institute start training specialists for the cyber police?
8. What specialties can students and cadets study at the institute?
9. What positions can graduates work in after finishing their studies?
10. How does the institute cooperate with police units?
11. What types of cybercrimes does the cyber police investigate?
12. How does the cyber police help prevent cybercrime?
13. What practical skills do graduates develop during their training?
14. Why is cooperation between education and law enforcement important?
15. How do graduates contribute to national cybersecurity?

Exercise 1. Match the Words with Their Definitions. Match the words (1–10) with the definitions (A–J).

1	cybersecurity	A. A person who studies information and data to find useful facts.
2	cybercrime	B. Actions taken to stop something bad from happening.
3	cadet	C. Protection of computer systems and networks from digital threats.
4	law enforcement	D. Criminal activities committed using computers or the Internet.
5	investigator	E. A student in a police or military training program.
6	information security	
7	cyberattack	

8	analyst	F. The protection of information from unauthorized access.
9	fraud	G. A person who examines crimes to discover the truth.
10	prevention	H. A dishonest act intended to obtain money or benefits.
		I. Activities of police and other authorities to maintain public order.
		J. An attempt to damage or gain unauthorized access to computer systems.

Exercise 2. Complete the Sentences. Fill in the blanks with the words from the box.

Word Box:

cybersecurity, cadets, investigators, cybercrime, analysts, cyberattacks, discipline, citizens, lieutenant, technologies

1. Modern _____ helps protect digital information and systems.
2. The cyber police investigate different types of _____.
3. _____ receive both academic and police training.
4. Future police officers must follow strict _____.
5. Cyber police officers investigate hacking and other _____.
6. Graduates can work as _____ in criminal investigations.
7. Some graduates become information _____ and process digital data.
8. New digital _____ create both opportunities and risks.
9. The cyber police educate _____ about online safety.
10. After graduation, cadets receive the rank of police _____.

Exercise 3. Choose the Correct Answer (A, B, or C).

1. Kharkiv National University of Internal Affairs prepares specialists in:
 - A) Agriculture
 - B) Cybersecurity
 - C) Medicine
2. Students usually study as:
 - A) Civilians
 - B) Soldiers
 - C) Detectives
3. Cadets combine their studies with:
 - A) Business practice
 - B) Police training
 - C) Medical training
4. Educational and Scientific Institute No. 4 specializes in:
 - A) Architecture

- B) Journalism
- C) Cybersecurity and information support
- 5. The institute started training specialists for the cyber police in:
 - A) 2010
 - B) 2015
 - C) 2020
- 6. In 2022 the institute was relocated because of:
 - A) Economic problems
 - B) Educational reforms
 - C) The full-scale invasion
- 7. Graduates may work as:
 - A) Pilots
 - B) Engineers
 - C) Pharmacists
- 8. The cyber police investigate:
 - A) Forest fires
 - B) Online fraud
 - C) Road construction
- 9. Cyber police officers also focus on:
 - A) Prevention
 - B) Entertainment
 - C) Marketing
- 10. Cooperation with police units helps cadets gain:
 - A) Professional experience
 - B) Financial support
 - C) Academic degrees

Exercise 4. Find the Missing Word. Complete the sentences using one suitable word from the text.

1. Cyber police officers investigate online _____.
2. Information systems must be protected from cyber _____.
3. The institute trains specialists for the National _____.
4. Graduates can work in criminal analysis _____.
5. Cadets receive practical police _____.
6. Cybersecurity helps create a safer digital _____.
7. The cyber police educate people about safe behavior on the _____.
8. Graduates learn how to build secure information _____.
9. The institute combines theory and _____.
10. Modern cyber threats can affect both national and personal _____.

***Exercise 5. Complete the Word Combinations. Match the words from Column A with the words from Column B to form common collocations from the text.**

Column A	Column B
----------	----------

1. cyber	A. systems
2. information	B. training
3. digital	C. security
4. practical	D. technologies
5. law	E. threats
6. cyber	F. enforcement
7. information	G. police
8. cyber	H. analysis
9. police	I. crime
10. modern	J. lieutenant

*** Exercise 6. Translate into English.** Translate the following phrases into English using the vocabulary from the text.

1. кібербезпека
2. кіберполіція
3. інформаційна безпека
4. правоохоронна діяльність
5. цифрові технології
6. розслідування кіберзлочинів
7. практична підготовка
8. онлайн-шахрайство
9. інформаційні системи
10. національна безпека

*** Exercise 7. Make your own sentences using the following words:**

1. cybersecurity
2. cadet
3. cyber police
4. investigator
5. cyberattack
6. analyst
7. information security
8. law enforcement
9. digital technologies
10. cybercrime

Glossary

information analysis - інформаційний аналіз
 confidential information - конфіденційна інформація
 criminal law - кримінальне право
 database management - управління базами даних
 cyber defence - кіберзахист

hacking - хакерство
phishing - фішинг
identity theft - крадіжка особистих даних
malware attack - атака шкідливого програмного забезпечення
digital infrastructure - цифрова інфраструктура
digital forensics - цифрова криміналістика
electronic evidence - електронні докази
investigative tools - інструменти розслідування
decision-making skills - навички прийняття рішень
teamwork - командна робота
analytical report - аналітичний звіт
critical thinking - критичне мислення
logical analysis - логічний аналіз
international cooperation - міжнародне співробітництво
professional environment - професійне середовище
legal responsibility - юридична відповідальність
human rights - права людини
professional ethics - професійна етика
public safety - громадська безпека

Text

Training specialists in data analysis and cyber security for the National Police of Ukraine

Cadets of the Cyber Police of the National Police of Ukraine receive modern professional training in the field of cybersecurity and information analysis. Their future profession is very important because cybercrime has become one of the biggest challenges in modern society. Criminals use digital technologies to steal information, attack computer systems, and commit online fraud. For this reason, cyber police cadets must develop strong technical and analytical skills during their studies.

The educational process combines theoretical knowledge with practical training. Cadets study criminal law, cybersecurity, digital communications, and information technologies. They also learn the basics of programming and database management. Special attention is paid to information protection and cyber defence methods. Future officers must understand how modern cyber threats affect individuals, organisations, and state institutions.

One of the most important subjects for cadets is cybersecurity. They study different types of cybercrime, including hacking, phishing, identity theft, and malware attacks. Cadets learn how cybercriminals gain access to confidential information and damage computer systems. They also study methods of preventing cyberattacks and protecting digital infrastructure. Knowledge of cybersecurity helps future officers respond effectively to online threats.

Another important area of training is digital forensics. Cadets learn how to collect, preserve, and analyse electronic evidence. They work with specialised

software and modern investigative tools. Digital evidence often plays a key role in criminal investigations. Future cyber police officers must know how to examine computers, mobile devices, and online activity. Accuracy and attention to detail are extremely important in this type of work.

Practical training is an essential part of education for cyber police cadets. They participate in simulations of cyber incidents and emergency situations. During practical exercises, cadets investigate fictional cybercrimes and solve technical problems in teams. These activities help them improve their decision-making skills and prepare for real professional tasks. Practical experience also develops communication and teamwork abilities.

Information and analytical support is another important part of cyber police work. Cadets learn how to process large amounts of digital information quickly and effectively. They study analytical methods used in criminal investigations and intelligence activities. Future specialists must identify important information, recognise threats, and prepare analytical reports. Critical thinking and logical analysis are necessary for successful police operations.

English language skills are also very important for cyber police cadets. Many cybercrimes are international, so officers often cooperate with foreign organisations and cybersecurity experts. Cadets study professional English vocabulary connected with information technologies and digital investigations. They learn how to communicate effectively in international professional environments. Knowledge of English gives future officers access to international experience and modern cybersecurity resources.

Ethics and legal responsibility are essential principles in the training of cyber police cadets. Future officers work with sensitive personal information and confidential police databases. They must follow legal procedures and respect human rights during investigations. Cadets study professional ethics, discipline, and responsible behaviour. Honesty and professionalism are necessary qualities for every cyber police officer.

The National Police of Ukraine continues to modernise the education of cyber police cadets. Educational institutions introduce innovative technologies and modern teaching methods into the learning process. Future officers must be prepared for new cyber threats and rapidly changing technologies. Their work plays an important role in protecting national security and public safety. Well-trained cyber police cadets are an important part of the future development of law enforcement in Ukraine.

Questions:

1. Why is the training of cyber police cadets important today?
2. What subjects do cadets study during their education?
3. Why is cybersecurity one of the most important subjects for cadets?
4. What types of cybercrime do future officers study?
5. What is digital forensics?
6. Why is practical training essential for cyber police cadets?

7. What skills do cadets develop during practical exercises?
8. Why are analytical skills important for future officers?
9. How does English help cyber police specialists in their work?
10. Why must cyber police officers follow ethical and legal principles?
11. What qualities are necessary for every cyber police officer?
12. How does the National Police of Ukraine modernise cyber police education?
13. Why is teamwork important in cyber police training?
14. What role does information analysis play in police investigations?
15. How do cyber police specialists help protect national security?

Exercise 8. Multiple Choice

1. Why is cybersecurity important today?
 - A) Because people do not use the Internet
 - B) Because cyber threats are increasing
 - C) Because technology is disappearing
 - D) Because there are no online risks
2. What does the university provide?
 - A) Only theoretical knowledge
 - B) Only physical training
 - C) Education and practical training
 - D) Only online courses
3. Who studies at the university?
 - A) Only cadets
 - B) Only students
 - C) Both students and cadets
 - D) Only teachers
4. What is the main difference between students and cadets?
 - A) Students work in police
 - B) Cadets combine study with police training
 - C) Students have more discipline
 - D) There is no difference
5. What is the main focus of Institute No. 4?
 - A) Medicine
 - B) Cybersecurity and analytical support
 - C) Agriculture
 - D) Art
6. When did the institute start training cyber police specialists?
 - A) 2010
 - B) 2015
 - C) 2020
 - D) 2024
7. Why was the institute relocated in 2022?
 - A) Because of renovation

- B) Because of weather
 - C) Because of the full-scale invasion
 - D) Because of student demand
8. What degree do graduates receive?
 - A) Master's degree
 - B) Doctor's degree
 - C) Bachelor's degree
 - D) No degree
 9. What rank do graduates get after finishing their studies?
 - A) Sergeant
 - B) Captain
 - C) Police lieutenant
 - D) General
 10. What crimes does the cyber police investigate?
 - A) Only traffic violations
 - B) Only financial crimes
 - C) Cybercrimes like hacking and fraud
 - D) Only offline crimes
 11. What do graduates learn to do?
 - A) Ignore cyber threats
 - B) Analyze and protect information systems
 - C) Only write reports
 - D) Only teach students
 12. Why is cooperation between the university and police important?
 - A) It reduces education quality
 - B) It gives practical experience
 - C) It stops training
 - D) It limits knowledge

Exercise 9. True / False

1. Cybersecurity is not important in modern society.
2. The number of cyber threats is increasing today.
3. Kharkiv National University of Internal Affairs trains only IT specialists.
4. Both students and cadets study cybersecurity at the university.
5. Cadets are civilians and do not follow strict discipline.
6. Educational and Scientific Institute No. 4 specializes in cybersecurity and analytical support.
7. The institute started training cyber police specialists in 2015.
8. The institute was relocated because of peaceful conditions in Kharkiv.
9. In 2024, the faculty was reorganized into an institute.
10. Graduates can work only in cyber police units.
11. The cyber police investigate crimes like hacking and online fraud.
12. The cyber police also work on prevention and education.

Exercise 10. Fill in the Gaps

1. Cybersecurity protects _____ systems from attacks.
2. Cadets receive _____ and practical training.
3. Cyber police investigate _____ crimes.
4. The university provides high-quality _____.
5. _____ theft is a serious cybercrime.
6. Hackers may use _____ software to damage systems.
7. Online _____ can affect many users.
8. The institute focuses on information and _____ support.
9. Students gain _____ experience during study.
10. Cyber police also focus on crime _____.
11. The institute was _____ in 2022 due to war.
12. Modern _____ technologies are widely used today.
13. Police officers work in different _____ units.
14. Cooperation improves the quality of _____.
15. The main goal is to protect _____ systems.

Exercise 11. Match the words with their meanings:

1. Cybersecurity	A. Illegal use of someone's personal data
2. Cadet	B. Protection of digital systems and data
3. Cybercrime	C. Harmful software
4. Investigation	D. Attack on computer systems
5. Malware	E. Process of collecting evidence about a crime
6. Cyberattack	F. Police unit fighting cybercrime
7. Identity theft	G. Use of modern computer technologies
8. Online fraud	H. Criminal activity on the Internet
9. Data protection	I. Working together
10. Cyber police	J. Protection of personal and official data
11. Digital technologies	K. Group of interconnected computers and data
12. Information system	L. A person in police training
13. Law enforcement	M. Activities of police and legal authorities
14. Cooperation	N. Stopping crimes before they happen
15. Prevention	O. Illegal online deception

***Exercise 12. Translate into English:**

1. кібербезпека
2. кіберзлочинність
3. кіберполіція
4. розслідування
5. шкідливе програмне забезпечення
6. захист даних
7. онлайн-шахрайство
8. викрадення даних

9. цифрові технології
10. правоохоронні органи
11. практичний досвід
12. співпраця
13. навчальний інститут
14. кібератака
15. запобігання злочинам

***Exercise 13. Put the words in the correct order:**

1. cybersecurity / important / is / very
2. cadets / police / become / future
3. investigate / cyber police / crimes / cyber
4. digital / use / technologies / students
5. protection / data / is / important
6. the / institute / specialists / trains
7. cybercrime / increasing / is
8. cooperation / is / important
9. hackers / systems / attack
10. police / public / protect / the
11. students / experience / gain / practical
12. cyber / threats / modern / are
13. information / systems / protect / we
14. training / includes / practice / theory
15. cyber police / fraud / investigate / online

***Exercise 14. Correct the mistakes:**

1. Cybercrime is not dangerous.
2. Cadets do not study.
3. Cyber police ignore online crimes.
4. Malware is always good.
5. Students never use computers.
6. Cybersecurity protects food.
7. The institute trains doctors.
8. Identity theft is legal.
9. Cyber police prevent fraud.
10. Digital technologies are useless.
11. Cooperation is not important.
12. Students have no practical training.
13. Cyberattacks help systems.
14. Police do not investigate crimes.
15. Cybersecurity is not needed today.

***Exercise 15. Discussion Questions**

1. Why is cybersecurity important today?
2. What is cybercrime?
3. What do cyber police do?
4. What is the role of cadets?
5. What skills do students need?
6. How can people stay safe online?
7. What is malware?
8. What is identity theft?
9. Why is cooperation important?
10. What do you know about cyberattacks?
11. Would you like to work in cyber police? Why?
12. What is digital technology?
13. How can cybercrime be prevented?
14. What is the role of education in cybersecurity?
15. What dangers exist on the Internet?

Exercise 16. Read the texts below. Match choices (A–H) to texts (1–5). There are three choices you do not need to use.

(1) _____ Future specialists in cyber police study different types of cybercrime, including online fraud, hacking, and identity theft. They learn how criminals use modern technologies to attack computer systems and steal personal data. During their education, students work with special cybersecurity software and digital investigation tools. They also learn how to collect electronic evidence and analyse online activity. In addition, students study methods of protecting confidential information from cyber threats and illegal access.

(2) _____ Information analysts in the National Police work with large amounts of digital information every day. Their task is to identify important facts, analyse data, and support criminal investigations. Students learn how to use databases, analytical platforms, and modern information systems. They also develop critical thinking and decision-making skills during their studies. Analytical specialists must work accurately because even small mistakes may influence investigations.

(3) _____ Practical training plays an essential role in the education of future cybersecurity specialists. Students participate in simulations of cyberattacks and learn how to respond to dangerous situations. During practical classes, they analyse real examples of online crimes and security breaches. They also work in teams to solve technical and investigative problems. Such activities help students gain professional experience and prepare for real police work.

(4) _____ Modern cybercrime investigations often involve cooperation with international organisations and foreign cybersecurity experts. For this reason, future police officers improve their English language skills during their education. Students learn professional vocabulary connected with information security and digital technologies. They also study international standards of cybersecurity and methods

used in other countries. Effective communication is necessary for successful international investigations and information exchange.

(5) _____ Cybersecurity specialists in the National Police must always follow ethical and legal principles in their work. They often deal with sensitive personal information and confidential police databases. Students study professional ethics and legal responsibility during their training. They learn how to protect citizens' privacy and use information responsibly. Future officers must understand the importance of honesty, responsibility, and professional behaviour in cybersecurity investigations.

Choices:

- A. Students develop skills in investigating online crime.
- B. Analytical thinking is essential for processing information.
- C. Practical exercises prepare students for real situations.
- D. International cooperation requires communication skills.
- E. Ethical behaviour is important in cybersecurity work.
- F. Many officers prefer working without computers.
- G. Some students study only traditional policing methods.
- H. Paper documents are replacing digital technologies.

Exercise 17. Listening. Listen the text and fill the missing space.

Cadets of the Cyber Police of the National Police of Ukraine are trained to become qualified specialists in 1. _____ and information-analytical support. Their role is very important because cybercrime is rapidly increasing in modern society. Criminals use advanced digital technologies to attack individuals, organisations, and government systems. Therefore, cadets must be prepared to respond to complex cyber threats.

The training programme combines theoretical knowledge with practical skills. Cadets study 2. _____, 3. _____, 4. _____, and digital technologies. They also learn how computer networks operate and how data is stored and protected. Special attention is given to information security and secure communication. A key part of training is cybercrime investigation. Cadets learn how to detect and analyse illegal online activities such as hacking, online fraud, and identity theft. They are trained to recognise suspicious digital behaviour and respond quickly to cyber incidents. These skills help reduce damage caused by 5. _____. Digital forensics is an important discipline in their education. Cadets learn how to collect and analyse electronic evidence from computers, mobile devices, and networks. They also practise recovering deleted data and studying digital traces left by criminals. Accuracy and attention to detail are essential in this work.

Practical training is an important part of the programme. Cadets participate in simulations of cyberattacks and 6. _____. They work in teams to solve technical problems and complete real-life scenarios. This helps them develop confidence and decision-making skills under pressure.

Information and analytical skills are essential for cyber police work. Cadets learn how to process large amounts of data and 7. _____ important information. They develop critical thinking and the ability to make logical conclusions. Analytical work supports effective criminal investigations.

Exercise 18. Watch the Video: <https://univd.edu.ua/en/video/1422> and answer the questions.

1. What is one of the main missions of Kharkiv National University of Internal Affairs?

- A. To train medical specialists for hospitals.
- B. To prepare qualified personnel for the National Police of Ukraine.
- C. To provide commercial IT services for businesses.
- D. To train military pilots.

2. What values are emphasized in the university's motto?

- A. Knowledge, Law, and Honor
- B. Service, Technology, and Success
- C. Justice, Security, and Innovation
- D. Discipline, Courage, and Loyalty

3. What kind of training do students and cadets receive at the university?

- A. Only theoretical education
- B. Only physical training
- C. Both theoretical and practical training
- D. Only online training

4. How does the university prepare future law enforcement officers?

- A. By focusing only on legal theory
- B. By combining academic education with practical professional training
- C. By providing only military training
- D. By teaching foreign languages only

5. Why is modern technology important in the educational process of the university?

- A. It helps students play educational games.
- B. It allows the university to replace teachers.
- C. It helps future officers develop professional skills and respond to modern challenges.
- D. It is used only for administrative purposes.

Exercise 19. Discussion Task

Answer the following question in 3–5 sentences.

How can graduates of Kharkiv National University of Internal Affairs contribute to cybersecurity in Ukraine?

FINAL TEST UNIT 1

1. What is cybersecurity?
 - A) Internet games
 - B) Protection of digital systems
 - C) Social media activity
 - D) Offline security only
2. Who are cadets?
 - A) Civilians only
 - B) Police trainees
 - C) Teachers
 - D) Doctors
3. What does cyber police do?
 - A) Build computers
 - B) Investigate cybercrime
 - C) Teach languages
 - D) Repair roads
4. What is identity theft?
 - A) Buying online goods
 - B) Stealing personal data
 - C) Writing emails
 - D) Using social media
5. What does malware mean?
 - A) Useful program
 - B) Harmful software
 - C) Internet provider
 - D) Antivirus system
6. What does the university provide?
 - A) Only theory
 - B) Education and training
 - C) Only sports
 - D) Only online games
7. Cyber threats are:
 - A) Decreasing
 - B) Disappearing
 - C) Increasing
 - D) Not important
8. Cyber police belong to:
 - A) Army
 - B) National Police
 - C) Private company
 - D) School system
9. What do cadets combine?
 - A) Work and rest

- B) Study and police training
 - C) Travel and sport
 - D) Internet and gaming
10. What is cyberattack?
- A) Computer game
 - B) Attack on systems
 - C) Social event
 - D) Lecture
11. What do graduates receive?
- A) Certificate only
 - B) Bachelor's degree
 - C) No qualification
 - D) Diploma only
12. What is cooperation?
- A) Fighting
 - B) Working together
 - C) Studying alone
 - D) Ignoring rules
13. Cyber police also do:
- A) Crime prevention
 - B) Cooking
 - C) Transport services
 - D) Farming
14. What is information system?
- A) Paper documents only
 - B) Computer-based system
 - C) TV program
 - D) Library books
15. What is the main goal of cybersecurity?
- A) Entertainment
 - B) Protection of information
 - C) Advertising
 - D) Shopping
16. phishing
- A) online fishing game
 - B) fake messages to steal data
 - C) software update
 - D) data protection
17. hacker
- A) cyber attacker
 - B) system repairer
 - C) teacher
 - D) hardware device

18. firewall
A) fire protection system
B) network security system
C) antivirus game
D) legal activity
19. malware
A) useful software
B) harmful software
C) hardware device
D) type of virus
20. encryption
A) data protection method
B) type of virus
C) internet speed
D) protection of digital systems
21. cyberattack
A) system attack
B) computer game
C) email service
D) social media
22. identity theft
A) stealing personal data
B) creating accounts
C) online shopping
D) website link
23. cybercrime
A) legal activity
B) illegal online activity
C) education system
D) single computer
24. antivirus
A) protection software
B) hacker tool
C) email service
D) unauthorized access to data
25. password
A) secret access code
B) public username
C) website link
D) internet speed
26. spam
A) useful emails
B) unwanted messages

- C) antivirus alerts
- D) advertising
- 27. network
 - A) connected systems
 - B) single computer
 - C) paper files
 - D) attack on systems
- 28. data breach
 - A) data protection
 - B) unauthorized access to data
 - C) system update
 - D) transport services
- 29. cybersecurity
 - A) internet games
 - B) protection of digital systems
 - C) social media
 - D) type of virus
- 30. cyber police
 - A) online criminals
 - B) law enforcement unit against cybercrime
 - C) IT company
 - D) online fishing game



Unit 2

Network security

Texts:

Text 1. Network security.

Text 2. The Basics of Cybersecurity.

***Text: Network Security and Data Protection in Cybersecurity.**

Text: Types of Malware and Protection Against Cyber Threats.

Text 3. Types of Cyberattacks and Methods of Prevention.

Text 4. Authentication, Authorization, and Access Control in Network Security.

Text 5. Network Protocols and Security Technologies in Cybersecurity.

Text 6. Key Tools and Technologies in Network Security.

Text 7. Key Concepts and Fundamentals of Network Security.

Glossary

Firewall - Мережевий екран (фаєрвол)

Encryption - Шифрування

Decryption - Розшифрування

Malware - Шкідливе програмне забезпечення

Virus - Комп'ютерний вірус

Phishing - Фішинг

Intrusion Detection System (IDS) - Система виявлення вторгнень

Intrusion Prevention System (IPS) - Система запобігання вторгненням

Virtual Private Network (VPN) - Віртуальна приватна мережа

Authentication - Аутентифікація

Authorization - Авторизація

Access Control - Контроль доступу

Data Breach - Витік даних

Cyberattack - Кібератака

Packet Filtering - Фільтрація пакетів

Network Protocol - Мережевий протокол

Secure Socket Layer (SSL) - Протокол захищених сокетів

Transport Layer Security (TLS) - Безпека транспортного рівня

Endpoint Security - Захист кінцевих пристроїв

Two-Factor Authentication (2FA) - Двофакторна аутентифікація

Text

Network security

Network security is an essential part of modern cybersecurity. Every organization uses a firewall to protect its internal systems from external threats. Encryption is applied to sensitive data to ensure that information remains confidential

during transmission. Decryption allows authorized users to access the original data when needed. Malware, such as viruses, worms, and Trojan horses, can cause serious damage to networks. Ransomware is especially dangerous because it blocks access to important files until a payment is made. Spyware secretly collects user information, while adware displays unwanted advertisements.

Phishing attacks trick users into revealing their passwords and personal data. More advanced attacks, such as spear phishing, target specific individuals or companies. A DDoS attack can overwhelm a server and make services unavailable. In a man-in-the-middle attack, hackers intercept communication between two parties. Brute force attacks attempt to guess passwords by trying many combinations. SQL injection targets databases by inserting malicious code. Zero-day attacks exploit unknown vulnerabilities before they are fixed.

Authentication and authorization are crucial for controlling access to systems. Many companies use two-factor or multi-factor authentication for better protection. Network protocols like HTTP, HTTPS, SSL, and TLS ensure secure communication over the internet. A VPN can create a secure connection even on public networks. Antivirus software, IDS, and IPS systems help detect and prevent cyber threats. Regular security patches are important to fix vulnerabilities. Backup systems ensure that data can be restored after a cyberattack. Organizations must also perform risk assessments and follow security policies to reduce the chances of a data breach.

Answer the questions:

1. What is the role of a firewall in network security?
2. Why is encryption important for protecting data?
3. What is the difference between a virus, a worm, and a Trojan horse?
4. How does ransomware affect users and organizations?
5. What is phishing and how does it work?
6. What happens during a DDoS attack?
7. What is a man-in-the-middle attack?
8. Why are authentication and authorization important?
9. How do VPNs help improve network security?
10. Why are backups and security patches essential for organizations?

Exercise 1. Multiple Choice: Network Security. Choose the correct answer (A, B, C, or D).

1. Which security tool protects internal systems from external threats?
A) VPN
B) Firewall
C) IDS
D) Encryption
2. What is the purpose of encryption?
A) To detect malware
B) To filter network packets

- C) To keep data confidential during transmission
 - D) To restore lost files
3. What process converts encrypted data back into its original form?
- A) Authentication
 - B) Authorization
 - C) Packet Filtering
 - D) Decryption
4. Which term refers to harmful software that can damage a network?
- A) Malware
 - B) VPN
 - C) TLS
 - D) Access Control
5. What type of malware can replicate itself and infect files?
- A) Spyware
 - B) Virus
 - C) Adware
 - D) Ransomware
6. Which cyberattack tricks users into revealing passwords and personal information?
- A) SQL Injection
 - B) DDoS Attack
 - C) Phishing
 - D) Brute Force Attack
7. What system is used to detect suspicious activities in a network?
- A) VPN
 - B) Firewall
 - C) IDS
 - D) SSL
8. Which system can automatically block detected threats?
- A) IPS
 - B) Authentication
 - C) TLS
 - D) Decryption
9. What does VPN stand for?
- A) Virtual Protected Network
 - B) Virtual Private Network
 - C) Verified Private Network
 - D) Virtual Packet Network
10. Which process verifies the identity of a user?
- A) Authorization
 - B) Access Control
 - C) Authentication
 - D) Encryption

11. What determines what resources a user is allowed to access?
- A) Authorization
 - B) Firewall
 - C) Decryption
 - D) Malware
12. Which term refers to restricting access to systems and resources?
- A) Data Breach
 - B) Access Control
 - C) Network Protocol
 - D) VPN
13. What is a data breach?
- A) A secure network connection
 - B) A method of authentication
 - C) Unauthorized exposure of sensitive information
 - D) A type of malware
14. Which term describes an attack against computer systems or networks?
- A) Packet Filtering
 - B) Cyberattack
 - C) Authorization
 - D) SSL
15. What is packet filtering used for?
- A) Encrypting files
 - B) Monitoring employees
 - C) Controlling network traffic based on rules
 - D) Creating backups
16. HTTP, HTTPS, SSL, and TLS are examples of:
- A) Malware
 - B) Security Patches
 - C) Network Protocols
 - D) Data Breaches
17. Which protocol was designed to secure communications before TLS?
- A) VPN
 - B) SSL
 - C) IDS
 - D) IPS
18. What does TLS provide?
- A) Endpoint protection
 - B) Secure communication over networks
 - C) Malware detection
 - D) Password recovery
19. What is the main goal of endpoint security?
- A) Protecting end-user devices
 - B) Managing databases

C) Creating VPN connections

D) Filtering packets

20. What additional security measure requires users to provide two forms of verification?

A) Packet Filtering

B) Data Breach

C) Two-Factor Authentication (2FA)

D) Decryption

*Firewall - Мережевий екран — фільтрує трафік між мережами

Encryption - Шифрування — перетворення даних у захищений вигляд

Decryption - Розшифрування — відновлення даних

Cybersecurity - Кібербезпека — захист систем і мереж

Network Security - Безпека мережі — захист мережевої інфраструктури

***Text: Network Security and Data Protection in Cybersecurity**

Cybersecurity is a critical field that focuses on protecting systems, networks, and data from digital threats. One of its key components is network security, which ensures the safety of network infrastructure. A firewall plays an important role in network security by filtering traffic between trusted and untrusted networks. It helps prevent unauthorized access and blocks harmful data.

Encryption is widely used to protect sensitive information by converting it into a secure format. This ensures that even if data is intercepted, it cannot be easily understood. Decryption is the process that allows authorized users to restore the original data from its encrypted form. Together, encryption and decryption provide confidentiality and data protection.

In modern organizations, cybersecurity strategies include multiple layers of defense. Network security tools, such as firewalls and encryption protocols, work together to reduce risks. Without proper protection, systems become vulnerable to cyberattacks. Therefore, companies invest in strong cybersecurity measures to keep their data safe.

***Answer the questions:**

1. What is the main goal of cybersecurity?
2. What role does a firewall play in network security?
3. Why is encryption important for protecting data?
4. What is the purpose of decryption?
5. Why do organizations invest in cybersecurity measures?

Text: The Basics of Cybersecurity

Cybersecurity is the practice of protecting computers, networks, and data from digital attacks. In today's connected world, it is essential for individuals and

organizations to stay safe online. Cybersecurity helps prevent unauthorized access, data theft, and damage to systems.

One of the key elements of cybersecurity is protecting personal information. Users should be careful when sharing data online and use strong passwords. A strong password usually includes letters, numbers, and symbols. Two-factor authentication adds an extra layer of security by requiring a second verification step.

Another important part of cybersecurity is protecting devices from malware. Malware includes viruses, worms, and other harmful software that can damage systems or steal data. Antivirus programs help detect and remove these threats.

Firewalls are also essential tools in cybersecurity. They control incoming and outgoing network traffic and block suspicious activity. Encryption is used to protect sensitive data by converting it into a secure format that only authorized users can read.

Safe online behavior is also very important. Users should avoid clicking on unknown links or downloading suspicious files. Cybersecurity awareness helps reduce the risk of phishing attacks and other online threats. By combining technology and good practices, users can significantly improve their online safety.

Questions:

1. What is cybersecurity?
2. Why is cybersecurity important in today's world?
3. What types of attacks does cybersecurity help prevent?
4. What is the purpose of protecting personal information online?
5. What makes a password strong?
6. What is two-factor authentication?
7. What is malware?
8. Name two examples of malware mentioned in the text.
9. What is the role of antivirus programs?
10. What is a firewall?
11. How does a firewall protect a network?
12. What is encryption used for?
13. Why should users avoid suspicious links and files?
14. What is phishing?
15. How can users improve their online safety?

Exercise 2.

Part 1: Multiple Choice (choose one correct answer):

1.What is cybersecurity?

- A) Game development
- B) Protection of computers and data
- C) Internet speed control
- D) Social media use

2.What does cybersecurity protect?

- A) Cars
- B) Computers and networks
- C) Books
- D) Electricity

3.What is one goal of cybersecurity?

- A) Increase ads
- B) Prevent unauthorized access
- C) Delete passwords
- D) Slow down systems

4.What is personal data?

- A) Weather info
- B) Private user information
- C) Public news
- D) Software updates

5.Why should users protect personal information?

- A) To share it freely
- B) To avoid identity theft
- C) To increase spam
- D) To download games

6.What is a strong password?

- A) 123456
- B) password
- C) Combination of letters, numbers, symbols
- D) Your name

7.What does two-factor authentication do?

- A) Deletes files
- B) Adds extra verification
- C) Blocks internet
- D) Creates viruses

8.What is malware?

- A) Safe software
- B) Harmful software
- C) Internet browser
- D) Firewall tool

9.What does antivirus software do?

- A) Creates passwords
- B) Detects malware
- C) Sends emails
- D) Speeds up Wi-Fi

10.What is a firewall?

- A) A game
- B) Network traffic filter
- C) A keyboard

D) A virus

Part 2: Read the statements and write True (T) or False (F).

1. Cybersecurity focuses on protecting systems, networks, and data from digital threats.
2. Network security is responsible for protecting network infrastructure.
3. A firewall increases internet speed by compressing network traffic.
4. A firewall filters traffic between trusted and untrusted networks.
5. Encryption converts data into a secure format to protect sensitive information.
6. Encrypted data can always be easily understood if it is intercepted.
7. Decryption restores original data from its encrypted form.
8. Only unauthorized users can perform decryption.
9. Encryption and decryption help ensure data confidentiality.
10. Cybersecurity strategies usually rely on a single layer of protection.
11. Firewalls and encryption protocols are important network security tools.
12. Without proper protection, systems may become vulnerable to cyberattacks.
13. Network security and cybersecurity have no connection with each other.
14. Companies invest in cybersecurity measures to protect their data.
15. A firewall can help prevent unauthorized access to a network.
16. Cybersecurity protects systems from attacks.
17. Weak passwords are safe to use.
18. Malware includes viruses and worms.
19. Antivirus software removes threats.
20. Firewalls allow all traffic without filtering.
21. Encryption protects sensitive data.
22. Cybersecurity is not important for individuals.
23. Two-factor authentication improves security.
24. Clicking unknown links is safe.
25. Cybersecurity helps prevent data theft.

Threats

Malware - Шкідливе ПЗ — загальна назва для вірусів, троянів тощо
Virus - Вірус — саморозповсюджуване шкідливе ПЗ
Worm - Черв'як — поширюється без участі користувача
Trojan Horse - Троян — маскується під корисну програму
Ransomware - Програма-вимагач — блокує доступ до даних
Spyware - Шпигунське ПЗ — збирає дані користувача
Adware - Рекламне ПЗ — показує небажану рекламу

Text: Types of Malware and Protection Against Cyber Threats

Malware is a general term used to describe different types of harmful software. It includes viruses, worms, Trojan horses, ransomware, spyware, and adware. A virus is a type of malware that can spread from one computer to another and damage files.

A worm is similar, but it can spread without any user action. Trojan horses disguise themselves as useful programs to trick users into installing them.

Ransomware is one of the most dangerous types of malware because it blocks access to data and demands payment. Spyware secretly collects information about users, such as passwords or browsing habits. Adware is less dangerous but still annoying, as it displays unwanted advertisements. These threats can affect both individuals and organizations.

To protect against malware, users should install antivirus software and keep their systems updated. It is also important to avoid downloading suspicious files or clicking unknown links. Understanding different types of malware helps people stay safe online.

Questions:

1. What is malware?
2. How does a worm differ from a virus?
3. What is the main characteristic of a Trojan horse?
4. Why is ransomware considered dangerous?
5. What can users do to protect themselves from malware?

Exercise 3.

Part 1. Complete the sentences with the correct words from the box.

Words to use:

Malware, Virus, Worm, Trojan Horse, Ransomware, Spyware, Adware

1. _____ is a general term used for harmful software such as viruses, worms, and Trojans.
2. A _____ can spread from one computer to another and infect files.
3. A _____ spreads automatically without requiring user action.
4. A _____ disguises itself as a legitimate program to trick users.
5. _____ blocks access to data and demands payment to restore it.
6. _____ secretly collects information about users, such as passwords and browsing habits.
7. _____ displays unwanted advertisements on a user's device.
8. Viruses, worms, and Trojan horses are all types of _____.
9. Users should avoid downloading suspicious files to reduce the risk of _____ infections.
10. Unlike a virus, a _____ does not need a user to open an infected file in order to spread.
11. A _____ may appear to be useful software, but it contains malicious code.
12. Organizations often use antivirus software to protect against _____.
13. _____ is considered one of the most dangerous cyber threats because it can make important files inaccessible.

14. Personal information can be stolen by _____ without the user's knowledge.
15. Frequent pop-up advertisements are often a sign of _____.

Part 2. Fill in the blanks:

1. Cybersecurity protects _____, networks, and data.
2. A strong _____ includes numbers and symbols.
3. _____ adds extra security verification.
4. _____ is harmful software.
5. A _____ controls network traffic.
6. Antivirus programs detect _____.
7. _____ protects data by encoding it.
8. Users should avoid _____ links.
9. Cybersecurity helps prevent _____ theft.
10. Malware includes viruses and _____.

Attacks

Phishing - Фішинг — шахрайські повідомлення для крадіжки даних
Spear Phishing - Цільовий фішинг — атака на конкретну особу
DDoS Attack - DDoS-атака — перевантаження сервера
Man-in-the-Middle (MITM) - Атака «людина посередині» — перехоплення даних
Brute Force Attack - Атака перебором — підбір пароля
SQL Injection - SQL-ін'єкція — атака на базу даних
Zero-day Attack - Атака нульового дня — використання невідомої вразливості

Text: Types of Cyberattacks and Methods of Prevention

Cyberattacks are becoming more common in today's digital world. One of the most widespread attacks is phishing, where attackers try to trick users into revealing personal information. Spear phishing is a more targeted version of phishing aimed at specific individuals or organizations. Another dangerous type is a DDoS attack, which overloads a server and makes it unavailable to users.

A man-in-the-middle attack happens when a hacker secretly intercepts communication between two parties. Brute force attacks involve trying many password combinations until the correct one is found. SQL injection is used to attack databases by inserting malicious code into queries. Zero-day attacks exploit vulnerabilities that are not yet known or fixed.

These attacks can cause serious damage, including data loss and financial problems. To prevent them, organizations use strong security systems and train employees to recognize threats. Awareness and proper protection are key to reducing risks.

Questions:

1. What is phishing and how does it work?
2. What is the difference between phishing and spear phishing?
3. What happens during a DDoS attack?
4. What is a brute force attack?
5. Why are zero-day attacks difficult to prevent?

Exercise 4. Match the cyberattack terms (1–7) with their correct meanings (A–G).**Words:**

1. Phishing ____
2. Spear Phishing ____
3. DDoS Attack ____
4. Man-in-the-Middle (MITM) ____
5. Brute Force Attack ____
6. SQL Injection ____
7. Zero-day Attack ____

Meanings:

- A. An attack that overloads a server or website with a large amount of traffic.
- B. A targeted phishing attack aimed at a specific person or organization.
- C. An attack that exploits a software vulnerability before it is known or fixed.
- D. Fraudulent messages designed to steal personal information, passwords, or financial data.
- E. An attack where a hacker secretly intercepts communication between two parties.
- F. An attack that attempts to guess a password by trying many different combinations.
- G. An attack that inserts malicious code into database queries to gain unauthorized access.

Exercise 5.*Part 1. Match the attacks with real-life examples.****Attacks:**

1. Phishing ____
2. Spear Phishing ____
3. DDoS Attack ____
4. MITM Attack ____
5. Brute Force Attack ____
6. SQL Injection ____
7. Zero-day Attack ____

Real-life examples:

- A. A hacker uses a newly discovered software flaw before developers release a patch.

- B. A fake email from a bank asks you to enter your password.
- C. An attacker targets a company's CEO with a personalized email.
- D. Millions of requests are sent to a website, causing it to crash.
- E. A hacker intercepts data sent over an unsecured public Wi-Fi network.
- F. An attacker repeatedly tries different passwords until one works.
- G. Malicious commands are entered into a website form to access database records.

Part 2. Matching. Match terms (1–10) with definitions (A–J)

1. Cybersecurity	A) Protects systems from attacks
2. Firewall	B) Filters network traffic
3. Malware	C) Harmful software
4. Antivirus	D) Protects against viruses
5. Encryption	E) Secures data by encoding
6. Password	F) Secret access code
7. Phishing	G) Fake attempt to steal data
8. Two-factor authentication	H) Extra login verification
9. Data	I) Information
10. Network	J) Connected systems

Authentication and Access

Authentication - Аутентифікація — перевірка особи
Authorization - Авторизація — надання прав доступу
Access Control - Контроль доступу — обмеження доступу
Password - Пароль — секретний код доступу
Biometric Authentication - Біометрична аутентифікація — за відбитком, обличчям
Two-Factor Authentication (2FA) - Двофакторна аутентифікація — 2 рівні перевірки
Multi-Factor Authentication (MFA) - Багатофакторна аутентифікація

Text: Authentication, Authorization, and Access Control in Network Security

Authentication and authorization are essential parts of network security. Authentication is the process of verifying a user's identity, while authorization determines what resources the user can access. The most common method of authentication is a password, but it is not always secure.

To improve security, many systems use two-factor authentication, which requires users to provide two forms of identification. Multi-factor authentication is even more secure, as it combines multiple verification methods, such as passwords, biometrics, or security tokens. Biometric authentication uses unique physical characteristics like fingerprints or facial recognition.

Access control systems help restrict access to sensitive data and ensure that only authorized users can view or modify it. Without proper authentication and

authorization, systems become vulnerable to cyberattacks. That is why organizations invest in strong access control mechanisms to protect their data and networks.

Questions:

1. What is the difference between authentication and authorization?
2. Why are passwords not always secure?
3. What is two-factor authentication?
4. How does biometric authentication work?
5. Why is access control important in network security?

***Exercise 6.**

Part 1. Translate the following sentences from English into Ukrainian. Use the vocabulary provided.

1. Authentication is the process of verifying a user's identity.
2. Authorization determines which resources a user can access.
3. A password is the most common method of authentication.
4. Two-factor authentication requires two forms of identification.
5. Multi-factor authentication provides a higher level of security.
6. Biometric authentication uses fingerprints or facial recognition.
7. Access control helps protect sensitive information from unauthorized users.
8. Organizations use authentication and authorization to improve network security.
9. Strong passwords are important for protecting user accounts.
10. Access control systems restrict access to confidential data.
11. Multi-factor authentication may combine passwords, biometrics, and security tokens.
12. Without proper authentication, systems can become vulnerable to cyberattacks.
13. Biometric authentication is becoming more popular in modern organizations.
14. Authorization is performed after successful authentication.
15. Companies invest in access control mechanisms to protect their networks and data.

Part 2. Translate the following sentences from Ukrainian into English. Use the vocabulary provided.

1. Cybersecurity is the practice of protecting computers, networks, and data from digital attacks.
2. Users should use strong passwords that include letters, numbers, and symbols.
3. Two-factor authentication adds an extra layer of security.
4. Malware includes viruses, worms, and other harmful software.
5. Firewalls control network traffic and block suspicious activity.
6. Encryption protects sensitive data by converting it into a secure format.
7. Antivirus programs help detect and remove malware.
8. Users should avoid clicking on unknown links.

9. Cybersecurity helps prevent data theft and unauthorized access.
10. Cybersecurity awareness reduces the risk of online threats.

Networks and Protocols

IP Address - IP-адреса — унікальний ідентифікатор пристрою
MAC Address - MAC-адреса — фізична адреса пристрою
Network Protocol - Мережевий протокол — правила передачі даних
HTTP - Протокол передачі гіпертексту
HTTPS - Захищений HTTP — із шифруванням
SSL - Протокол захищених сокетів
TLS - Протокол безпеки транспортного рівня
VPN - Віртуальна приватна мережа — захищене з'єднання

Text: Network Protocols and Security Technologies in Cybersecurity

Network protocols are essential for communication between devices on the internet. Protocols like HTTP and HTTPS define how data is transmitted. HTTPS is more secure because it uses encryption to protect information. SSL and TLS are cryptographic protocols that ensure secure communication over networks.

A VPN, or Virtual Private Network, allows users to create a secure connection, especially when using public Wi-Fi. It hides the user's IP address and encrypts internet traffic. Antivirus software is another important tool that helps detect and remove malware. Systems like IDS and IPS monitor network activity and prevent suspicious behavior.

Regular security patches are necessary to fix vulnerabilities in software. Backup systems also play a key role in protecting data by allowing recovery after an attack. By combining these technologies, organizations can build strong network security and protect their information from threats.

Questions:

1. What is the purpose of network protocols?
2. What is the difference between HTTP and HTTPS?
3. How does a VPN improve security?
4. What is the role of antivirus software?
5. Why are security patches and backups important?

***Exercise 7.**

Part 1. Reorder the words to form correct sentences. Use the given vocabulary.

1. is / unique / IP Address / device / an / identifier / a
2. physical / MAC Address / is / device / the / of / address / a
3. rules / Network Protocol / defines / data / transmission / for
4. Hypertext Transfer Protocol / HTTP / stands / for
5. secure / HTTPS / is / HTTP / version / a / of
6. encryption / SSL / uses / secure / communication / for

7. TLS / provides / transport / security / layer
8. VPN / creates / secure / a / connection / virtual
9. hides / IP Address / VPN / user's / the
10. internet traffic / VPN / encrypts
11. between / devices / protocols / communication / enable / network
12. HTTPS / more / than / HTTP / secure / is
13. data / protect / encryption / helps
14. public Wi-Fi / VPN / on / security / improves
15. internet / devices / connect / protocols / allow

Part 2. Put the words in the correct order:

1. protect / Cybersecurity / systems / helps / and / data / networks
2. strong / should / use / passwords / users
3. adds / authentication / security / two-factor / extra / an / layer
4. includes / malware / worms / viruses / and / software / harmful
5. network / firewall / traffic / controls / a
6. sensitive / encryption / protects / data
7. remove / antivirus / malware / helps / programs
8. avoid / users / suspicious / should / files / downloading
9. block / firewalls / activity / suspicious
10. improve / safety / cybersecurity / online / helps

Protect systems

<p>Antivirus Software - Антивірусне ПЗ — виявляє загрози</p> <p>IDS (Intrusion Detection System) - Система виявлення вторгнень</p> <p>IPS (Intrusion Prevention System) - Система запобігання вторгненням</p> <p>Endpoint Security - Захист кінцевих пристроїв</p> <p>Security Patch - Оновлення безпеки — виправлення вразливостей</p> <p>Backup - Резервне копіювання — збереження даних</p>
--

Text: Key Tools and Technologies in Network Security

Network security relies on various tools and technologies to protect systems from cyber threats. One of the most important tools is antivirus software, which detects and removes malware from computers. It helps protect users from viruses, worms, and other harmful programs.

Intrusion Detection Systems (IDS) monitor network traffic and identify suspicious activity. Intrusion Prevention Systems (IPS) go one step further by blocking potential attacks before they can harm the system. Firewalls also play a key role by filtering incoming and outgoing network traffic based on security rules.

Security patches are regularly released to fix vulnerabilities in software and operating systems. Installing these updates is essential to prevent hackers from

exploiting weaknesses. Backup systems are also very important because they allow users to restore lost data after an attack or system failure.

By using a combination of antivirus software, IDS, IPS, firewalls, patches, and backups, organizations can significantly improve their cybersecurity and reduce risks.

Questions:

1. What is the main purpose of antivirus software?
2. What does an Intrusion Detection System (IDS) do?
3. How is an Intrusion Prevention System (IPS) different from IDS?
4. Why are security patches important?
5. How do backup systems help in cybersecurity?

Exercise 8.

Part 1. Find and correct the mistakes in the sentences. Use the correct cybersecurity terms.

1. IDS blocks all incoming attacks before they enter the system.
2. Antivirus software only monitors network traffic but does not remove malware.
3. IPS is used to detect suspicious activity but does not prevent attacks.
4. Endpoint Security protects only the central server of a company.
5. Security patches are optional updates that improve computer speed.
6. Backup systems are used to create viruses for testing purposes.
7. IDS and IPS are not related to network security tools.
8. Antivirus software is useless against worms and Trojans.
9. Security patches are used to introduce new vulnerabilities into systems.
10. Backup systems permanently delete old data instead of saving it.
11. Endpoint Security protects only mobile devices and ignores computers.
12. IPS only detects attacks but does not block them.
13. IDS prevents attacks before they happen.
14. Antivirus software detects and removes malware from systems.
15. Security patches fix vulnerabilities in software and operating systems.

Part 2. Correct mistakes

1. Cybersecurity is the process of creating viruses for testing systems.
2. Strong passwords should only include numbers.
3. Two-factor authentication removes the need for passwords.
4. Malware is a type of hardware used to protect computers.
5. Firewalls increase internet speed by removing encryption.
6. Encryption makes data readable for everyone online.
7. Antivirus programs create viruses to test security systems.
8. Users should click on all links to stay safe online.
9. Cybersecurity has no connection to online safety.
10. Firewalls block suspicious network activity.

Other important definitions

Data Breach	- Витік даних — несанкціонований доступ
Vulnerability	- Вразливість — слабе місце системи
Exploit	- Експлойт — використання вразливості
Risk Assessment	- Оцінка ризиків
Security Policy	- Політика безпеки
Digital Certificate	- Цифровий сертифікат
Public Key	- Відкритий ключ
Private Key	- Приватний ключ
Hashing	- Хешування — перетворення даних у фіксований код
Social Engineering	- Соціальна інженерія — маніпуляції людьми
Cloud Security	- Безпека хмарних сервісів
Endpoint	- Кінцевий пристрій (ПК, смартфон)

Text: Key Concepts and Fundamentals of Network Security

In network security, understanding key concepts helps organizations protect their data effectively. A data breach occurs when unauthorized users gain access to sensitive information. This can lead to financial loss and damage to reputation. A vulnerability is a weakness in a system that can be exploited by attackers, while an exploit is a method used to take advantage of that weakness.

A security policy defines rules and procedures for protecting data and systems within an organization. Risk assessment is the process of identifying and evaluating potential threats. Digital certificates are used to verify the identity of websites and ensure secure communication.

Public and private keys are part of encryption systems. The public key is used to encrypt data, while the private key is used to decrypt it. Hashing transforms data into a fixed-length code to protect its integrity. Social engineering involves manipulating people into revealing confidential information.

Cloud security focuses on protecting data stored in cloud services. An endpoint refers to any device connected to a network, such as a computer or smartphone. Securing endpoints is essential because they are common targets for cyberattacks.

Questions:

1. What is a data breach?
2. What is the difference between a vulnerability and an exploit?
3. Why is a security policy important?
4. How do public and private keys work in encryption?
5. What is social engineering in cybersecurity?

Exercise 9. Multiple Choice. Choose one correct answer (A, B, C or D):

1. What is the main purpose of a firewall?
A) Store files

- B) Filter network traffic
 - C) Create passwords
 - D) Encrypt emails
2. What does encryption do?
 - A) Deletes data
 - B) Converts data into secure form
 - C) Blocks websites
 - D) Speeds up internet
 3. Which attack demands payment to restore access?
 - A) Phishing
 - B) Ransomware
 - C) SQL injection
 - D) Spoofing
 4. What is phishing?
 - A) A backup method
 - B) A type of firewall
 - C) A trick to steal data
 - D) A secure protocol
 5. What is a worm?
 - A) Needs user action to spread
 - B) Spreads automatically
 - C) A hardware device
 - D) A password tool
 6. Which system detects attacks?
 - A) IDS
 - B) VPN
 - C) HTTP
 - D) DNS
 7. Which system blocks attacks automatically?
 - A) IDS
 - B) IPS
 - C) FTP
 - D) SSL
 8. What does HTTPS provide?
 - A) Faster internet
 - B) Encryption and security
 - C) File storage
 - D) Virus scanning
 9. What is a Trojan horse?
 - A) A safe program
 - B) Malware disguised as useful software
 - C) A firewall tool
 - D) A browser

10. What is a DDoS attack?
 - A) Password reset
 - B) Overloading a server
 - C) File encryption
 - D) Data backup
11. What is authorization?
 - A) Checking identity
 - B) Giving access rights
 - C) Encrypting data
 - D) Scanning viruses
12. What is a VPN used for?
 - A) Gaming
 - B) Secure connection
 - C) Virus creation
 - D) File deletion
13. What is spyware?
 - A) Improves speed
 - B) Collects user data secretly
 - C) Deletes malware
 - D) Encrypts files
14. What is a vulnerability?
 - A) Strong protection
 - B) System weakness
 - C) Antivirus tool
 - D) Password type
15. What is social engineering?
 - A) Hardware repair
 - B) Manipulating people
 - C) Data encryption
 - D) Network setup

Exercise 10. True / False

1. A worm needs user action to spread.
2. HTTPS is more secure than HTTP.
3. A virus can spread between computers.
4. Backups help recover lost data.
5. Malware is a general term for harmful software.
6. A firewall allows all traffic by default.
7. Encryption protects data confidentiality.
8. A Trojan horse is always harmless.
9. IDS prevents attacks automatically.
10. VPN hides user IP address.
11. Ransomware steals passwords only.

12. Authentication verifies identity.
13. Authorization gives access rights.
14. Zero-day attacks use unknown vulnerabilities.
15. Antivirus software protects against malware.

Exercise 11. Fill the gaps.

1. Network _____ are essential for communication between devices on the internet.
2. HTTPS is more secure because it uses _____ to protect information.
3. SSL and TLS are cryptographic protocols that ensure secure _____ over networks.
4. A VPN hides the user's IP address and _____ internet traffic.
5. Antivirus software helps detect and remove _____ from computers.
6. IDS systems monitor network traffic and identify _____ activity.
7. IPS systems can block potential _____ before they harm the system.
8. Firewalls filter incoming and outgoing network _____ based on security rules.
9. Security _____ are necessary to fix vulnerabilities in software and operating systems.
10. Backup systems allow users to restore lost _____ after an attack or system failure.

***Exercise 12. Matching. Match terms (1-15) with definitions:**

1. Malware	A) Used to decrypt data
2. Firewall	B) Harmful software
3. Encryption	C) Filters network traffic
4. IDS	D) Detects attacks
5. IPS	E) Prevents attacks
6. VPN	F) Secure connection network
7. Virus	G) Self-spreading malware
8. Worm	H) Malware disguised as useful software
9. Trojan Horse	I) Blocks access to data for payment
10. Ransomware	J) Collects user data secretly
11. Spyware	K) Shows ads
12. Adware	L) Copy of data for recovery
13. Backup	M) Encrypts data
14. Public Key	N) Malware that spreads automatically
15. Private Key	O) Used to encrypt data

***Exercise 13. Translate into English.**

1. Автентифікація та авторизація є важливими частинами мережевої безпеки.
2. Найпоширенішим методом автентифікації є пароль.
3. Двофакторна автентифікація вимагає дві форми підтвердження особи.

4. Багатофакторна автентифікація поєднує кілька методів перевірки.
5. Біометрична автентифікація використовує відбитки пальців або розпізнавання обличчя.
6. Системи контролю доступу допомагають захищати конфіденційні дані.
7. Фішинг є одним із найпоширеніших типів кібератак.
8. DDoS-атака може перевантажити сервер і зробити його недоступним.
9. SQL-ін'єкція використовується для атаки на бази даних.
10. Обізнаність і належний захист допомагають зменшити ризики.

***Exercise 14. Put the words in the correct order:**

1. essential / authentication / network / are / authorization / and / parts / of / security
2. process / authentication / verifying / the / identity / is / of / a / user's
3. secure / always / password / not / a / is
4. systems / many / use / authentication / two-factor / security / to / improve
5. methods / combines / authentication / verification / multi-factor / multiple
6. sensitive / systems / protect / control / access / data
7. users / phishing / attackers / into / trick / try / revealing / information / personal / to
8. unavailable / attack / a / server / DDoS / make / can / a
9. combinations / attacks / password / brute / involve / many / force / trying
10. protection / awareness / reducing / proper / risks / are / key / to

***Exercise 15. Correct the mistakes:**

1. Without authentication and authorization, systems become vulnerable to cyberattacks.
2. Multi-factor authentication combines passwords, biometrics, and security tokens.
3. Firewalls filter incoming and outgoing network traffic.
4. IDS monitors network activity and identifies suspicious behavior.
5. IPS blocks potential attacks before they can damage the system.
6. Security patches fix vulnerabilities in software and operating systems.
7. Backup systems help restore lost data after an attack.
8. Spear phishing targets specific individuals or organizations.
9. A man-in-the-middle attack secretly intercepts communication between users.
10. Organizations use strong security systems to reduce cybersecurity risks.

Exercise 16. Discussion Questions:

1. What is a data breach and why can it be dangerous for organizations?
2. How does a vulnerability differ from an exploit?
3. Why is a security policy important in an organization?
4. What is the purpose of a risk assessment in cybersecurity?
5. How do digital certificates help ensure secure communication?
6. What is the difference between a public key and a private key in encryption?
7. Why is hashing important for data integrity?

8. What is social engineering and why is it effective for attackers?
9. Why are endpoints considered common targets for cyberattacks?
10. What is the difference between a virus, a worm, and a Trojan horse?
11. Why is ransomware considered one of the most dangerous types of malware?
12. How do spyware and adware affect users differently?
13. What steps can users take to protect themselves from malware?
14. Why is it important to avoid suspicious files and unknown links?
15. How does understanding cybersecurity threats help improve online safety?

Exercise 17.

Part 1. Read the texts below. Match choices (A–H) to texts (1–5). There are three choices you do not need to use.

1. _____ When using a computer or smartphone, it is important to install updates regularly. Updates fix security problems and improve system performance. Without them, devices can become vulnerable to cyberattacks. Many hackers exploit old software versions to gain access to systems. That is why users should enable automatic updates whenever possible.

2. _____ Downloading software only from official websites or trusted app stores reduces the risk of installing harmful programs. Many viruses and malware spread through unofficial sources. Some fake websites look very similar to real ones and can deceive users. Always check the source before downloading anything. This helps keep your device safe from hidden threats.

3. _____ Using strong passwords is one of the simplest ways to protect your accounts. A strong password should include letters, numbers, and special characters, and should not be easy to guess. Weak passwords can be cracked by attackers in a short time. It is also important not to use the same password for different accounts. Password managers can help store them securely.

4. _____ Antivirus programs help detect and remove malicious software. They also scan files and warn users about potential threats before they can cause damage. Modern antivirus tools often work in real time to protect systems continuously. However, they should be updated regularly to recognize new viruses. Combining antivirus software with safe behavior increases protection.

5. _____ It is important to avoid clicking on unknown links in emails or messages. Cybercriminals often use fake messages to steal personal information or install malware. These attacks are called phishing and can look very convincing. Users should always check the sender before opening links. Being careful online helps prevent many security problems.

Choices:

- A. Use only trusted sources to download applications.
- B. Turn off your computer when not in use.
- C. Install antivirus software to protect your device.
- D. Regular updates improve security and fix vulnerabilities.
- E. Never use the internet.

- F. Use strong passwords for your accounts.
- G. Avoid suspicious links in emails and messages.
- H. Share your passwords with friends for safety.

***Part 2. Read the texts below. Match choices (A–H) to texts (1–5). There are three choices you do not need to use.**

Texts

1. ____ This method protects data by converting it into a secure format that cannot be read without a special key. It is widely used when sending sensitive information over the internet. Even if hackers intercept the data, they will not be able to understand it. Only authorized users with the correct key can restore the original information. This process is essential for maintaining confidentiality in modern communication systems.

2. ____ This security tool monitors network traffic and blocks suspicious activity before it can harm the system. It acts as a barrier between trusted and untrusted networks. It is commonly used in both home and corporate networks to increase protection. The system follows predefined security rules to decide which data packets are allowed. It helps prevent unauthorized access and cyberattacks.

3. ____ This type of attack tricks users into revealing personal information, such as passwords or bank details, by sending fake messages or emails. These messages often look like they come from trusted organizations. Users may be directed to fake websites designed to steal their data. The attackers rely on human error rather than technical weaknesses. Awareness and caution are key to avoiding this threat.

4. ____ This security method requires users to provide two different forms of identification before accessing an account, making unauthorized access more difficult. Typically, it combines something the user knows, like a password, with something they have, such as a phone. Sometimes biometric data like fingerprints is also used. This approach significantly increases account security. It is widely used in banking and online services.

5. ____ This is harmful software that can damage systems, steal data, or disrupt computer operations. It includes viruses, worms, and Trojan horses. It can spread through email attachments, downloads, or infected websites. Once inside a system, it may run silently without the user noticing. To protect against it, users should install security tools and avoid suspicious files.

Choices:

- A. Firewall
- B. Encryption
- C. Phishing
- D. Two-Factor Authentication (2FA)
- E. Malware
- F. VPN

- G. Authentication
- H. Antivirus Software

Exercise 18. Listening. Listen the text and answer the questions.

Text: Safe Use of Devices and Software

Safe use of devices and software is very important in today's digital world. People use computers, smartphones, and tablets every day, so protecting them from threats is essential. One of the most important rules is to install software updates regularly. Updates fix security problems and help prevent cyberattacks.

It is also important to download programs only from official websites or trusted app stores. Unofficial sources may contain viruses or other types of malware that can damage devices or steal personal data. Users should also install antivirus software, which helps detect and remove harmful programs.

Another key element of safety is using strong passwords. A strong password includes letters, numbers, and symbols, and it should not be easy to guess. It is also recommended not to use the same password for different accounts and to change passwords regularly.

Users should be careful with emails and messages, especially if they contain unknown links. These may be phishing attempts designed to steal personal information. In such cases, it is better not to click on the links and delete the message immediately.

Finally, creating backups of important data is very important. Backups allow users to restore files if they are lost due to a virus or system failure. By following these rules, people can significantly improve the security of their devices and protect their personal information.

Questions:

1. Why is safe use of devices and software important in today's world?
2. What is the purpose of software updates?
3. Where should users download programs from to stay safe?
4. What risks can unofficial software contain?
5. How does antivirus software help protect devices?
6. What makes a password strong and secure?
7. Why should users avoid using the same password for different accounts?
8. What are phishing messages designed to do?
9. What should a user do if they receive a suspicious email or link?
10. Why are backups important for data protection?

Exercise 19. Video Comprehension Task. Watch the video: <https://www.youtube.com/watch?v=VINyUsm0W4w> and choose the correct answer:

1. **What is the main purpose of network security?**
A. To increase the speed of the Internet.

- B. To protect networks and data from unauthorized access and cyber threats.
- C. To create new computer programs.
- D. To improve the design of websites.

2. Which of the following is an example of a network security threat?

- A. Software update
- B. Firewall
- C. Malware attack
- D. Strong password

3. What is the primary function of a firewall?

- A. To create backups of files
- B. To monitor and control incoming and outgoing network traffic
- C. To speed up Internet connections
- D. To remove viruses from a computer

4. Why do organizations use Virtual Private Networks (VPNs)?

- A. To increase computer storage space
- B. To create websites
- C. To encrypt data and provide secure communication over the Internet
- D. To install software updates

5. What is one benefit of implementing network security measures?

- A. Reduced protection of sensitive information
- B. Increased risk of cyberattacks
- C. Better protection of data and network resources
- D. Elimination of all computer problems

***Exercise 20. Discussion Questions. Answer in 2–3 sentences.**

1. Why are firewalls and VPNs important for network security?
2. Why is network security important for businesses and government organizations?

FINAL TEST UNIT 2

1. What is a software update?

- A. Deleting files
- B. Fixing bugs and improving security
- C. Turning off the internet
- D. Creating viruses

2. Why is it important to install updates?

- A. To increase ads
- B. To reduce system speed
- C. To protect the system from threats
- D. To delete programs

3. Where is it safest to download software from?

- A. Any website
- B. Social media
- C. Official app stores or websites
- D. Unknown links

4. What can unofficial software contain?

- A. Photos
- B. Viruses and malware
- C. Only music
- D. System updates

5. What is a strong password?

- A. 123456
- B. Your username
- C. A mix of letters, numbers, and symbols
- D. Your birth date

6. What is NOT recommended for passwords?

- A. Using different passwords
- B. Using strong passwords
- C. Sharing passwords with others
- D. Changing passwords regularly

7. What does antivirus software do?

- A. Deletes the internet
- B. Protects against malicious software
- C. Creates files
- D. Increases Wi-Fi speed

8. What is phishing?

- A. A system update
- B. Password creation
- C. A scam to steal personal data
- D. Antivirus scanning

9. Which is an example of phishing?

- A. Windows update
- B. Fake email from a bank
- C. Antivirus scan
- D. Downloading software

10. What should you do with suspicious links?

- A. Open them
- B. Ignore and delete them
- C. Send them to friends
- D. Download them

11. What is malware?

- A. Antivirus software
- B. A protection program
- C. Software that harms systems
- D. An update

12. Which is an example of malware?

- A. Microsoft Word
- B. Antivirus software
- C. A computer virus
- D. A browser

13. What does a virus do?

- A. Protects data
- B. Works faster
- C. Spreads and damages files
- D. Updates the system

14. Why is a Trojan horse dangerous?

- A. It improves performance
- B. It disguises itself as useful software
- C. It increases memory
- D. It removes ads

15. What is a worm?

- A. A harmless program
- B. Malware that spreads automatically
- C. Antivirus software
- D. A browser

16. What is ransomware?

- A. Learning software
- B. Malware that blocks data and demands payment
- C. A system update
- D. A game

17. What is spyware?

- A. Antivirus software
- B. Gaming software

- C. Software that steals information
- D. System update

18. What does adware do?

- A. Protects the system
- B. Shows unwanted advertisements
- C. Removes viruses
- D. Updates software

19. What is an endpoint?

- A. A server
- B. A device connected to a network
- C. Antivirus software
- D. A password

20. Why should devices be protected?

- A. For gaming only
- B. Because they are not important
- C. Because they can be attacked
- D. To reduce internet usage

21. What is a firewall?

- A. A game
- B. Network protection system
- C. A virus
- D. A browser

22. What does a firewall do?

- A. Deletes files
- B. Filters network traffic
- C. Creates viruses
- D. Changes passwords

23. What is a backup?

- A. A virus
- B. A copy of data
- C. A password
- D. Antivirus software

24. Why are backups important?

- A. For gaming
- B. To restore lost data
- C. To delete files
- D. To reduce memory

25. What is social engineering?

- A. Software update
- B. Manipulating people to reveal information
- C. Antivirus protection
- D. File compression

26. What is a vulnerability?

- A. A strong security feature
- B. A weakness in a system
- C. A backup file
- D. A password

27. What is an exploit?

- A. A system update
- B. A method to use a vulnerability
- C. Antivirus software
- D. A firewall

28. What is cloud security?

- A. Protecting cloud-stored data
- B. Playing online games
- C. Downloading files
- D. Creating passwords

29. Why is endpoint security important?

- A. Because endpoints are not used
- B. Because endpoints are common attack targets
- C. Because endpoints are always safe
- D. Because endpoints are offline

30. What is the best way to stay safe online?

- A. Use weak passwords
- B. Click all links
- C. Use antivirus and safe behavior
- D. Never update software

***Additional tasks**

***Glossary**

Password - A secret code used to access an account

Two-factor authentication (2FA) - Extra security step requiring two types of verification

Update - New version of software that improves security or performance

Security patch - Fix for software vulnerabilities

Vulnerability - Weak point in a system that can be exploited

Antivirus software - Program that detects and removes malware

Malware - Harmful software such as viruses or worms

Phishing - Fraud technique to steal personal data

VPN (Virtual Private Network) - Tool that encrypts internet connection

Backup - Copy of data used for recovery

***Text: General Rules for Safe Use of Devices and Software**

In today's digital world, people use computers, smartphones, and various applications every day. To stay safe, it is important to follow general rules for secure use of devices and software. One of the most important rules is to use strong and

unique passwords for all accounts. Users should also enable two-factor authentication whenever it is available.

Another important rule is to keep software and operating systems updated. Updates often include security patches that fix vulnerabilities and protect devices from cyberattacks. Installing antivirus software is also essential because it helps detect and remove malware.

Users should be careful when downloading programs or files from the internet. It is important to download software only from trusted sources. Clicking on unknown links or opening suspicious email attachments can lead to phishing attacks or malware infections.

Public Wi-Fi networks can be dangerous, so it is better to use a VPN when connecting to them. A VPN encrypts internet traffic and protects personal data. Users should also regularly back up their data to prevent loss in case of system failure or cyberattacks.

By following these simple rules, users can significantly reduce security risks and protect their personal information.

***Questions:**

1. Why is it important to use strong passwords?
2. What is the purpose of two-factor authentication?
3. Why should users keep software updated?
4. What is a security patch?
5. What does antivirus software do?
6. Why should users avoid downloading files from unknown sources?
7. What is phishing?
8. How can public Wi-Fi networks be dangerous?
9. What is the purpose of a VPN?
10. Why are backups important?

***Exercise 1. Multiple choice. Safe Use of Devices and Software**

1. What is the main purpose of using strong passwords?

- A) To make login slower
- B) To protect accounts from unauthorized access
- C) To delete viruses
- D) To improve internet speed

2. What does two-factor authentication add?

- A) A new device
- B) Extra security verification
- C) Faster login
- D) More ads

3. Why should software be updated regularly?

- A) To change design only
- B) To fix security vulnerabilities

- C) To delete files
- D) To reduce storage

4.What is a security patch?

- A) A game update
- B) A fix for software weaknesses
- C) A virus
- D) A password

5.What does antivirus software do?

- A) Creates websites
- B) Detects and removes malware
- C) Speeds up Wi-Fi
- D) Stores files

6.What is phishing?

- A) A type of firewall
- B) A scam to steal personal data
- C) A software update
- D) A backup method

7.Why is downloading from trusted sources important?

- A) It increases speed
- B) It reduces security risks
- C) It adds ads
- D) It deletes updates

8.What does a VPN do?

- A) Deletes viruses
- B) Encrypts internet traffic
- C) Blocks all websites
- D) Increases spam

9.Why are public Wi-Fi networks risky?

- A) They are too fast
- B) They may be unsafe and unprotected
- C) They are always encrypted
- D) They cost money

10.Why are backups important?

- A) To increase speed
- B) To recover lost data
- C) To install apps
- D) To block ads

***Exercise 2. True / False**

1. Strong passwords improve security.
2. Software updates are not important.
3. Antivirus software protects against malware.
4. Phishing is a type of cyberattack.

5. VPN protects internet traffic.
6. Public Wi-Fi is always completely safe.
7. Backups help restore lost data.
8. Security patches fix vulnerabilities.
9. Downloading from unknown sources is safe.
10. Two-factor authentication increases security.

***Exercise 3. Fill in the Blanks:**

1. A _____ protects systems from malware.
2. A _____ is a secret code for login.
3. _____ adds extra login security.
4. _____ is harmful software.
5. A _____ encrypts internet traffic.
6. A _____ is used to restore data.
7. A _____ fixes software vulnerabilities.
8. _____ is a scam to steal data.
9. Users should avoid _____ websites.
10. _____ helps detect viruses.

***Exercise 4. Matching. Match terms (1–10) with definitions (A–J)**

1. Password	A) Extra login verification
2. Antivirus	B) Copy of data for recovery
3. Malware	C) Weak point in a system
4. VPN	D) Secret access code
5. Update	E) Protection tool for networks
6. Phishing	F) Harmful software
7. Backup	G) Fraud to steal data
8. Firewall	H) Security software update
9. Vulnerability	I) Tool for secure connection
10. Two-factor authentication	J) Software that removes malware

***Exercise 5. Read the texts below. Match choices (A–H) to texts (1–5). There are three choices you do not need to use.**

Text

1. ____ To stay safe online, users should always create strong and unique passwords for each account. A password should not be easy to guess and should include different types of characters. It is also recommended to avoid using the same password across multiple platforms. If one account is compromised, others can also be at risk. Good password management is one of the first steps in protecting personal data.

2. ____ Software developers regularly release updates to improve performance and security. These updates often include security patches that fix vulnerabilities in the system. If users do not install updates, their devices may remain exposed to

cyberattacks. Hackers often exploit old software versions to gain access to data. Therefore, keeping systems updated is essential for safety.

3. ____ This type of program is designed to protect devices from harmful software such as viruses and worms. It scans files and applications to detect suspicious activity. When a threat is found, it can remove or isolate it before it causes damage. Many users install it as a basic layer of protection. Without it, systems are more vulnerable to cyberattacks.

4. ____ When using the internet, users should be careful about what they download. Files and applications should only be obtained from trusted sources. Opening unknown email attachments or clicking suspicious links can lead to serious security problems. These actions may result in stolen data or infected devices. Awareness of online threats helps prevent such risks.

5. ____ When connecting to public Wi-Fi networks, users face increased security risks. To protect their data, they should use a special tool that encrypts internet traffic. This tool creates a secure connection even on unsafe networks. It hides the user's activity from hackers and protects personal information. It is especially important when using banking or other sensitive services online.

Choices:

- A. Password
- B. Two-factor authentication (2FA)
- C. Update
- D. Security patch
- E. Antivirus software
- F. Malware
- G. Phishing
- H. VPN (Virtual Private Network)

***Exercise 6. Test. Safe Use of Devices & Programs + Basic Network Safety Rules. Choose the correct answer (A, B, C, or D).**

1. One of the most important security rules is to use _____ passwords.
 - A) simple
 - B) weak
 - C) strong
 - D) short
2. A strong password should include letters, numbers, and _____.
 - A) images
 - B) symbols
 - C) sounds
 - D) videos
3. Two-factor authentication adds an extra layer of _____.
 - A) speed

- B) security
 - C) memory
 - D) storage
4. Users should install software updates to fix _____.
A) games
B) vulnerabilities
C) keyboards
D) screens
5. A security patch is used to fix _____ in software.
A) features
B) vulnerabilities
C) websites
D) users
6. Antivirus software helps protect against _____.
A) malware
B) monitors
C) printers
D) cables
7. Malware includes viruses, worms, and _____ programs.
A) useful
B) harmful
C) fast
D) free
8. Users should download software only from _____ sources.
A) unknown
B) trusted
C) random
D) hidden
9. Opening suspicious email attachments may lead to _____.
A) updates
B) infections
C) backups
D) encryption
10. A backup is used to _____ data.
A) delete
B) recover
C) hide
D) compress
11. A VPN is used to _____ internet traffic.
A) delete
B) encrypt
C) slow
D) open

12. VPN protects users on _____ Wi-Fi networks.
- A) private
 - B) public
 - C) offline
 - D) wired only
13. Public Wi-Fi networks can be _____.
- A) safe
 - B) dangerous
 - C) faster
 - D) encrypted
14. Encryption makes data _____ to unauthorized users.
- A) readable
 - B) invisible
 - C) unreadable
 - D) faster
15. A firewall controls _____ traffic.
- A) network
 - B) sound
 - C) video
 - D) file
16. Firewalls block _____ activity.
- A) suspicious
 - B) normal
 - C) fast
 - D) offline
17. Users should avoid clicking _____ links.
- A) unknown
 - B) official
 - C) safe
 - D) updated
18. Phishing attacks try to steal _____.
- A) hardware
 - B) personal data
 - C) screens
 - D) cables
19. Safe network behavior reduces the risk of _____.
- A) cyberattacks
 - B) printing
 - C) typing
 - D) storage
20. Cybersecurity includes protecting both devices and _____.
- A) networks
 - B) keyboards

- C) monitors
 - D) cables
21. Keeping software updated improves _____.
A) risk
B) security
C) delay
D) attack
22. Antivirus programs should be updated _____.
A) rarely
B) regularly
C) never
D) manually only
23. Strong security depends on technology and _____ behavior.
A) risky
B) safe
C) random
D) slow
24. Backup systems help recover data after a _____.
A) success
B) failure
C) login
D) update
25. Encryption protects data during _____.
A) storage only
B) transmission
C) deletion
D) printing
26. A secure system reduces the risk of _____ access.
A) authorized
B) unauthorized
C) fast
D) local
27. Cybersecurity awareness helps users avoid _____.
A) threats
B) keyboards
C) monitors
D) cables
28. Installing unknown software can introduce _____.
A) security
B) malware
C) updates
D) backups

29. A secure password should NOT be _____.
A) complex
B) unique
C) reused
D) strong
30. Network security protects information from _____.
A) threats
B) printers
C) screens
D) keyboards



Unit 3

Collecting and analysing data methods in computer networks

Text 1. Research into Methods of Data Collection and Network Traffic Analysis in Cybersecurity

Text 2. Collecting and Analysing Data Methods in Computer Networks

Text 3. Active Information Gathering in Computer Networks

Text 4. Traffic Analysis in Computer Networks

Glossary

Data collection - збір даних

The process of gathering information from systems and networks - процес збору інформації із систем і мереж

Network traffic - мережевий трафік

Data moving across a computer network - дані, що передаються комп'ютерною мережею

Log file - файл журналу (лог-файл)

A record of system or user activities - запис дій системи або користувача

Log analysis - аналіз журналів (логів)

Examining logs to detect problems or attacks - перевірка логів для виявлення проблем або атак

Packet - пакет даних

A small unit of data transmitted over a network - невелика одиниця даних, що передається мережею

Packet capture - перехоплення пакетів

Collecting network packets for analysis - збір мережевих пакетів для аналізу

Packet sniffer - аналізатор пакетів (сніфер)

Tool that monitors and captures network traffic - інструмент для моніторингу та перехоплення мережевого трафіку

Network traffic analysis - аналіз мережевого трафіку

Studying data flow to detect anomalies - дослідження потоку даних для виявлення аномалій

Anomaly - аномалія

Unusual or suspicious behavior in a system - незвична або підозріла поведінка в системі

Intrusion Detection System (IDS) - система виявлення вторгнень

System that detects suspicious activity - система, що виявляє підозрілу активність

Intrusion Prevention System (IPS) - система запобігання вторгненням

System that blocks detected attacks - система, що блокує виявлені атаки
Machine learning - машинне навчання
Technology that learns patterns from data - технологія, що навчається на основі даних і виявляє закономірності
Real-time monitoring - моніторинг у реальному часі
Continuous observation of system activity - безперервне спостереження за активністю системи
Cyber threat - кіберзагроза
Any potential danger to digital systems - будь-яка потенційна небезпека для цифрових систем
Security analyst - аналітик з кібербезпеки
Specialist who investigates cybersecurity incidents - спеціаліст, який розслідує інциденти кібербезпеки

Text

Research into Methods of Data Collection and Network Traffic Analysis in Cybersecurity

Cybersecurity research often focuses on how data is collected and how network traffic is analyzed to detect threats. Organizations collect different types of data from computer networks, including logs, packet information, and user activity records. This data helps security specialists understand what is happening inside a system.

One common method of data collection is log analysis. Logs record events such as user logins, file access, and system errors. By analyzing logs, experts can identify unusual behavior that may indicate a cyberattack. Another important method is packet capture, where network packets are collected and examined in detail. Tools like packet sniffers allow analysts to inspect data traveling across a network.

Network traffic analysis is used to monitor communication between devices. It helps detect anomalies such as unusual data transfers, unauthorized access attempts, or malware activity. Security teams often use Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to automate this process.

Machine learning is also increasingly used in cybersecurity research. It helps detect patterns in large amounts of network data and identify potential threats faster than manual analysis. Combined with real-time monitoring, these methods improve the ability to respond to cyberattacks quickly.

Overall, data collection and network traffic analysis are essential for understanding threats, improving security systems, and protecting digital infrastructure.

Questions:

1. What is data collection in cybersecurity?
2. What information do log files contain?
3. What is log analysis used for?
4. What is a network packet?

5. What is packet capture?
6. What does a packet sniffer do?
7. What is network traffic analysis?
8. What is an anomaly in a network?
9. How do IDS and IPS help in cybersecurity?
10. Why is machine learning useful in cybersecurity?

Exercise 1. Multiple Choice

1. What is data collection in cybersecurity?
 - A) Deleting files
 - B) Gathering information from systems
 - C) Creating viruses
 - D) Blocking internet
2. What is network traffic?
 - A) Computer games
 - B) Data moving across a network
 - C) Antivirus software
 - D) Passwords
3. What is a log file?
 - A) A game file
 - B) A record of system events
 - C) A virus
 - D) A browser
4. What is log analysis used for?
 - A) Entertainment
 - B) Detecting attacks and issues
 - C) Increasing speed
 - D) Gaming
5. What is a packet?
 - A) A type of virus
 - B) A small unit of data
 - C) A firewall
 - D) A password
6. What does packet capture do?
 - A) Deletes packets
 - B) Collects network data
 - C) Creates websites
 - D) Blocks users
7. What is a packet sniffer?
 - A) Antivirus tool
 - B) Tool for monitoring network traffic
 - C) Password manager
 - D) VPN

8. What is an anomaly?
 - A) Normal behavior
 - B) Suspicious behavior
 - C) Software update
 - D) Backup
9. What is IDS used for?
 - A) Playing games
 - B) Detecting attacks
 - C) Deleting files
 - D) Creating passwords
10. Why is machine learning used in cybersecurity?
 - A) For entertainment
 - B) To detect patterns in data
 - C) To slow systems
 - D) To store photos

Exercise 2. True / False

1. Data collection helps analyze cyber threats.
2. Log files contain user and system activity.
3. Network traffic is unrelated to cybersecurity.
4. Packet capture collects network data.
5. A packet sniffer analyzes network traffic.
6. An anomaly means normal behavior.
7. IDS detects suspicious activity.
8. IPS blocks cyberattacks.
9. Machine learning helps analyze large data sets.
10. Network traffic analysis is useless in cybersecurity.

Exercise 3. Fill in the Blanks

1. _____ is the process of gathering data from systems.
2. _____ records system events and user actions.
3. _____ is data moving across a network.
4. A _____ is a small unit of data.
5. _____ analysis examines logs for threats.
6. _____ captures network packets.
7. A _____ monitors network traffic.
8. An _____ is suspicious behavior.
9. _____ detects cyberattacks automatically.
10. _____ helps find patterns in large data sets.

Glossary:

Computer network - Комп'ютерна мережа

Data analysis - Аналіз даних

Passive information gathering - Пасивний збір інформації
Active information gathering - Активний збір інформації
Network monitoring - Моніторинг мережі
Traffic analysis - Аналіз трафіку
Encryption - Шифрування
Decryption - Розшифрування
IP address - IP-адреса
MAC address - MAC-адреса
Session - Сесія
Session hijacking - Перехоплення сесії
Vulnerability - Вразливість
Unauthorized access - Несанкціонований доступ

Text: Collecting and Analysing Data Methods in Computer Networks

Collecting and analysing data in computer networks is a key part of modern cybersecurity. Organizations rely on these methods to understand network behaviour and to detect possible threats. One of the most widely used approaches is passive information gathering, which involves collecting data without directly interacting with the target system. This method is less risky because it does not change the network environment and is therefore harder to detect.

In passive analysis, security specialists often monitor network traffic and study data packets as they move through the system. Each packet contains important information such as IP addresses, which help identify devices, and other communication details. Traffic analysis is used to examine these packets and discover patterns of normal or suspicious activity. Packet sniffing tools can also be used to capture and analyse network traffic, and Wireshark is one of the most common examples.

Although passive methods are useful, they may not always provide enough detailed information. For deeper investigation, analysts may use active information gathering, which involves direct interaction with the network or system. This can include scanning ports, testing services, and identifying vulnerabilities. However, active methods are more easily detected by security systems.

Intrusion Detection Systems (IDS) play an important role in monitoring such activities. An IDS observes network traffic and alerts administrators when suspicious behaviour is detected. To protect sensitive information during analysis, encryption is used to secure data, while decryption allows authorized users to access the original content.

Network security also depends on proper identification of devices. IP addresses and MAC addresses help distinguish different devices in a network. In addition, network sessions represent active connections between users and servers. One serious threat in this area is session hijacking, where attackers attempt to take control of an active session to gain unauthorized access.

Firewalls support network security by controlling traffic and blocking suspicious connections. They work together with monitoring tools to reduce risks and protect systems. Cybersecurity professionals often combine both passive and active methods to achieve more accurate results. However, all data collection must follow ethical and legal rules to avoid unauthorized access.

Continuous monitoring and analysis help organizations identify vulnerabilities before attackers can exploit them. By using these techniques responsibly, companies can significantly improve their overall cybersecurity and protect sensitive information from threats.

Questions to the Text

1. What is passive information gathering?
2. Why is passive information gathering considered less risky?
3. What is the purpose of network monitoring?
4. What does traffic analysis examine?
5. What information can be found in data packets?
6. What is packet sniffing used for?
7. Name one tool used for packet sniffing.
8. How is active information gathering different from passive?
9. Give examples of active information gathering methods.
10. What can Intrusion Detection Systems detect?
11. What does an IDS do when it finds suspicious activity?
12. Why is encryption important in data analysis?
13. What is decryption used for?
14. What do IP addresses identify?
15. What do MAC addresses represent?
16. What is a network session?
17. What is session hijacking?
18. Why is session hijacking dangerous?
19. How do firewalls help in network security?
20. Why is continuous monitoring important in cybersecurity?

Exercise 4. Matching. Match terms (31–40) with definitions (A–J)

1. Data collection	A) Detects suspicious activity
2. Log file	B) Collects system information
3. Packet	C) Small unit of data
4. Packet capture	D) Records system events
5. Packet sniffer	E) Blocks attacks
6. Network traffic analysis	F) Studies data flow in a network
7. Anomaly	G) Unusual behavior
8. IDS	H) Tool for capturing data
9. IPS	I) Technology that learns from data
10. Machine learning	J) Tool for monitoring traffic

***Exercise 5. Translate into English**

1. Дослідження з кібербезпеки часто зосереджуються на зборі даних та аналізі мережевого трафіку.
2. Організації збирають різні типи даних із комп'ютерних мереж.
3. Логи записують події, такі як вхід користувача в систему та помилки системи.
4. Аналіз логів допомагає виявити незвичну поведінку в системі.
5. Перехоплення пакетів дозволяє спеціалістам детально досліджувати мережеві пакети.
6. Аналізатори пакетів контролюють дані, що передаються мережею.
7. Аналіз мережевого трафіку допомагає виявляти несанкціоновані спроби доступу.
8. Системи IDS та IPS автоматизують процес виявлення атак.
9. Машинне навчання допомагає знаходити закономірності у великих обсягах даних.
10. Моніторинг у реальному часі покращує здатність швидко реагувати на кібератаки.

***Exercise 6. Put the words in the correct order**

1. often / focuses / cybersecurity research / on / data collection
2. collect / organizations / different types / of data / from computer networks
3. helps / this data / security specialists / understand / a system
4. analysis / common method / log / is / one / of data collection
5. logs / events / record / such as / user logins
6. experts / unusual behavior / can identify / by analyzing logs
7. packet sniffers / analysts / inspect / allow / data / to
8. network traffic analysis / to monitor / is used / communication between devices
9. machine learning / patterns / helps detect / in network data
10. real-time monitoring / improves / the ability / to respond / quickly / to cyberattacks

***Exercise 7. Correct mistakes**

1. Cybersecurity research often focus on how data are collected.
2. Organizations collects different types of data from computer network.
3. This data help security specialists understands what is happening inside a system.
4. One common method of data collection are log analysis.
5. Logs records events such as user logins and system errors.
6. Experts can identifies unusual behavior by analyze logs.
7. Packet sniffers allows analysts inspect data traveling across a network.
8. Network traffic analysis are used to monitor communication between devices.
9. Machine learning help detect patterns in large amounts of network data.
10. These methods improves the ability to respond to cyberattacks quickly.

Exercise 8. Discussion questions

1. Why is data collection important in cybersecurity research?
2. What types of data do organizations collect from computer networks?
3. How does log analysis help security specialists detect cyber threats?
4. What information can be found in log files?
5. Why is packet capture useful for network analysis?
6. How do packet sniffers help analysts inspect network traffic?
7. What kinds of anomalies can network traffic analysis detect?
8. How do IDS and IPS systems improve cybersecurity protection?
9. Why is machine learning becoming more important in cybersecurity research?
10. How does real-time monitoring help organizations respond to cyberattacks?

Glossary

Active information gathering - Активний збір інформації
Network scanning - Сканування мережі
Port scanning - Сканування портів
Vulnerability - Вразливість
Exploitation - Експлуатація вразливості
Network reconnaissance - Розвідка мережі
Penetration testing - Тестування на проникнення
Attack surface - Поверхня атаки
Unauthorized access - Несанкціонований доступ
Intrusion Detection System (IDS) - Система виявлення вторгнень
Intrusion Prevention System (IPS) - Система запобігання вторгненням
Service detection - Виявлення сервісів
Host discovery - Виявлення хостів
Brute force attack - Атака перебором
Authentication - Аутентифікація
Security assessment - Оцінка безпеки

Text: Active Information Gathering in Computer Networks

Active information gathering is a key technique in cybersecurity used to collect detailed information about computer networks through direct interaction with the target system. Unlike passive methods, it generates network activity and can therefore be detected by security tools. This approach is commonly used in network reconnaissance and penetration testing to identify potential weaknesses in systems.

One of the main techniques in active information gathering is network scanning. Security specialists use scanning tools to discover active devices, services, and open ports within a network. Port scanning is especially important because it helps identify which ports are open on a system and which services are running on them. Open ports may indicate possible vulnerabilities that could be exploited if they are not properly secured.

Another important technique is host discovery, which is used to determine which devices are currently active in a network. After identifying active hosts, analysts can study the network structure in more detail. This process helps create a map of the network, including devices, connections, and services. Network reconnaissance builds a clearer picture of the system and its potential attack surface.

Active information gathering is widely used in penetration testing, which is a controlled and authorized attempt to evaluate system security. During penetration testing, security professionals simulate real attacks to find vulnerabilities before cybercriminals can exploit them. A vulnerability is a weakness in a system that may allow unauthorized access or damage if discovered by attackers.

Security tools such as Intrusion Detection Systems (IDS) and firewalls play an important role during active scanning. IDS systems monitor network activity and can detect unusual or suspicious scanning behaviour. Firewalls may block or limit scanning attempts to protect the system from potential threats. Because active scanning generates visible traffic, it is usually easy for security systems to identify.

Attackers may also use active information gathering techniques for malicious purposes. For example, they may perform brute force attacks to guess passwords or test system authentication. However, strong authentication mechanisms and security monitoring tools can help prevent such attacks.

Although active information gathering is a powerful method for improving cybersecurity, it must always be used ethically and legally. Unauthorized scanning or testing of systems is illegal in many countries. Therefore, organizations only allow active security testing with proper permission and strict rules. When used correctly, active information gathering helps reduce risks and strengthens overall network security.

Questions to the Text

1. What is active information gathering in cybersecurity?
2. How is active information gathering different from passive methods?
3. What is the purpose of network scanning?
4. What does port scanning help to identify?
5. Why are open ports considered important in security analysis?
6. What is host discovery used for?
7. What does network reconnaissance help to map?
8. Why can IDS easily detect active scanning activities?
9. What is the role of a firewall in active scanning?
10. What is penetration testing?
11. Why do security experts perform penetration testing?
12. What is a vulnerability?
13. What is the attack surface of a network?
14. What type of attack is brute force?
15. Why must active information gathering be used ethically and legally?

Exercise 9. Read the texts below. Match choices (A–H) to texts (1–5). There are three choices you do not need to use.

1. _____ Cybersecurity specialists often use log analysis to investigate suspicious activity in computer systems. Log files contain information about user actions, file access, and system events. By studying these records, analysts can detect unusual behavior and possible cyberattacks.
2. _____ Packet capture is an important method of collecting data in computer networks. During this process, network packets are captured and examined in detail. Security experts use packet sniffers to monitor data moving across a network and identify potential threats.
3. _____ Network traffic analysis helps organizations monitor communication between devices. Analysts look for anomalies such as unauthorized access attempts, malware activity, or unusual data transfers. This method improves the detection of security incidents.
4. _____ Machine learning technologies are becoming more common in cybersecurity research. These systems can process large amounts of network data and recognize suspicious patterns automatically. This helps security teams respond to threats faster than with manual analysis alone.
5. _____ Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are widely used to protect networks. IDS detects suspicious activities, while IPS can automatically block attacks. Combined with real-time monitoring, these systems improve network security.

Choices

- A. The role of artificial intelligence in detecting cyber threats
- B. Methods of monitoring communication in networks
- C. Advantages of cloud storage systems
- D. The use of log files in cybersecurity investigations
- E. Automatic systems for detecting and preventing attacks
- F. The history of the Internet
- G. Packet capture and packet sniffing tools
- H. Social media security problems

Exercise 10. Reading Task: Passive vs Active Information Gathering

Read the texts below. Match choices (A–H) to texts (1–5). There are three choices you do not need to use.

Text

1. ____ This method of information gathering does not involve direct interaction with the target system. Analysts collect data from publicly available sources such as websites, public databases, and network logs. Because it does not generate network

traffic, it is usually difficult to detect. It is considered a safer approach for early-stage cybersecurity analysis.

2. ____ This technique involves actively interacting with a target system to collect detailed technical information. It may include scanning networks, identifying open ports, and discovering running services. Unlike passive methods, it generates visible network traffic and can be detected by security systems.

3. ____ This method is often used to map the structure of a network by identifying active devices and their connections. It requires sending requests to systems and analyzing their responses. Security professionals use it to find vulnerabilities before attackers can exploit them.

4. ____ This approach relies on observing network traffic without sending any requests to the target system. Analysts may use public information and monitoring tools to study user behaviour and system patterns. It is commonly used in intelligence gathering and early reconnaissance.

5. ____ This technique is more aggressive and may involve port scanning, service detection, and vulnerability assessment. It can trigger alerts in security systems such as IDS and firewalls. It is widely used in penetration testing to evaluate system security.

Options

- A. Passive information gathering
- B. Active information gathering
- C. Encryption
- D. Firewall
- E. Malware
- F. VPN
- G. Authentication
- H. Traffic analysis

Exercise 11. Listen to the dialogue and answer the questions.

Dialogue

Teacher: Today we are going to discuss passive and active information gathering. Do you know the difference between them?

Cadet: I think both methods are used to collect information about a target, but I am not sure how they differ.

Teacher: That's correct. Passive information gathering means collecting information without directly interacting with the target system. For example, security specialists may use search engines, social media platforms, public websites, or WHOIS databases.

Cadet: So, the target does not know that someone is gathering information?

Teacher: Exactly. Passive methods usually leave no trace and are difficult to detect.

Cadet: What about active information gathering?

Teacher: Active information gathering involves direct interaction with the target. Security professionals may use tools such as Nmap to scan networks, identify open ports, or discover running services.

Cadet: Does that mean the target can detect such activity?

Teacher: Yes. Active reconnaissance generates network traffic, and security systems may identify the scanning attempts.

Cadet: Which method is better?

Teacher: Both methods are important. Passive information gathering is safer and helps collect basic information. Active information gathering provides more detailed technical information. Cybersecurity professionals often combine both approaches during security assessments and penetration testing.

Cadet: I understand. Passive reconnaissance is less risky, while active reconnaissance provides more accurate information.

Teacher: Exactly. Using both methods responsibly helps organizations identify vulnerabilities and improve security.

Answer the Questions

1. What is passive information gathering?
2. Name two sources used in passive information gathering.
3. Why is passive information gathering difficult to detect?
4. What is active information gathering?
5. Which tool is mentioned in the dialogue?
6. What information can active reconnaissance reveal?
7. Why can active information gathering be detected?
8. Which method is considered safer?
9. Why do cybersecurity professionals use both methods?
10. What is the goal of information gathering in cybersecurity?

***Exercise 12. True or False**

1. Passive information gathering directly interacts with the target system.
2. WHOIS databases can be used for passive reconnaissance.
3. Active information gathering may generate network traffic.
4. Nmap is used for network scanning.
5. Passive information gathering provides more technical details than active information gathering.
6. Security systems can detect active reconnaissance.
7. Cybersecurity professionals use only active information gathering.
8. Both methods are useful during penetration testing.

Text: Traffic Analysis in Computer Networks

Traffic analysis in computer networks is an important technique used in cybersecurity to monitor and understand how data moves through a system. It involves examining network traffic to detect patterns, performance issues, and

potential security threats. Organizations use traffic analysis to ensure that their networks operate efficiently and securely.

Network traffic consists of small units of data called packets. Each packet contains information such as source and destination IP addresses, as well as data related to communication between devices. By inspecting these packets, security specialists can understand how information flows across the network.

One of the main goals of traffic analysis is network monitoring. Continuous monitoring helps detect unusual behaviour that may indicate a cyberattack. For example, a sudden increase in traffic may suggest a distributed denial-of-service (DDoS) attack. Security systems can respond quickly to such events and reduce potential damage.

Packet capture is another important technique used in traffic analysis. It allows analysts to collect data packets for deeper inspection. Tools like Wireshark are commonly used for this purpose. After capturing packets, analysts perform packet inspection to understand the content and structure of network communication.

Traffic analysis also helps with anomaly detection. An anomaly is any activity that does not match normal network behaviour. These anomalies may indicate malware infections, unauthorized access, or system misconfigurations. Intrusion Detection Systems (IDS) are often used to automatically detect such suspicious activities.

Performance monitoring is another key aspect of traffic analysis. Analysts study bandwidth, latency, and throughput to ensure that the network is functioning properly. High latency or low throughput may indicate technical problems or overloaded systems.

Encryption plays an important role in modern networks. While encrypted traffic protects user data, it can also make analysis more difficult. In such cases, analysts focus on metadata rather than content. Decryption is only performed when authorized and necessary for security investigations.

Firewalls also support traffic analysis by filtering incoming and outgoing data. They help block suspicious connections and reduce the risk of cyberattacks. By combining monitoring tools, IDS systems, and firewalls, organizations can improve their overall network security.

Effective traffic analysis allows cybersecurity professionals to detect threats early and respond quickly. It is an essential part of maintaining a safe and reliable computer network environment.

Questions to the Text

1. What is traffic analysis in computer networks?
2. What are network packets?
3. What information is contained in a packet?
4. What is the main goal of network monitoring?
5. What can a sudden increase in traffic indicate?
6. What is packet capture used for?

7. Name one tool used for packet capture.
8. What is packet inspection?
9. What is anomaly detection in traffic analysis?
10. What types of problems can anomalies indicate?
11. How do IDS systems help in traffic analysis?
12. What network performance metrics are analyzed?
13. Why can encryption make traffic analysis more difficult?
14. What is the role of firewalls in traffic analysis?
15. Why is traffic analysis important for cybersecurity?

***Exercise 13. Write T (True) or F (False).**

1. Traffic analysis is used to monitor how data moves through a network. ____
2. Network packets do not contain any useful information. ____
3. Network monitoring helps detect unusual behaviour. ____
4. A sudden decrease in traffic may indicate a DDoS attack. ____
5. Packet capture allows analysts to collect data packets. ____
6. Wireshark is used for packet inspection and capture. ____
7. An anomaly is normal network behaviour. ____
8. IDS systems help detect suspicious activity automatically. ____
9. Bandwidth, latency, and throughput are performance metrics. ____
10. Encryption makes traffic analysis easier. ____

***Exercise 14. Fill in the Gaps. Use the words from the box:**

(packets, traffic analysis, anomaly, IDS, encryption, packet capture, monitoring, bandwidth, firewall, latency)

1. _____ is used to examine network traffic and detect patterns.
2. Network _____ consists of small units of data.
3. _____ helps detect unusual activity in a network.
4. An _____ is any activity that differs from normal behaviour.
5. _____ is used to collect data packets for analysis.
6. _____ systems automatically detect suspicious activity.
7. _____ protects data but can make analysis more difficult.
8. High _____ may indicate network performance problems.
9. A _____ blocks suspicious network connections.
10. Network _____ is important for detecting cyberattacks.

***Exercise 15. Match the Words with Their Definitions. Match (1–10) with (A–J).**

Words:	Definitions:
1. Packet	A. A system that blocks or filters network traffic
2. Traffic analysis	B. A unit of data transmitted across a network
3. Packet capture	C. The process of examining network traffic
4. Anomaly	D. The time delay in data transmission

5. IDS	E. A tool that detects suspicious activity
6. Firewall	F. A method of collecting network data for analysis
7. Bandwidth	G. A system used to observe network activity
8. Latency	H. The amount of data that can be transmitted
9. Encryption	I. A security method that protects data by encoding it
10. Network monitoring	J. Any activity that does not match normal behaviour

Exercise 16. Translate the following sentences into English using the vocabulary from the text "Traffic Analysis in Computer Networks".

1. Аналіз трафіку допомагає виявляти потенційні загрози безпеці в комп'ютерних мережах.
2. Мережевий трафік складається з невеликих одиниць даних, які називаються пакетами.
3. Кожен пакет містить IP-адреси джерела та призначення.
4. Безперервний моніторинг мережі допомагає виявляти незвичну поведінку.
5. Раптове збільшення трафіку може свідчити про DDoS-атаку.
6. Захоплення пакетів дозволяє аналітикам збирати дані для детальнішого аналізу.
7. Системи виявлення вторгнень автоматично визначають підозрілу активність у мережі.
8. Аналіз трафіку допомагає виявляти шкідливе програмне забезпечення та несанкціонований доступ.
9. Брандмауери фільтрують вхідний і вихідний трафік та блокують підозрілі з'єднання.
10. Ефективний аналіз трафіку дозволяє фахівцям з кібербезпеки швидко реагувати на загрози.

Exercise 17. Match the terms (1–10) with their definitions (A–J).

Terms

1. Traffic Analysis
2. Packet
3. Network Monitoring
4. Packet Capture
5. Packet Inspection
6. Anomaly Detection
7. Intrusion Detection System (IDS)
8. Firewall
9. Encryption
10. Throughput

Definitions

- A. A security system that monitors network activity and identifies suspicious behaviour.
- B. The process of converting data into a secure format to protect it from unauthorized access.
- C. A small unit of data transmitted across a network.
- D. The process of collecting and examining network traffic to identify patterns, problems, and threats.
- E. The amount of data successfully transmitted through a network during a specific period of time.
- F. A technique used to collect network packets for detailed analysis.
- G. A process of examining the content and structure of captured packets.
- H. A security device that filters incoming and outgoing network traffic according to predefined rules.
- I. The continuous observation of network activity to ensure proper operation and detect unusual behaviour.
- J. The process of identifying activities that differ from normal network behaviour.

Exercise 18. Video: Network Traffic Analysis with Wireshark. Watch the video: <https://www.youtube.com/watch?v=nS8KweAV1g0> and choose the correct answer:

Vocabulary from the Video:

- **Network Traffic Analysis** – аналіз мережевого трафіку
- **Packet Capture** – захоплення пакетів
- **Packet Inspection** – інспекція пакетів
- **Wireshark** – Wireshark (аналізатор мережевого трафіку)
- **Network Monitoring** – моніторинг мережі
- **Suspicious Activity** – підозріла активність
- **Malware** – шкідливе програмне забезпечення
- **Cyber Threat** – кіберзагроза
- **Intrusion Detection** – виявлення вторгнень
- **Network Communication** – мережеве з'єднання / комунікація мережі

Part A. Multiple Choice:

1. What is the main purpose of network traffic analysis?

- A. To create websites
- B. To monitor and analyze network communications
- C. To increase Internet speed
- D. To develop mobile applications

2. Which tool is primarily used in the video for traffic analysis?

- A. Metasploit
- B. Nmap

- C. Wireshark
- D. Burp Suite

3. What does packet capture allow analysts to do?

- A. Delete suspicious files
- B. Collect and examine network packets
- C. Encrypt all network traffic
- D. Create user accounts

4. Why is traffic analysis important in cybersecurity?

- A. It helps design computer hardware.
- B. It helps identify suspicious network activity and security threats.
- C. It improves graphic design.
- D. It replaces antivirus software.

5. What information can analysts obtain from captured packets?

- A. Only file names
- B. Only passwords
- C. Details about network communication and transmitted data
- D. Only IP addresses

Part B. Answer the Questions

- 6. What is a packet in a computer network?
- 7. How does Wireshark help cybersecurity professionals?
- 8. What suspicious activities can traffic analysis reveal?
- 9. Why is packet inspection important?
- 10. How can traffic analysis improve network security?

FINAL TEST UNIT 3

1. What is the main purpose of data collection in cybersecurity?

- A. To create computer games
- B. To detect threats and monitor systems
- C. To increase Internet speed
- D. To design websites

2. What does network traffic mean?

- A. Cars on the road
- B. Emails only
- C. Data moving across a network
- D. Computer passwords

3. Which file records system and user activities?

- A. Media file
- B. Audio file
- C. Log file
- D. Image file

4. What is log analysis used for?

- A. Creating databases
- B. Detecting problems and attacks
- C. Printing documents
- D. Installing software

5. What is a packet?

- A. A type of virus
- B. A small unit of transmitted data
- C. A security password
- D. A computer monitor

6. What is packet capture?

- A. Deleting network data
- B. Encrypting passwords
- C. Collecting packets for analysis
- D. Restarting servers

7. Which tool monitors network traffic?

- A. Packet sniffer
- B. Text editor
- C. Web browser
- D. Media player

8. What can network traffic analysis detect?

- A. Music files
- B. Anomalies and malware activity
- C. Printer errors only
- D. Video quality

9. What is an anomaly in cybersecurity?

- A. Normal system behavior
- B. Unusual or suspicious activity
- C. A type of hardware
- D. A network cable

10. What does IDS stand for?

- A. Internet Data Service
- B. Intrusion Detection System
- C. Internal Data Server
- D. Integrated Device System

11. What is the function of an IDS?

- A. To play multimedia files
- B. To detect suspicious activity
- C. To create websites
- D. To repair hardware

12. What does IPS stand for?

- A. Intrusion Prevention System
- B. Internet Protection Software
- C. Internal Packet Service
- D. Integrated Prevention Server

13. What does an IPS do?

- A. Blocks detected attacks
- B. Creates log files
- C. Increases memory size
- D. Controls printers

14. Which technology can learn patterns from data?

- A. Bluetooth
- B. Machine learning
- C. Video streaming
- D. Cloud printing

15. What is real-time monitoring?

- A. Monitoring once a month
- B. Continuous observation of activity
- C. Manual file copying
- D. Offline communication

16. What is a cyber threat?

- A. A type of software update
- B. A potential danger to digital systems
- C. A computer game
- D. A database program

17. Who investigates cybersecurity incidents?

- A. Security analyst
- B. Web designer

- C. Accountant
- D. Photographer

18. What information can logs contain?

- A. User logins and system errors
- B. Music playlists
- C. Weather forecasts
- D. Video recordings only

19. Why is packet capture important?

- A. It improves screen brightness
- B. It allows detailed packet analysis
- C. It creates presentations
- D. It changes passwords automatically

20. What do packet sniffers inspect?

- A. Network traffic
- B. Computer keyboards
- C. Printed documents
- D. USB devices

21. Which activity may indicate a cyberattack?

- A. Unusual behavior in logs
- B. Listening to music
- C. Watching videos
- D. Using a calculator

22. What helps monitor communication between devices?

- A. Network traffic analysis
- B. Photo editing software
- C. Antivirus installation only
- D. Word processing

23. Which systems automate attack detection?

- A. GPS systems
- B. IDS and IPS
- C. Video players
- D. Office applications

24. What can machine learning identify?

- A. Food recipes
- B. Suspicious patterns in data
- C. Printer models
- D. Battery size

25. Why is machine learning useful in cybersecurity?

- A. It detects threats faster
- B. It reduces monitor size
- C. It changes operating systems
- D. It creates games

26. What improves quick response to cyberattacks?

- A. Real-time monitoring
- B. Social media
- C. Video editing
- D. Graphic design

27. What is malware activity?

- A. Suspicious software behavior
- B. A network cable problem
- C. A printer installation
- D. A monitor update

28. Why is data analysis important?

- A. It helps understand threats
- B. It creates websites
- C. It replaces hardware
- D. It deletes logs

29. What do organizations collect from networks?

- A. Packet information and logs
- B. Printed books
- C. Camera lenses
- D. Sound systems

30. What is the overall goal of network security research?

- A. Protecting digital infrastructure
- B. Selling computers
- C. Playing online games
- D. Watching movies



Unit 4

Modern information systems and networks protection

Text 1. Modern Information Systems and Networks Protection

Text 2. Cloud Computing Security

Text 3. Security of Information Systems and Networks

Text 4. Security in Wireless Networks

Text 5. Security in Operating Systems

Text: Malware (Malicious Software)

Glossary:

Information system - Інформаційна система

Antivirus software - Антивірусне програмне забезпечення

IDS (Intrusion Detection System) - Система виявлення вторгнень

Encryption - Шифрування

VPN (Virtual Private Network) - Віртуальна приватна мережа

Access control - Контроль доступу

Multi-factor authentication (MFA) - Багатофакторна аутентифікація

Patch management - Управління оновленнями (патчами)

Network monitoring - Моніторинг мережі

Traffic analysis - Аналіз трафіку

Malware - Шкідливе ПЗ

Data protection - Захист даних

Unauthorized access - Несанкціонований доступ

Read the text and answer for the questions

Text: Modern Information Systems and Networks Protection

Modern information systems and networks protection is a critical part of cybersecurity. As organizations rely more on digital technologies, protecting data, systems, and network infrastructure becomes increasingly important.

Information systems include computers, servers, databases, and software applications that store and process data. Networks connect these systems and allow communication between devices. However, this connectivity also creates risks, as attackers can exploit vulnerabilities to gain unauthorized access.

One of the key elements of protection is the use of security technologies such as firewalls, antivirus software, and intrusion detection systems (IDS). Firewalls filter incoming and outgoing traffic, while antivirus programs detect and remove malicious software. IDS monitors network activity and alerts administrators about suspicious behavior.

Encryption is another essential method of protection. It ensures that data is unreadable to unauthorized users during transmission. Virtual Private Networks (VPNs) also provide secure communication channels, especially when using public networks.

Access control is used to limit who can access systems and data. Strong passwords, multi-factor authentication (MFA), and user permissions help prevent unauthorized access.

Regular updates and patch management are also important. Software vulnerabilities are often exploited by attackers, so keeping systems updated reduces security risks.

Finally, network monitoring and traffic analysis help detect anomalies and potential threats in real time. Combined with proper security policies and user awareness, these measures provide comprehensive protection for modern information systems and networks.

Questions

1. What is the purpose of modern information systems protection?
2. What are information systems?
3. Why do networks create security risks?
4. What does a firewall do?
5. What is the role of antivirus software?
6. What does an IDS detect?
7. Why is encryption important?
8. What is the function of a VPN?
9. What is access control?
10. How does MFA improve security?
11. What is a vulnerability?
12. Why is patch management important?
13. What is network monitoring?
14. What is traffic analysis used for?
15. How can organizations improve cybersecurity?

Exercise 1. Multiple Choice

1. What is cybersecurity?
 - A) Gaming
 - B) Protection of systems and data
 - C) Social media
 - D) Music
2. Information systems include:
 - A) Only phones
 - B) Computers, servers, databases
 - C) Only websites
 - D) Only emails

3. Firewall is used to:
 - A) Store data
 - B) Filter network traffic
 - C) Delete files
 - D) Create passwords
4. Antivirus software:
 - A) Speeds internet
 - B) Detects malware
 - C) Creates networks
 - D) Deletes logs
5. IDS is used to:
 - A) Detect suspicious activity
 - B) Block all users
 - C) Play games
 - D) Backup data
6. Encryption:
 - A) Deletes data
 - B) Protects data
 - C) Sends emails
 - D) Blocks users
7. VPN provides:
 - A) Fast gaming
 - B) Secure connection
 - C) File storage
 - D) Password reset
8. Access control limits:
 - A) Speed
 - B) User access
 - C) Internet
 - D) Hardware
9. MFA adds:
 - A) Extra security
 - B) Speed
 - C) Memory
 - D) Storage
10. Patch management:
 - A) Deletes systems
 - B) Updates software
 - C) Creates malware
 - D) Blocks traffic

Exercise 2. True / False

1. Networks have no risks

2. Firewalls filter traffic
3. Antivirus detects malware
4. Encryption protects data
5. VPN is insecure
6. MFA improves security
7. Vulnerabilities are strengths
8. Updates reduce risks
9. Monitoring helps detect threats
10. Traffic analysis is useless

Exercise 3. Fill in the Blanks

1. Cybersecurity protects _____ and data.
2. A _____ filters network traffic.
3. Antivirus detects _____.
4. _____ protects data using coding.
5. VPN creates a secure _____.
6. Access control limits _____ access.
7. MFA means _____ authentication.
8. A vulnerability is a _____.
9. _____ management updates systems.
10. Traffic _____ detects anomalies.

Exercise 4. Find the mistake in the sentence and correct it

1. HTTPS does not protect data.
2. Session hijacking is a safe process.
3. Firewall creates viruses.
4. Cookies store hardware components.
5. Malware improves system performance.
6. IDS blocks all attacks automatically.
7. VPN makes connection less secure.
8. Encryption deletes data permanently.
9. Packet sniffers destroy network traffic.
10. MFA reduces security.

Glossary

Cloud computing - Хмарні обчислення

Cloud security - Безпека хмарних обчислень

Data protection - Захист даних

Multi-factor authentication (MFA) - Багатофакторна аутентифікація

IaaS - Інфраструктура як послуга

PaaS - Платформа як послуга

SaaS - Програмне забезпечення як послуга

Cloud provider - Хмарний провайдер

Shared responsibility - Спільна відповідальність
Misconfiguration - Неправильна конфігурація
IDS - Система виявлення вторгнень
IPS - Система запобігання вторгненням
Logging - Журналювання
Monitoring - Моніторинг
Unauthorized access - Несанкціонований доступ

Read the text and answer for the questions

Text: Cloud Computing Security

Cloud computing security is an essential part of modern cybersecurity. Cloud services allow users and organizations to store data, run applications, and access resources over the Internet instead of using local servers.

There are different types of cloud services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). While cloud computing offers flexibility and scalability, it also introduces security risks.

One of the main concerns is data protection. Sensitive information stored in the cloud can be targeted by attackers. If proper security measures are not in place, unauthorized users may gain access to confidential data.

Encryption is a key method for protecting data in the cloud. It ensures that data remains secure both during transmission and while stored. Access control mechanisms, such as strong passwords and multi-factor authentication (MFA), help ensure that only authorized users can access cloud resources.

Another important aspect is shared responsibility. Cloud providers are responsible for securing the infrastructure, while users are responsible for securing their data, applications, and access settings.

Regular monitoring and logging are important for detecting suspicious activity. Security tools such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) are also used in cloud environments.

Misconfiguration is one of the most common cloud security issues. Incorrect settings can expose data to the public. Therefore, proper configuration and regular audits are essential.

In conclusion, cloud computing security requires a combination of encryption, access control, monitoring, and proper configuration to protect data and systems.

Questions

1. What is cloud computing?
2. What are the main types of cloud services?
3. Why is cloud security important?
4. What is data protection?
5. How does encryption protect data?
6. What is access control?
7. What is MFA?

8. What is shared responsibility in the cloud?
9. What are cloud providers responsible for?
10. What are users responsible for?
11. What is misconfiguration?
12. Why is monitoring important?
13. What is logging?
14. What tools are used for cloud security?
15. What risks exist in cloud computing?

***Exercise 5. Match the English terms (1–18) with their Ukrainian equivalents (A–R)**

1	Information system	A. Вразливість
2	Network	B. Моніторинг мережі
3	Cybersecurity	C. Мережа
4	Firewall	D. Аналіз трафіку
5	Antivirus software	E. Шкідливе ПЗ
6	IDS (Intrusion Detection System)	F. Захист даних
7	Encryption	G. Контроль доступу
8	VPN (Virtual Private Network)	H. Кібербезпека
9	Access control	I. Система виявлення вторгнень
10	Authentication	J. Інформаційна система
11	Multi-factor authentication (MFA)	K. Антивірусне програмне забезпечення
12	Vulnerability	L. Віртуальна приватна мережа
13	Patch management	M. Управління оновленнями (патчами)
14	Network monitoring	N. Аутентифікація
15	Traffic analysis	O. Багатофакторна аутентифікація
16	Malware	P. Несанкціонований доступ
17	Data protection	Q. Шифрування
18	Unauthorized access	R. Мережевий екран

***Exercise 6. Read the texts below. Match choices (A–H) to texts (1–5). There are three choices you do not need to use.**

Texts

1. ____ This security technology filters incoming and outgoing network traffic. It helps block unauthorized connections and protects systems from external threats. A firewall can be configured according to an organization's security policies. It is one of the most important components of network security. Many companies use both hardware and software firewalls for better protection.

2. ____ This method converts information into a coded form so that only authorized users can read it. It is widely used to protect data during transmission over networks. Encryption helps prevent cybercriminals from stealing sensitive

information. It is commonly used in online banking, e-commerce, and secure communication systems. Strong encryption significantly improves data protection.

3. ____ Organizations use this process to ensure that software is regularly updated. It helps fix vulnerabilities and reduces the risk of cyberattacks. Security patches are released by software vendors to address known weaknesses. Without regular updates, systems become more vulnerable to attackers. Effective patch management is an essential part of cybersecurity.

4. ____ This security measure requires users to verify their identity using two or more methods, such as a password and a code sent to a mobile device. It provides a higher level of security than a password alone. Even if a password is stolen, unauthorized users may still be unable to access the system. Many online services and organizations now require this protection method. It is considered a best practice for securing accounts.

5. ____ This activity involves observing network performance and detecting suspicious behavior in real time. It helps administrators identify potential threats quickly. Monitoring tools collect information about network traffic and system activities. Unusual patterns may indicate cyberattacks or technical problems. Continuous monitoring improves the overall security and reliability of information systems.

Choices

- A. Firewall
- B. Network monitoring
- C. Malware
- D. Encryption
- E. Multi-factor authentication (MFA)
- F. Patch management
- G. VPN (Virtual Private Network)
- H. Data protection

*Exercise 7. Put the words in the correct order to make sentences.

1. information / store / systems / and / process / data
2. connect / networks / devices / different / and / systems
3. unauthorized / firewall / access / helps / prevent / a
4. software / malicious / detects / antivirus / and / removes
5. network / monitors / activity / an / IDS
6. encryption / protects / during / transmission / data
7. secure / VPNs / communication / provide / channels
8. access / control / limits / users / authorized / to
9. authentication / improves / security / multi-factor
10. vulnerabilities / reduce / management / patch / helps
11. monitoring / network / detect / threats / helps
12. traffic / administrators / analysis / identify / anomalies / helps

- 13.cybersecurity / protects / systems / networks / and
- 14.attackers / exploit / vulnerabilities / can
- 15.data / protection / organizations / for / essential / is

Exercise 8. Read the text below. For questions (1-10) choose the correct answer (A, B, C or D).

MODERN CYBERSECURITY

Today, organizations rely heavily on digital technologies and information systems. As a result, (1) _____ has become one of the most important areas of information technology. Companies need to protect their networks, systems, and data from cyber threats.

A computer (2) _____ connects devices and allows them to communicate with each other. However, attackers may try to exploit system vulnerabilities and gain unauthorized access. To reduce risks, organizations use various security tools.

One of the most common security technologies is a (3) _____, which filters incoming and outgoing traffic. Another important tool is (4) _____, which detects and removes malicious software from computers and servers.

Many organizations also use an IDS, a system designed to detect suspicious network activity and alert administrators about possible attacks. In addition, (5) _____ helps convert information into a secure code that unauthorized users cannot read.

When employees work remotely, a (6) _____ provides a secure connection to company resources through public networks. This technology helps protect sensitive information during transmission.

Another important aspect of cybersecurity is (7) _____, which limits access to systems and data. To improve security even further, companies often implement MFA, requiring users to verify their identity through multiple methods.

Regular software updates and (8) _____ help fix known weaknesses before attackers can exploit them. Organizations also perform network monitoring and traffic analysis to identify threats in real time.

Without proper security measures, valuable information may be stolen, damaged, or lost. Therefore, effective (9) _____ is essential for modern organizations. These practices help prevent cyber incidents and ensure the safety of digital resources and (10) _____.

	A	B	C	D
1	Cybersecurity	Malware	Network	Vulnerability
2	Firewall	Database	Network	Encryption
3	Firewall	VPN	Authentication	Traffic analysis

4	Antivirus software	Access control	Network monitoring	Patch management
5	Encryption	Malware	Authentication	Monitoring
6	VPN	Firewall	Vulnerability	IDS
7	Access control	Malware	Traffic analysis	Encryption
8	Patch management	Network	VPN	Data protection
9	Data protection	Malware	Vulnerability	Traffic
10	Networks	Passwords	Viruses	Updates

Exercise 9. TEST: Modern Information Systems and Cybersecurity Vocabulary.
Choose the correct answer (A, B, C or D).

1. What is an information system?

- A. A type of virus
- B. A set of tools for data storage and processing
- C. A hacking method
- D. A password system

2. A network is used to:

- A. Delete data
- B. Connect devices
- C. Encrypt files only
- D. Block users

3. Cybersecurity means:

- A. Buying computers
- B. Protecting systems and data
- C. Creating websites
- D. Installing games

4. A firewall is used to:

- A. Increase speed
- B. Filter network traffic
- C. Delete viruses only
- D. Store passwords

5. Antivirus software:

- A. Detects and removes malware
- B. Creates networks
- C. Encrypts passwords
- D. Monitors users

6. IDS stands for:

- A. Internet Data System
- B. Internal Device Service
- C. Intrusion Detection System
- D. Information Data Security

7. Encryption is used to:

- A. Break systems
- B. Code information securely
- C. Delete files
- D. Monitor traffic

8. VPN provides:

- A. Faster games
- B. Secure connection over networks
- C. Free internet
- D. Password storage

9. Access control means:

- A. Blocking internet
- B. Limiting system access
- C. Increasing traffic
- D. Deleting accounts

10. Authentication is:

- A. System update
- B. Identity verification
- C. Malware removal
- D. Data backup

11. MFA means:

- A. One password login
- B. Multi-factor authentication
- C. Malware filtering application
- D. Main firewall access

12. A vulnerability is:

- A. System strength
- B. Weakness in a system
- C. Antivirus tool
- D. Encryption method

13. Patch management is:

- A. Game installation
- B. Software updating process
- C. Network creation
- D. Data deletion

14. Network monitoring is used to:

- A. Play games
- B. Observe network activity
- C. Delete users
- D. Encrypt files

15. Traffic analysis helps to:

- A. Print documents
- B. Identify network patterns
- C. Increase storage
- D. Create passwords

16. Malware is:

- A. Security tool
- B. Harmful software
- C. Network device
- D. Encryption method

17. Data protection ensures:

- A. Data loss
- B. Safety of information
- C. Faster internet
- D. Open access

18. Unauthorized access means:

- A. Allowed entry
- B. Legal login
- C. Illegal system access
- D. System update

19. Information systems include:

- A. Only smartphones
- B. Computers and software
- C. Only internet cables
- D. Only passwords

20. A network connects:

- A. Only files

- B. Devices and systems
- C. Only users
- D. Only apps

Read the text and answer the questions

Text: Security of Information Systems and Networks

Security of information systems and networks is a fundamental aspect of modern cybersecurity. As organizations depend on digital infrastructure, protecting systems, data, and communications becomes essential.

Information systems include hardware, software, databases, and applications that store and process information. Networks connect these systems and enable communication, but they also introduce security risks. Attackers can exploit vulnerabilities to gain unauthorized access, steal data, or disrupt services.

To protect systems and networks, organizations use multiple security measures. Firewalls filter incoming and outgoing traffic, preventing unauthorized connections. Antivirus software detects and removes malware such as viruses, worms, and ransomware. Intrusion Detection Systems (IDS) monitor network activity and alert administrators about suspicious behavior, while Intrusion Prevention Systems (IPS) can block threats automatically.

Encryption is used to protect data during transmission, ensuring that only authorized users can read it. Virtual Private Networks (VPNs) provide secure communication channels, especially when users access systems remotely.

Access control is another important component. It ensures that only authorized users can access specific resources. Techniques such as strong passwords and multi-factor authentication (MFA) significantly improve security.

Regular updates and patch management are essential for fixing vulnerabilities. Network monitoring and traffic analysis help detect anomalies, such as unusual traffic patterns or unauthorized data transfers.

Overall, a combination of technologies, policies, and user awareness is required to ensure the security of information systems and networks.

Questions

1. What is the purpose of security in information systems?
2. What do information systems include?
3. Why do networks create security risks?
4. What does a firewall do?
5. What is the role of antivirus software?
6. What is IDS used for?
7. What is the difference between IDS and IPS?
8. Why is encryption important?
9. What does a VPN provide?
10. What is access control?

11. How does MFA improve security?
12. What is a vulnerability?
13. Why is patch management important?
14. What is network monitoring?
15. What does traffic analysis help detect?

Exercise 10. Multiple Choice

1. Cybersecurity protects:
 - A) Games
 - B) Systems and data
 - C) Music
 - D) Photos
2. Firewall:
 - A) Stores files
 - B) Filters traffic
 - C) Deletes users
 - D) Creates apps
3. Antivirus detects:
 - A) Hardware
 - B) Malware
 - C) Emails
 - D) Logs
4. IDS:
 - A) Blocks everything
 - B) Detects threats
 - C) Encrypts data
 - D) Creates passwords
5. IPS:
 - A) Only detects
 - B) Detects and blocks
 - C) Deletes files
 - D) Stores data
6. Encryption:
 - A) Deletes data
 - B) Protects data
 - C) Sends emails
 - D) Speeds internet
7. VPN provides:
 - A) Storage
 - B) Secure connection
 - C) Games
 - D) Music

8. Access control limits:
 - A) Speed
 - B) User access
 - C) Files
 - D) Internet
9. Vulnerability is:
 - A) Strength
 - B) Weakness
 - C) Tool
 - D) System
10. Traffic analysis detects:
 - A) Photos
 - B) Anomalies
 - C) Music
 - D) Games

***Exercise 11. True / False**

1. Networks are always safe
2. Firewalls filter traffic
3. Antivirus removes malware
4. Encryption protects data
5. VPN is insecure
6. MFA improves security
7. Vulnerabilities are useful
8. Updates reduce risks
9. Monitoring detects threats
10. Traffic analysis is useless

***Exercise 12. Fill in the Blanks**

Part A	Part B
1. Cybersecurity protects _____ and data.	1. Malware is _____ software.
2. A _____ filters traffic.	2. A virus spreads through _____.
3. Antivirus detects _____.	3. A worm spreads _____.
4. _____ protects data during transmission.	4. Trojan looks _____ but is harmful.
5. VPN creates a secure _____.	5. Ransomware _____ files.
6. Access control limits _____ access.	6. Spyware _____ user data.
7. MFA means _____ authentication.	7. Adware shows _____.
8. A vulnerability is a _____.	8. Phishing _____ users.
9. _____ management updates systems.	9. Antivirus _____ malware.
	10. Firewall filters _____.

10. Traffic _____ detects anomalies.	
--------------------------------------	--

*Exercise 13. Matching

Part A:

1. Firewall	A) Detects threats
2. Antivirus	B) Blocks threats
3. IDS	C) Filters traffic
4. IPS	D) Protects data
5. Encryption	E) Secure connection
6. VPN	F) Extra security layer
7. MFA	G) Weakness
8. Vulnerability	H) Detects anomalies
9. Traffic analysis	I) Observes network
10. Network monitoring	J) Removes malware

Part B:

1. Virus	A) Harmful software
2. Worm	B) Collects data
3. Trojan	C) Shows ads
4. Ransomware	D) Encrypts files
5. Spyware	E) Filters traffic
6. Adware	F) Detects threats
7. Antivirus	G) Tricks users
8. Firewall	H) Spreads automatically
9. Phishing	I) Spreads via files
10. Malware	J) Fake program

Glossary

Wireless network (Wi-Fi) - Безпроводна мережа (Wi-Fi)

WPA2 / WPA3 - Протоколи безпеки Wi-Fi

Unauthorized access - Несанкціонований доступ

SSID - Ім'я мережі

MAC address - MAC-адреса

MAC filtering - Фільтрація MAC-адрес

Router - Маршрутизатор

Firmware - Вбудоване програмне забезпечення

Public Wi-Fi - Публічний Wi-Fi

MITM attack (Man-in-the-Middle) - Атака «людина посередині»

VPN - Віртуальна приватна мережа

Data interception - Перехоплення даних

Read the text and answer the questions

Text: Security in Wireless Networks

Wireless network security is an important part of modern cybersecurity. Wireless networks (Wi-Fi) are widely used in homes, offices, and public places because they provide convenient and flexible access to the Internet. However, they are more vulnerable to attacks than wired networks because signals can be intercepted over the air.

One of the main risks in wireless networks is unauthorized access. Attackers can connect to unsecured Wi-Fi networks and gain access to sensitive data. Weak passwords and outdated encryption protocols make this risk even higher.

To protect wireless networks, strong encryption methods such as WPA2 and WPA3 are used. These protocols ensure that data transmitted over the network is secure. Using strong and complex passwords is also essential to prevent unauthorized access.

Another important measure is disabling SSID broadcasting or changing the default network name. This makes the network less visible to potential attackers. Additionally, MAC address filtering can be used to allow only specific devices to connect to the network.

Public Wi-Fi networks are especially dangerous because they are often not secure. Attackers can perform man-in-the-middle (MITM) attacks to intercept data. Using a VPN helps protect data when connecting to public networks.

Regular monitoring of network activity and updating router firmware are also important steps. These measures help detect suspicious behavior and fix security vulnerabilities.

In conclusion, wireless network security requires a combination of encryption, access control, monitoring, and user awareness.

Questions

1. Why are wireless networks more vulnerable than wired networks?
2. What is unauthorized access?
3. How can weak passwords affect security?
4. What are WPA2 and WPA3 used for?
5. Why is encryption important in Wi-Fi networks?
6. What is SSID?
7. How does MAC filtering improve security?
8. Why is public Wi-Fi dangerous?
9. What is a MITM attack?
10. How does a VPN protect users?
11. Why is firmware updating important?
12. What is network monitoring?
13. How can users improve wireless security?
14. What is data interception?
15. Why is user awareness important?

*Exercise 14. Multiple Choice

Part A:

1. Wireless networks use:
 - A) Cables only
 - B) Radio signals
 - C) USB
 - D) Files
2. Main risk of Wi-Fi:
 - A) Speed
 - B) Unauthorized access
 - C) Storage
 - D) Hardware
3. WPA3 is used for:
 - A) Gaming
 - B) Encryption
 - C) Storage
 - D) Printing
4. Weak password:
 - A) Improves security
 - B) Reduces security
 - C) Has no effect
 - D) Blocks users
5. SSID is:
 - A) Password
 - B) Network name
 - C) Virus
 - D) File
6. MAC filtering:
 - A) Blocks all traffic
 - B) Allows specific devices
 - C) Deletes data
 - D) Encrypts files
7. Public Wi-Fi is:
 - A) Always safe
 - B) Often insecure
 - C) Fast only
 - D) Private
8. MITM attack:
 - A) Improves security
 - B) Intercepts communication
 - C) Deletes files
 - D) Updates system
9. VPN provides:
 - A) Games

Part B:

1. Malware is:
 - A) Safe software
 - B) Harmful software
 - C) Update
 - D) Backup
2. Virus spreads:
 - A) Automatically without user
 - B) Through infected files
 - C) Only by internet
 - D) Never
3. Worm:
 - A) Needs user action
 - B) Spreads automatically
 - C) Is safe
 - D) Is antivirus
4. Trojan horse:
 - A) Is safe
 - B) Looks legitimate but harmful
 - C) Deletes system
 - D) Updates OS
5. Ransomware:
 - A) Speeds system
 - B) Encrypts files
 - C) Deletes apps
 - D) Blocks internet
6. Spyware:
 - A) Shows ads
 - B) Collects data
 - C) Deletes files
 - D) Updates system
7. Adware:
 - A) Protects system
 - B) Shows ads
 - C) Encrypts data
 - D) Removes malware
8. Phishing:
 - A) Protects users
 - B) Tricks users
 - C) Deletes files
 - D) Updates OS
9. Antivirus:
 - A) Creates malware

B) Secure connection C) Storage D) Music 10. Firmware update: A) Adds risks B) Fixes vulnerabilities C) Deletes network D) Blocks users	B) Detects malware C) Deletes users D) Blocks internet 10. Firewall: A) Filters traffic B) Stores data C) Encrypts files D) Deletes apps
--	---

***Exercise 15. True / False**

Part A: 1. Wi-Fi is always secure 2. Encryption protects data 3. WPA3 is a security protocol 4. Weak passwords are safe 5. Public Wi-Fi is risky 6. VPN protects data 7. SSID is a virus 8. MAC filtering controls access 9. Firmware updates improve security 10. MITM attacks intercept data	Part B: 1. Malware is safe 2. Virus spreads through files 3. Worm needs user action 4. Trojan is always safe 5. Ransomware encrypts data 6. Spyware collects information 7. Adware shows ads 8. Phishing is safe 9. Antivirus detects malware 10. Firewall filters traffic
---	---

Glossary

Operating system (OS) - Операційна система

User account - Обліковий запис користувача

Permission - Дозвіл

Patch / Update - Оновлення (патч)

Worm - Черв'як

Ransomware - Програма-вимагач

Antivirus software - Антивірусне ПЗ

Disk encryption - Шифрування диска

Unauthorized access - Несанкціонований доступ

System monitoring - Моніторинг системи

Read the text and answer the questions.

Text: Security in Operating Systems

Security in operating systems is a key part of cybersecurity because operating systems (OS) manage hardware, software, and user access. Popular operating systems such as Windows, Linux, and macOS are widely used, which makes them common targets for cyberattacks.

An operating system controls processes, memory, files, and devices. If the OS is not secure, attackers can exploit vulnerabilities to gain unauthorized access, install malware, or take full control of the system.

One of the main security mechanisms in operating systems is access control. It ensures that only authorized users can access files and resources. User accounts, passwords, and permissions help protect sensitive data.

Another important feature is system updates and patch management. Developers regularly release updates to fix vulnerabilities and improve security. If users do not install updates, their systems become easy targets for attackers.

Antivirus software and built-in security tools help detect and remove malware such as viruses, worms, and ransomware. Firewalls in operating systems monitor and control network traffic.

Encryption is used to protect data stored on the system and during transmission. Disk encryption ensures that even if a device is stolen, the data remains protected.

User awareness also plays a critical role. Unsafe actions such as downloading unknown files or clicking suspicious links can compromise system security.

In conclusion, operating system security requires a combination of technical protection, regular updates, and responsible user behavior.

Questions

1. Why is operating system security important?
2. What does an operating system manage?
3. Why are operating systems common targets for attackers?
4. What is access control?
5. How do user accounts help security?
6. What is a vulnerability?
7. Why are updates important?
8. What does antivirus software do?
9. How does a firewall protect the system?
10. What is encryption used for?
11. What is disk encryption?
12. How can users reduce security risks?
13. What is unauthorized access?
14. Why is monitoring important?
15. What happens if systems are not updated?

***Exercise 15. Translate the following sentences into English using the vocabulary from the text “Cloud Computing Security”.**

1. Хмарні обчислення дозволяють користувачам зберігати дані та запускати програми через Інтернет.
2. Існують різні типи хмарних сервісів, такі як IaaS, PaaS і SaaS.

3. Хмарні технології забезпечують гнучкість і масштабованість, але також створюють ризики безпеки.
4. Захист даних є однією з головних проблем у хмарних обчисленнях.
5. Шифрування використовується для захисту даних у хмарі під час передачі та зберігання.
6. Механізми контролю доступу гарантують, що лише авторизовані користувачі можуть отримати доступ до ресурсів.
7. Багатофакторна автентифікація підвищує рівень безпеки облікових записів.
8. Постачальники хмарних послуг відповідають за безпеку інфраструктури.
9. Користувачі відповідають за захист своїх даних і налаштувань доступу.
10. Неправильна конфігурація може призвести до витоку даних.

Exercise 16. Match the English Terms (1–18) with Ukrainian Equivalents (A–R)
Match the terms related to “Malware (Malicious Software)” with their Ukrainian translations.

Terms (English)	Equivalents (Ukrainian)
1. Malware	A. троянська програма
2. Virus	B. мережа
3. Worm	C. фішинг
4. Trojan horse	D. шкідливе програмне забезпечення
5. Ransomware	E. оновлення системи
6. Spyware	F. мережевий черв'як
7. Adware	G. антивірусне програмне забезпечення
8. Phishing	H. кібербезпека / міжмережевий екран (фаєрвол)
9. Antivirus software	I. файл
10. Firewall	J. програма-вимагач
11. File	K. шпигунське програмне забезпечення
12. Network	L. вірус
13. System update	M. несанкціонований доступ
14. Security vulnerability	N. вкладення електронної пошти
15. Unauthorized access	O. шкідливий вебсайт
16. Email attachment	P. рекламне програмне забезпечення
17. Malicious website	Q. поведінка користувача
18. User behavior	R. вразливість безпеки

Exercise 17. Read the text below.

Part A. For questions (1–10) choose the correct answer (A, B, C or D).

Adware - Рекламне ПЗ

Phishing - Фішинг

Attachment - Вкладення

Malicious website - Шкідливий вебсайт

Malware (Malicious Software)

Malware is one of the most dangerous threats in cybersecurity. It is designed to damage systems, steal data, or gain unauthorized access to computers and networks.

There are different types of malware. A virus attaches itself to files and spreads when the file is opened. A worm spreads automatically through networks without user action. A Trojan horse looks like a legitimate program but secretly performs harmful actions.

Ransomware is a type of malware that encrypts files and demands payment to restore access. Spyware secretly collects user information, while adware displays unwanted advertisements and may track user behavior.

Malware often enters systems through email attachments, malicious websites, or infected software. One of the most common methods of attack is (1) _____, where attackers trick users into revealing personal information or downloading harmful files.

To protect systems, organizations use (2) _____, which detects and removes malicious software. A (3) _____ helps block suspicious network connections and unauthorized access.

Regular (4) _____ are important because they fix security vulnerabilities in software. Without them, systems become easier targets for attackers.

Another important defense mechanism is (5) _____, which filters network traffic and blocks harmful connections based on security rules.

To detect suspicious behavior inside a network, companies use (6) _____, which monitors activity and alerts administrators about potential threats.

When malware infects a system, it may cause (7) _____, meaning attackers can access the system without permission.

In some cases, attackers use (8) _____, a method that tries many password combinations until the correct one is found.

Modern cybersecurity also relies on (9) _____, which ensures that data is unreadable to unauthorized users even if it is intercepted.

Finally, strong (10) _____ such as updates, firewalls, and user awareness help reduce the risk of cyberattacks.

No.	A	B	C	D
1	Phishing	Encryption	Firewall	Database
2	Antivirus software	VPN	Traffic analysis	Malware
3	Firewall	Password	Adware	Network

No.	A	B	C	D
4	System updates	Virus attacks	Emails	Users
5	Firewall	Spyware	Encryption	Ransomware
6	IDS	VPN	Malware	Phishing
7	Unauthorized access	Backup	Encryption	Firewall
8	Brute force attack	Phishing	Trojan horse	Adware
9	Encryption	Firewall	Antivirus	Network
10	Security measures	Passwords	Malware types	Databases

Part B. Answer for the questions:

1. What is malware?
2. What is the purpose of malware?
3. How does a virus spread?
4. What is the difference between a worm and a virus?
5. What is a Trojan horse?
6. What does ransomware do?
7. What is spyware used for?
8. What does adware do?
9. How does malware enter a system?
10. What is phishing?
11. How does antivirus software help?
12. What is the role of a firewall?
13. Why are updates important?
14. How can users avoid malware?
15. What is unauthorized access?

Exercise 18. Listening.

Part A: Listen to the text and fill in the gaps with the missing words.

Word Bank:

firewalls, encryption, vulnerabilities, monitoring, antivirus, networks, access control, VPN, IDS, cybersecurity

Modern information systems and network protection are essential parts of (1) _____. Organizations use computers, servers, databases, and software applications to process and store information.

(2) _____ connect devices and allow communication between systems. However, attackers may exploit security (3) _____ to gain unauthorized access to data.

To improve security, organizations use technologies such as (4) _____, which filter incoming and outgoing traffic. Another important tool is (5) _____ software, which detects and removes malicious programs.

An (6) _____ monitors network activity and alerts administrators about suspicious behavior. Data protection is also supported by (7) _____, which converts information into a secure format.

A (8) _____ creates a secure communication channel when users access systems remotely. Organizations also implement (9) _____ to ensure that only authorized users can access specific resources.

Finally, network (10) _____ helps identify threats and unusual activity in real time.

Part B: Listen to the dialogue and choose the correct answer (A, B, or C).

Dialogue

Instructor: Why is protecting information systems important?

Cadet: Because organizations store large amounts of sensitive information in digital systems.

Instructor: Correct. What technologies are commonly used to protect networks?

Cadet: Firewalls, antivirus software, encryption, and intrusion detection systems.

Instructor: What does a firewall do?

Cadet: It filters network traffic and blocks unauthorized connections.

Instructor: Why is encryption important?

Cadet: It protects data by making it unreadable to unauthorized users.

Instructor: How can organizations reduce security risks?

Cadet: By installing updates, monitoring networks, using strong authentication methods, and training users.

Questions

1. Why is information systems protection important?
 - A. To improve Internet speed
 - B. To protect sensitive information
 - C. To create websites
2. Which technology filters network traffic?
 - A. Firewall
 - B. VPN
 - C. Database
3. What is the purpose of encryption?
 - A. To increase storage space
 - B. To create backups
 - C. To protect data
4. Which system detects suspicious network activity?
 - A. IDS
 - B. Browser

- C. Operating system
- 5. How can organizations reduce security risks?
 - A. By ignoring updates
 - B. By using security measures and training users
 - C. By disabling passwords

Exercise 19. Watch the video: https://glasp.co/youtube/NIRXtMg-0z8?utm_source **and choose the correct answer:**

Vocabulary from the Video:

Information System – інформаційна система
Network Security – мережева безпека
Cyber Threat – кіберзагроза
Firewall – міжмережевий екран (фаєрвол)
Vulnerability – вразливість
Encryption – шифрування
Access Control – контроль доступу
Intrusion Detection System (IDS) – система виявлення вторгнень
Unauthorized Access – несанкціонований доступ
Cyberattack – кібератака

Part A. Multiple Choice

Choose the correct answer (A, B, C, or D).

1. Why is network security important?

- A. To improve website design
- B. To protect networks from cyber threats
- C. To increase computer speed
- D. To reduce Internet costs

2. What is one of the main goals of network security?

- A. To create mobile applications
- B. To store more data
- C. To protect information and resources
- D. To replace operating systems

3. Which security technology filters network traffic?

- A. VPN
- B. Firewall
- C. Database
- D. Browser

4. What can attackers exploit to gain access to systems?

- A. Updates
- B. Firewalls
- C. Vulnerabilities
- D. Password managers

5. Which of the following is a common cyber threat?

- A. Malware
- B. Printer
- C. Router cable
- D. Monitor

Part B. Answer the Questions

- 6. What is network security?
- 7. Why do organizations need to protect their information systems?
- 8. What role does a firewall play in network security?
- 9. What is a vulnerability?
- 10. How can organizations improve the security of their networks?

***Additional tasks**

Exercise 1. Fill in the Blanks

Part A

- 1. Wireless networks use _____ signals.
- 2. Weak _____ reduce security.
- 3. WPA3 provides _____.
- 4. SSID is a network _____.
- 5. MAC filtering controls _____.
- 6. Public Wi-Fi is often _____.
- 7. MITM attacks _____ data.
- 8. VPN creates a secure _____.
- 9. Firmware updates fix _____.
- 10. Network _____ detects threats.

Part B

- 1. Malware is _____ software.
- 2. A virus spreads through _____.
- 3. A worm spreads _____.
- 4. Trojan looks _____ but is harmful.
- 5. Ransomware _____ files.
- 6. Spyware _____ user data.
- 7. Adware shows _____.
- 8. Phishing _____ users.
- 9. Antivirus _____ malware.
- 10. Firewall filters _____.

Exercise 2. Matching

Part A

1. WPA3	A) Secure connection
2. VPN	B) Network name
3. SSID	C) Device controller
4. Firewall	D) Protects data
5. MITM	E) Interception attack
6. MAC filtering	F) Controls devices
7. Router	G) Security protocol
8. Encryption	H) Risky network
9. Public Wi-Fi	I) Observes activity
10. Monitoring	J) Filters traffic

Part B

11. Virus	A) Harmful software
12. Worm	B) Collects data
13. Trojan	C) Shows ads
14. Ransomware	D) Encrypts files
15. Spyware	E) Filters traffic
16. Adware	F) Detects threats
17. Antivirus	G) Tricks users
18. Firewall	H) Spreads automatically
19. Phishing	I) Spreads via files
20. Malware	J) Fake program

Exercise 3. Discuss the questions:

Part A

1. What is Wi-Fi security?
2. What is WPA3?
3. What is a MITM attack?
4. Why is VPN important?
5. How can you protect a wireless network?
6. What is SSID and why is it important?
7. What is MAC filtering used for in wireless networks?
8. Why are public Wi-Fi networks considered risky?
9. What does firmware update do for a router?
10. What security measures help prevent unauthorized access to Wi-Fi networks?

Part B

1. What is malware?
2. What is a virus?

3. What is a worm?
4. What is a Trojan horse?
5. What is ransomware?
6. What is spyware?
7. What is adware?
8. What is phishing?
9. What does antivirus do?
10. What does a firewall do?

Exercise 4: Multiple Choice

Part A:

1. OS security protects:
 - A) Games
 - B) System and data
 - C) Music
 - D) Photos
2. OS manages:
 - A) Only files
 - B) Hardware and software
 - C) Only internet
 - D) Only passwords
3. Access control limits:
 - A) Speed
 - B) User access
 - C) Storage
 - D) Files
4. Vulnerability is:
 - A) Strength
 - B) Weakness
 - C) Tool
 - D) Program
5. Updates:
 - A) Add risks
 - B) Fix vulnerabilities
 - C) Delete data
 - D) Block users
6. Antivirus detects:
 - A) Hardware
 - B) Malware
 - C) Files
 - D) Users
7. Firewall:
 - A) Filters traffic

- B) Stores data
 - C) Deletes files
 - D) Encrypts emails
8. Encryption:
- A) Deletes data
 - B) Protects data
 - C) Blocks users
 - D) Restarts system
9. Disk encryption protects:
- A) Network
 - B) Stored data
 - C) Emails
 - D) Speed
10. Malware:
- A) Safe software
 - B) Harmful software
 - C) Update
 - D) Backup

Part B:

11. Malware is:
- A) Safe software
 - B) Harmful software
 - C) Update
 - D) Backup
12. Virus spreads:
- A) Automatically without user
 - B) Through infected files
 - C) Only by internet
 - D) Never
13. Worm:
- A) Needs user action
 - B) Spreads automatically
 - C) Is safe
 - D) Is antivirus
14. Trojan horse:
- A) Is safe
 - B) Looks legitimate but harmful
 - C) Deletes system
 - D) Updates OS
15. Ransomware:
- A) Speeds system
 - B) Encrypts files

- C) Deletes apps
- D) Blocks internet
- 16. Spyware:
 - A) Shows ads
 - B) Collects data
 - C) Deletes files
 - D) Updates system
- 17. Adware:
 - A) Protects system
 - B) Shows ads
 - C) Encrypts data
 - D) Removes malware
- 18. Phishing:
 - A) Protects users
 - B) Tricks users
 - C) Deletes files
 - D) Updates OS
- 19. Antivirus:
 - A) Creates malware
 - B) Detects malware
 - C) Deletes users
 - D) Blocks internet
- 20. Firewall:
 - A) Filters traffic
 - B) Stores data
 - C) Encrypts files
 - D) Deletes apps

Exercise 5: True / False

1. OS security is not important
2. OS controls system resources
3. Updates reduce risks
4. Antivirus removes malware
5. Firewalls filter traffic
6. Encryption protects data
7. Weak passwords are safe
8. Vulnerabilities are useful
9. Monitoring detects threats
10. Malware is safe

Exercise 6: Fill in the Blanks

1. OS manages _____ and software.
2. Access control limits _____.

3. Antivirus detects _____.
4. Updates fix _____.
5. Firewall filters _____.
6. Encryption protects _____.
7. Disk encryption protects _____ data.
8. Vulnerability is a _____.
9. Unauthorized _____ is dangerous.
10. System _____ detects threats.

Exercise 7: Matching

1. OS	A) Harmful software
2. Antivirus	B) Filters traffic
3. Firewall	C) Protects data
4. Encryption	D) Weakness
5. Vulnerability	E) Fixes system
6. Update	F) Controls system
7. Disk encryption	G) Protects disk
8. User account	H) User identity
9. Malware	I) Detects threats
10. Monitoring	J) Security process

Exercise 8. Discuss the questions:

1. What is an operating system?
2. What is OS security?
3. What is access control?
4. What is malware?
5. What does antivirus do?
6. What is a firewall?
7. What is encryption?
8. What is disk encryption?
9. What is a vulnerability?
10. Why are updates important?

FINAL TEST UNIT 4

PART 1: MULTIPLE CHOICE

1. What is the main responsibility of a cloud provider?
 - A) User passwords
 - B) Infrastructure security
 - C) User data
 - D) Applications

2. What does MFA provide?
 - A) Faster login
 - B) Multiple authentication factors
 - C) Data storage
 - D) Encryption
3. What is the biggest cloud security risk?
 - A) Hardware failure
 - B) Misconfiguration
 - C) Speed
 - D) Cost
4. Which service model gives most control?
 - A) SaaS
 - B) PaaS
 - C) IaaS
 - D) None
5. What does encryption do?
 - A) Deletes data
 - B) Protects data
 - C) Sends data
 - D) Stores data
6. What is IAM?
 - A) Identity and Access Management
 - B) Internet Access Mode
 - C) Internal Admin Module
 - D) Information Analysis Method
7. Public S3 bucket risk:
 - A) Faster access
 - B) Data exposure
 - C) Better performance
 - D) Backup
8. API keys should be:
 - A) Public
 - B) Hidden
 - C) Shared
 - D) Deleted
9. Logging helps:
 - A) Delete data
 - B) Track activity
 - C) Speed system
 - D) Encrypt data
10. IDS does:
 - A) Blocks traffic
 - B) Detects threats

- C) Deletes files
- D) Encrypts data
- 11. IPS does:
 - A) Detect only
 - B) Detect and block
 - C) Store logs
 - D) Encrypt
- 12. VPN provides:
 - A) Storage
 - B) Secure connection
 - C) Backup
 - D) Speed
- 13. Least privilege means:
 - A) Full access
 - B) Minimal access
 - C) No access
 - D) Shared access
- 14. Cloud logging example:
 - A) CloudTrail
 - B) Word
 - C) Excel
 - D) Paint
- 15. Data at rest means:
 - A) Moving data
 - B) Stored data
 - C) Deleted data
 - D) Shared data

PART 2: SCENARIO-BASED

- 16. Cloud bucket is public. What do you do?
 - A) Ignore
 - B) Restrict access
 - C) Delete logs
 - D) Restart
- 17. Login from 2 countries in 5 minutes.
 - A) Normal
 - B) Compromise
 - C) Update
 - D) Backup
- 18. API key leaked on GitHub.
 - A) Ignore
 - B) Rotate key
 - C) Share
 - D) Delete system
- 19. High CPU on cloud VM.



- A) Normal
 - B) Malware/cryptominer
 - C) Update
 - D) Backup
20. Logging disabled.
- A) Safe
 - B) Suspicious
 - C) Update
 - D) Backup
21. User gets admin role suddenly.
- A) Normal

- B) Privilege escalation
- C) Backup
- D) Update

22. Large data transfer at night.

- A) Backup
- B) Data exfiltration
- C) Update
- D) Normal

23. Multiple VMs created automatically.

- A) Normal
- B) Resource abuse
- C) Backup
- D) Update

24. No MFA on admin account.

- A) Safe
- B) Risky
- C) Normal
- D) Backup

25. Unknown IP accessing cloud DB.

- A) Normal
- B) Unauthorized access
- C) Backup
- D) Update

Unit 5

Cyberattacks and network security

Text 1. Cyberattacks and Network Security

Text 2. Denial-of-Service (DoS) Attacks

Text 3. SQL Injection Attacks

Text 4. Social Engineering

Text 5. Vulnerability Testing

Text 6. Network Protection Services and Mechanisms

Glossary

Cyberattack - Кібератака
Network security - Безпека мережі
Information system - Інформаційна система
Malware - Шкідливе програмне забезпечення
Phishing - Фішинг
DDoS attack - DDoS-атака
Brute force attack - Атака перебором паролів
SQL injection - SQL-ін'єкція
Man-in-the-middle attack - Атака «людина посередині»
Firewall - Мережевий екран (фаєрвол)
Encryption - Шифрування
Authentication - Аутентифікація
Authorization - Авторизація
Intrusion Detection System (IDS) - Система виявлення вторгнень
Intrusion Prevention System (IPS) - Система запобігання вторгненням
VPN (Virtual Private Network) - Віртуальна приватна мережа
Security patch - Оновлення безпеки
Vulnerability - Вразливість
Data breach - Витік даних
Access control - Контроль доступу
Denial-of-Service (DoS) attack - Атака «відмова в обслуговуванні»
Distributed Denial-of-Service (DDoS) attack - Розподілена атака «відмова в обслуговуванні»
Server - Сервер
Network traffic - Мережевий трафік
Bandwidth - Пропускна здатність
Overload - Перевантаження
Botnet - Ботнет (мережа заражених пристроїв)
Request - Запит
Availability - Доступність
Service disruption - Порушення роботи сервісу
Firewall - Мережевий екран (фаєрвол)
Mitigation - Зменшення шкоди / захист
Cyberattack - Кібератака
IP address - IP-адреса
Blocking - Блокування
SQL Injection - SQL-ін'єкція
Database - База даних
Query - Запит
Input field - Поле введення
Malicious code - Шкідливий код
Vulnerability - Вразливість

Attack - Атака
Unauthorized access - Несанкціонований доступ
Authentication - Аутентифікація
Data breach - Витік даних
Web application - Веб-додаток
Server - Сервер
Exploitation - Експлуатація (вразливості)
Security patch - Оновлення безпеки
Input validation - Перевірка введення
Social engineering - Соціальна інженерія
Phishing - Фішинг
Spear phishing - Цільовий фішинг
Pretexting - Створення вигаданого приводу (легенди)
Baiting - Приманка
Impersonation - Видавання себе за іншу особу
Scam - Шахрайство
Attack vector - Вектор атаки
Sensitive information - Конфіденційна інформація
Password - Пароль
Trust - Довіра
Manipulation - Маніпуляція
Victim - Жертва
Security awareness - Обізнаність у сфері безпеки
Vulnerability - Вразливість
Vulnerability testing - Тестування на вразливості
Penetration testing (Pentest) - Тестування на проникнення
Security audit - Аудит безпеки
Exploit - Експлойт (інструмент/код для використання вразливості)
Attack simulation - Імітація атаки
Risk assessment - Оцінка ризиків
Weakness - Слабке місце
System security - Безпека системи
Network security - Безпека мережі
Authentication - Аутентифікація
Authorization - Авторизація
Report - Звіт
Security team - Команда безпеки
Network protection services - Сервіси захисту мережі
Security mechanisms - Механізми безпеки
Firewall - Мережевий екран (фаєрвол)
Intrusion Detection System (IDS) - Система виявлення вторгнень
Intrusion Prevention System (IPS) - Система запобігання вторгненням
Antivirus software - Антивірусне програмне забезпечення

Encryption - Шифрування
VPN (Virtual Private Network) - Віртуальна приватна мережа
Authentication - Аутентифікація
Authorization - Авторизація
Access control - Контроль доступу
Security patch - Оновлення безпеки
Backup - Резервне копіювання
Monitoring - Моніторинг
Threat detection - Виявлення загроз

Text: Cyberattacks and Network Security

Cyberattacks are intentional actions that target computer systems, networks, or information systems in order to steal, damage, or disrupt data. In today's digital world, cyberattacks have become more frequent and more complex. Attackers use different methods depending on their goals and the weaknesses of a system.

One of the most common cyberattack methods is phishing. In phishing attacks, users are tricked into revealing personal information such as passwords or bank details. Another dangerous type is malware, which includes viruses, worms, and ransomware that can damage systems or block access to data. DDoS attacks are also widely used to overload servers and make services unavailable.

More advanced attacks include SQL injection, where attackers insert malicious code into databases, and brute force attacks, where many password combinations are tested until the correct one is found. Man-in-the-middle attacks allow criminals to secretly intercept communication between two parties and steal sensitive information.

To protect information systems, organizations use a combination of technical and organizational security measures. Firewalls are used to filter network traffic and block suspicious connections. Encryption protects data by converting it into a secure format that only authorized users can read. Authentication and authorization systems ensure that only verified users can access resources.

Additional protection is provided by IDS and IPS systems. IDS monitors network activity and detects suspicious behaviour, while IPS can automatically block potential threats. VPNs are used to create secure connections over public networks, protecting user data from interception.

Regular security updates and patches help fix vulnerabilities in software. Access control systems limit who can view or modify sensitive data. Companies also use backup systems to restore information after a cyberattack or data breach.

Effective network security requires a combination of technology, regular updates, and user awareness. Only by using multiple layers of protection can organizations reduce risks and protect their information systems from modern cyber threats.

Questions to the Text

1. What is a cyberattack?

2. What is the main goal of cyberattacks?
3. What is phishing used for?
4. What types of malware are mentioned in the text?
5. What is a DDoS attack?
6. What is SQL injection?
7. How does a brute force attack work?
8. What happens in a man-in-the-middle attack?
9. What is the role of a firewall?
10. How does encryption protect data?
11. What is the difference between authentication and authorization?
12. What does an IDS do?
13. How does an IPS differ from IDS?
14. Why is a VPN useful in network security?
15. What is the purpose of security patches?
16. What is a vulnerability in a system?
17. Why are backups important?
18. What is a data breach?
19. Why is user awareness important in cybersecurity?
20. What helps organizations reduce cyber risks?

Exercise 1. Multiple Choice. Choose the correct answer (A, B, C or D).

1. What is phishing used for?
 - A) Speeding up internet
 - B) Stealing personal information
 - C) Encrypting files
 - D) Updating software
2. Which attack overloads a server?
 - A) SQL injection
 - B) Phishing
 - C) DDoS attack
 - D) VPN attack
3. What does malware include?
 - A) Only firewalls
 - B) Viruses, worms, ransomware
 - C) Only passwords
 - D) Only networks
4. What is the purpose of a firewall?
 - A) To create viruses
 - B) To filter network traffic
 - C) To hack systems
 - D) To store data
5. What does encryption do?
 - A) Deletes files

- B) Converts data into a secure format
 - C) Shares passwords
 - D) Opens ports
6. What is used to monitor network activity?
- A) IDS
 - B) VPN
 - C) SQL
 - D) Malware
7. What is a brute force attack?
- A) Data backup
 - B) Password guessing
 - C) Firewall filtering
 - D) File encryption
8. What does a VPN do?
- A) Blocks antivirus
 - B) Encrypts internet connection
 - C) Deletes malware
 - D) Opens databases
9. What is two-factor authentication (2FA)?
- A) A type of malware
 - B) A method of using two passwords
 - C) An extra layer of account security
 - D) A firewall feature
10. Which password is the strongest?
- A) 12345678
 - B) password123
 - C) John2005
 - D) T7#qL9@xP2!
11. What should you do if you receive a suspicious email?
- A) Click all links
 - B) Reply with your password
 - C) Delete it or report it as phishing
 - D) Forward it to everyone
12. Which of the following is a good cybersecurity practice?
- A) Sharing passwords with friends
 - B) Using the same password for every account
 - C) Regularly updating software
 - D) Disabling antivirus software

Exercise 2. True / False. Write T (True) or F (False).

- 1. Cyberattacks are always harmless. ____
- 2. Phishing tricks users into revealing passwords. ____
- 3. Malware includes only viruses. ____

4. DDoS attacks can make services unavailable. ____
5. Encryption protects data from unauthorized reading. ____
6. IDS blocks all attacks automatically. ____
7. Firewalls filter network traffic. ____
8. SQL injection targets databases. ____
9. VPN increases security on public networks. ____
10. Backups help restore data after attacks. ____

Exercise 3. Fill in the Gaps

Use the words from the box:

phishing, firewall, encryption, malware, DDoS, IDS, VPN, brute force, vulnerability, backup

1. _____ is used to trick users into giving personal data.
2. A _____ filters network traffic.
3. _____ protects data by converting it into a secure form.
4. _____ includes viruses, worms, and ransomware.
5. A _____ attack overloads a server.
6. _____ monitors network activity and detects threats.
7. A _____ helps create secure internet connections.
8. A _____ attack tries many passwords.
9. A system weakness is called a _____.
10. A _____ is used to restore data after failure.

Exercise 4. Read the text and answer the questions.

Text: Denial-of-Service (DoS) Attacks

A Denial-of-Service (DoS) attack is a type of cyberattack that aims to make a computer system or network unavailable to its users. The attacker does this by overwhelming a server with a large number of requests, which the system cannot handle. As a result, the service becomes slow or completely stops working.

A more powerful version of this attack is the Distributed Denial-of-Service (DDoS) attack. In a DDoS attack, multiple compromised devices, often called a botnet, are used to send traffic to the target system at the same time. Because the requests come from many different sources, it is harder to stop the attack.

The main goal of DoS and DDoS attacks is to overload network traffic and reduce the availability of online services. These attacks can affect websites, online banking systems, government services, and many other platforms. Even a short disruption can cause financial loss and damage to reputation.

Attackers often target the bandwidth of a server. When bandwidth is fully used, legitimate users cannot access the service. Some attacks also exploit vulnerabilities in network systems to increase their effectiveness.

To protect against DoS and DDoS attacks, organizations use firewalls and special filtering systems. These tools help detect and block suspicious traffic.

Intrusion Detection Systems (IDS) can also identify unusual activity and alert administrators. In more advanced systems, traffic is distributed across multiple servers to reduce overload.

Although it is difficult to fully prevent these attacks, proper security measures can significantly reduce their impact. Continuous monitoring and quick response are essential for maintaining service availability.

Questions to the Text

1. What is the main goal of a DoS attack?
2. How does a DoS attack affect a system?
3. What is the difference between DoS and DDoS attacks?
4. What is a botnet?
5. Why are DDoS attacks harder to stop?
6. What does “availability” mean in cybersecurity?
7. Which systems can be affected by DoS attacks?
8. What happens when bandwidth is fully used?
9. How do attackers increase the effectiveness of attacks?
10. What tools are used to protect against DoS attacks?
11. What does a firewall do in this context?
12. What is the role of IDS systems?
13. Why is continuous monitoring important?
14. Can DoS attacks be fully prevented? Why or why not?
15. What is the impact of service disruption?

*Exercise 5. Match the Words with Their Definitions. Match (1–10) with (A–J).

Words:	Definitions:
1. DoS attack	A. A group of infected devices used to launch attacks
2. DDoS attack	B. The ability of a system to stay accessible and working
3. Botnet	C. A cyberattack that makes a system unavailable
4. Server	D. A system that filters and blocks network traffic
5. Network traffic	E. The interruption of normal service operation
6. Bandwidth	F. The amount of data transmitted over a network
7. Firewall	G. A powerful attack using many devices at once
8. Availability	H. A computer that provides services to users
9. Overload	I. Too many requests causing system failure
10. Service disruption	J. The capacity of a network to handle data

*Exercise 6. Translate the Sentences

1. Атака DoS робить сервер недоступним для користувачів.
2. DDoS-атака використовує багато пристроїв одночасно.
3. Ботнет складається з заражених комп'ютерів.
4. Сервер не може обробити занадто багато запитів.

5. Брандмауер допомагає блокувати підозрілий трафік.
6. Перевантаження мережі викликає збій системи.
7. Пропускна здатність мережі обмежена.
8. Важливо захищати онлайн-сервіси від атак.
9. IDS допомагає виявляти підозрілу активність.
10. Атаки можуть зашкодити репутації компанії.

***Exercise 7. Put the Words in the Correct Order. Rearrange the words to make correct sentences.**

1. attack / DoS / a / is / cyberattack
2. users / unavailable / makes / server / a / a / attack
3. many / uses / DDoS / devices / attack / a
4. traffic / network / is / overloaded
5. botnet / infected / a / is / devices / of / group
6. firewall / traffic / filters / network
7. requests / server / too many / cannot / handle / a
8. availability / system / is / important
9. attacks / services / disrupt / can
10. protection / security / requires / strong

Exercise 8. Read the text and answer the questions:

Text: SQL Injection Attacks

SQL injection is a type of cyberattack that targets databases through vulnerable web applications. It happens when attackers insert malicious SQL code into input fields, such as login forms or search boxes. If the system does not properly validate user input, this code can be executed by the database.

The main goal of SQL injection is to gain unauthorized access to sensitive information stored in a database. Attackers can retrieve usernames, passwords, financial data, or even delete important records. In some cases, they can also change or manipulate data inside the system.

SQL injection attacks exploit vulnerabilities in web applications. These vulnerabilities often appear when developers do not properly sanitize user input. For example, combining user input directly with SQL queries can create serious security risks.

A successful SQL injection attack can lead to a data breach, which may cause financial and reputational damage to organizations. Attackers may also bypass authentication systems and gain full access to restricted areas of a website or application.

To protect against SQL injection, developers must use input validation and parameterized queries. These methods ensure that user input is treated as data, not as executable code. Security patches are also important because they fix known vulnerabilities in software systems.

Firewalls and intrusion detection systems can help detect suspicious database activity, but the most effective protection is secure coding practices. Regular testing of web applications is necessary to identify and remove weaknesses before attackers can exploit them.

SQL injection remains one of the most dangerous and common web security threats. Understanding how it works helps developers build safer and more reliable systems.

Questions to the Text

1. What is SQL injection?
2. What is the main target of SQL injection attacks?
3. How do attackers insert malicious code into a system?
4. What happens if user input is not validated?
5. What is the main goal of SQL injection attacks?
6. What type of information can attackers steal?
7. How can attackers damage or modify data?
8. What causes vulnerabilities in web applications?
9. What is a data breach?
10. How can attackers bypass authentication systems?
11. What is input validation?
12. Why are parameterized queries important?
13. What role do security patches play?
14. Can firewalls fully prevent SQL injection attacks? Why?
15. Why is secure coding important in preventing SQL injection?

Exercise 9. Correct the Mistakes. Find and correct the mistakes in the sentences.

1. SQL injection is a type of network attack that targets firewalls.
2. Attackers insert malicious HTML code into databases.
3. If user input is validated, SQL injection becomes easier.
4. SQL injection can only steal passwords, not other data.
5. A successful attack can lead to a data backup.
6. Developers should combine user input directly with SQL queries.
7. Input validation treats code as executable commands.
8. Security patches create new vulnerabilities in systems.
9. Firewalls can completely stop all SQL injection attacks.
10. SQL injection is not related to web applications.

Exercise 10. Discuss the Questions. Answer the questions (speaking or writing).

1. What is SQL injection in your own words?
2. Why is SQL injection dangerous for organizations?
3. How do attackers use input fields in SQL injection attacks?
4. What types of data can be stolen from databases?
5. What is a data breach and what are its consequences?

6. Why is input validation important in web applications?
7. How do parameterized queries improve security?
8. Can firewalls fully protect systems from SQL injection? Why or why not?
9. What role do developers play in preventing SQL injection?
10. Why is secure coding important in cybersecurity?

Exercise 11. Read the text and answer the questions.

Text: Social Engineering

Social engineering is a type of cyberattack that does not focus on breaking technical systems but instead targets human psychology. Attackers use manipulation and deception to trick people into revealing sensitive information such as passwords, financial details, or access codes.

One of the most common forms of social engineering is phishing. In phishing attacks, victims receive fake emails or messages that look like they come from trusted organizations. These messages often contain links that lead to fake websites designed to steal personal data. Spear phishing is a more targeted version of this attack, where a specific person or organization is carefully selected.

Another technique is pretexting, where the attacker creates a false identity or story to gain the victim's trust. Baiting is also common, where attackers offer something attractive, such as free software or a USB device, to lure users into installing malware. Impersonation involves pretending to be a colleague, technician, or authority figure in order to gain access to information or systems.

Social engineering is dangerous because it exploits human trust rather than system vulnerabilities. Even strong technical security systems cannot fully protect against these attacks if users are not careful.

To prevent social engineering attacks, organizations focus on security awareness training. Employees are taught to recognize suspicious messages, avoid sharing personal information, and verify identities before taking action. Strong security policies and verification procedures also help reduce risks.

In conclusion, social engineering remains one of the most effective cyberattack methods because it targets people rather than technology. Awareness and caution are the most important defenses against it.

Questions to the Text

1. What is social engineering?
2. What does social engineering target instead of technical systems?
3. What is the main goal of social engineering attacks?
4. What is phishing?
5. How do phishing messages usually look?
6. What is spear phishing?
7. What is pretexting?
8. What does baiting involve?
9. What is impersonation in social engineering?

10. Why is social engineering dangerous?
11. Why can technical security systems be insufficient against social engineering?
12. What is security awareness training?
13. How can employees protect themselves from social engineering attacks?
14. Why is verifying identity important?
15. Why is social engineering considered very effective?

Exercise 11. True / False. Write T (True) or F (False).

1. Social engineering targets computer systems only. ____
2. Phishing is a form of social engineering. ____
3. Spear phishing is a general attack on many users. ____
4. Social engineering uses manipulation and deception. ____
5. Baiting involves offering something attractive to the victim. ____
6. Social engineering exploits human trust. ____
7. Technical systems always fully protect against social engineering. ____
8. Impersonation means pretending to be someone else. ____
9. Security awareness training helps prevent attacks. ____
10. Social engineering is based on psychological tricks. ____

***Exercise 12. Multiple Choice.** Choose the correct answer (A, B, C or D).

1. What does social engineering mainly target?
 - A) Hardware
 - B) Human psychology
 - C) Internet speed
 - D) Software updates
2. What is phishing used for?
 - A) Fixing systems
 - B) Stealing sensitive information
 - C) Updating antivirus
 - D) Encrypting files
3. Spear phishing is:
 - A) Random attack
 - B) Targeted attack
 - C) Hardware attack
 - D) Firewall update
4. What is pretexting?
 - A) Creating a fake identity or story
 - B) Installing antivirus
 - C) Encrypting data
 - D) Updating software
5. What is baiting?
 - A) Blocking attacks
 - B) Offering something attractive to trick users

- C) Scanning networks
- D) Encrypting messages
- 6. Impersonation means:
 - A) Deleting files
 - B) Pretending to be someone else
 - C) Encrypting data
 - D) Backing up data
- 7. Social engineering is dangerous because it exploits:
 - A) Internet speed
 - B) Human trust
 - C) Hardware failure
 - D) Software bugs only
- 8. Security awareness training helps users:
 - A) Hack systems
 - B) Recognize suspicious activity
 - C) Write malware
 - D) Disable firewalls

***Exercise 13. Fill in the Gaps**

Use the words from the box:

(phishing, impersonation, manipulation, trust, baiting, awareness, pretexting, victim, social engineering, sensitive information)

1. _____ is a cyberattack that targets human psychology.
2. Attackers use _____ to trick people.
3. The main goal is to steal _____.
4. A _____ is the person who is attacked.
5. _____ is a form of fake email attack.
6. _____ involves pretending to be someone else.
7. _____ is when attackers create a fake story.
8. _____ involves offering something attractive to trick users.
9. These attacks exploit human _____.
10. Security _____ helps prevent attacks.

***Exercise 14. Read the text and answer the questions.**

Text: Vulnerability Testing

Vulnerability testing is the process of identifying weaknesses in computer systems, networks, and applications that could be exploited by attackers. It is an important part of cybersecurity because it helps organizations find and fix security problems before criminals can use them.

One common method of vulnerability testing is penetration testing, also known as pentesting. During a penetration test, security experts simulate real cyberattacks to check how well a system can resist threats. These experts use tools and techniques

similar to those used by hackers, but their goal is to improve security rather than cause damage.

Another important process is vulnerability scanning. This involves using automated tools to detect known weaknesses in software, operating systems, and network configurations. After scanning, security teams analyze the results and decide which vulnerabilities need to be fixed first.

Risk assessment is also an essential part of vulnerability testing. It helps organizations understand how serious each vulnerability is and what impact it could have on the system. Based on this analysis, companies can prioritize security improvements.

After testing, a detailed report is created. This report includes information about discovered vulnerabilities, their severity, and recommendations for fixing them. Developers and security teams then apply security patches and improve system configuration.

Vulnerability testing helps organizations strengthen their defenses and reduce the risk of cyberattacks. Regular testing is necessary because new vulnerabilities appear all the time as software and systems change.

Questions to the Text

1. What is vulnerability testing?
2. Why is vulnerability testing important in cybersecurity?
3. What is penetration testing (pentesting)?
4. What is the goal of penetration testing?
5. How is penetration testing different from real hacking?
6. What is vulnerability scanning?
7. What tools are used in vulnerability scanning?
8. What happens after scanning is completed?
9. What is risk assessment used for?
10. Why is it important to prioritize vulnerabilities?
11. What information is included in a vulnerability report?
12. Who uses the results of vulnerability testing?
13. What is the role of security patches?
14. Why must vulnerability testing be done regularly?
15. What is the main purpose of vulnerability testing overall?

***Exercise 15. Read the texts below. Match choices (A–H) to texts (1–5). There are three choices you do not need to use.**

Text

1. _____ This process helps organizations find weaknesses in their systems before attackers can use them. Security experts simulate real attacks to test how strong the protection is. The goal is to improve security, not to damage the system. Different attack methods are used during the test. After the testing is completed, experts

explain which vulnerabilities were found. Organizations can then improve their security based on the results.

2. _____ Automated tools are used to scan software and networks for known security problems. After scanning, results are analyzed to determine which issues are the most dangerous and need urgent fixing. The scanning process is fast and can check many systems at the same time. Regular scanning helps detect new vulnerabilities before they become serious problems.

3. _____ After testing a system, specialists create a document that explains all discovered problems. It also includes recommendations for fixing vulnerabilities and improving overall security. The report often lists the severity of each weakness. Developers and system administrators use this information to make the necessary improvements.

4. _____ This process evaluates how dangerous each weakness is and what damage it could cause. Based on this analysis, organizations decide which problems must be solved first. Some vulnerabilities have a higher risk than others. Risk assessment helps companies use their time and resources more effectively.

5. _____ Security teams use updates and fixes to close weaknesses in software and operating systems. These fixes help prevent attackers from exploiting known problems in the system. Security patches should be installed as soon as possible. Keeping software updated is one of the simplest ways to improve cybersecurity.

Options (A–H)

- A. Vulnerability scanning
- B. Penetration testing
- C. Risk assessment
- D. Security report
- E. Encryption process
- F. Firewall configuration
- G. Malware analysis
- H. Security patching

Exercise 16. Match the English terms (1–18) with their Ukrainian equivalents (A–R)

English Terms	Ukrainian Equivalents
1. Vulnerability	A. Мережевий екран (файрвол)
2. Penetration testing	B. Аутентифікація
3. Security audit	C. Вразливість
4. Exploit	D. Оцінка ризиків

5. Risk assessment	Е. Тестування на проникнення
6. Attack simulation	Ф. Авторизація
7. Security report	Г. Шкідливе програмне забезпечення
8. Weakness	Н. Атака-експлойт (використання вразливості)
9. System security	І. Безпека системи
10. Network security	Ж. Безпека мережі
11. Authentication	К. Витік даних
12. Authorization	Л. Система виявлення вторгнень
13. Malware	М. Шифрування
14. Firewall	Н. Звіт з безпеки
15. Encryption	О. Тестування/імітація атаки
16. Data breach	Р. Слабке місце
17. Intrusion detection system (IDS)	Q. Аудит безпеки
18. Security patch	Р. Оновлення безпеки

Exercise 17. Put the Words in the Correct Order. Use the cybersecurity vocabulary to make correct sentences.

1. vulnerability / a / system / is / weakness / in / a
2. penetration testing / security / improves / system / the
3. attackers / exploit / vulnerabilities / can
4. firewall / network / a / traffic / filters
5. encryption / protects / sensitive / data
6. risk assessment / helps / identify / risks
7. security audit / checks / system / the
8. malware / damages / computer / systems
9. authentication / verifies / user / identity
10. authorization / controls / access / resources
11. IDS / suspicious / detects / activity
12. security patch / fixes / vulnerabilities
13. data breach / is / a / security / incident
14. exploit / uses / a / vulnerability / attack
15. network security / protects / systems / connected

Exercise 18. Read the text and answer the questions.

Text: Network Protection Services and Mechanisms

Network protection services and security mechanisms are essential for ensuring the safety of computer systems and data. In modern organizations, a combination of tools and technologies is used to protect networks from cyber threats and unauthorized access.

One of the most important security mechanisms is the firewall. It controls incoming and outgoing network traffic and blocks suspicious connections based on

predefined security rules. Firewalls are often the first line of defense in network security systems.

Another key tool is the Intrusion Detection System (IDS), which monitors network activity and identifies suspicious behavior. If a potential threat is detected, the system sends alerts to security administrators. The Intrusion Prevention System (IPS) goes a step further by automatically blocking or preventing detected attacks.

Encryption is also widely used to protect sensitive data. It converts information into a secure format that can only be read by authorized users. VPN services use encryption to create secure connections over public networks, protecting user privacy and data.

Authentication and authorization mechanisms ensure that only verified users can access system resources. Access control systems define what actions users are allowed to perform.

Additional services such as antivirus software help detect and remove malware, while security patches fix vulnerabilities in software systems. Backup systems ensure that data can be restored in case of cyberattacks or system failures.

Together, these services and mechanisms create a strong security environment that protects networks from a wide range of cyber threats.

Questions to the Text

1. What is the purpose of network protection services?
2. What does a firewall do?
3. Why is a firewall considered the first line of defense?
4. What is the function of an IDS?
5. How does IPS differ from IDS?
6. What is encryption used for?
7. How does a VPN protect users?
8. What is authentication?
9. What is authorization?
10. What does access control define?
11. What is the role of antivirus software?
12. What are security patches used for?
13. Why are backup systems important?
14. What happens when IDS detects a threat?
15. How do these mechanisms work together to protect networks?

Exercise 19. Multiple Choice. Choose the correct answer (A, B, C or D).

1. What is the main purpose of a firewall?
 - A) To create viruses
 - B) To filter network traffic
 - C) To delete files
 - D) To increase speed
2. What does IDS do?
 - A) Encrypts data

- B) Detects suspicious activity
 - C) Blocks websites
 - D) Stores passwords
3. IPS is different from IDS because it:
- A) Monitors only
 - B) Blocks attacks automatically
 - C) Deletes data
 - D) Slows networks
4. What is encryption used for?
- A) Breaking systems
 - B) Protecting data
 - C) Deleting files
 - D) Sharing passwords
5. VPN helps to:
- A) Hack systems
 - B) Create secure connections
 - C) Increase malware
 - D) Remove firewalls
6. Authentication means:
- A) Deleting users
 - B) Verifying identity
 - C) Blocking traffic
 - D) Updating software
7. Authorization controls:
- A) Internet speed
 - B) User permissions
 - C) Hardware
 - D) Antivirus
8. Backup is used to:
- A) Encrypt data
 - B) Restore data
 - C) Hack systems
 - D) Block users
9. What is the main function of antivirus software?
- A) To detect and remove malware
 - B) To create user accounts
 - C) To encrypt databases
 - D) To increase internet speed
10. What do security patches do?
- A) Create new vulnerabilities
 - B) Fix known software weaknesses
 - C) Block all websites
 - D) Delete backup files

11. What happens when an IDS detects a threat?
 - A) It deletes the system
 - B) It sends an alert to administrators
 - C) It formats the hard drive
 - D) It automatically encrypts all files
12. Why are network protection mechanisms important?
 - A) They make computers slower
 - B) They protect networks from cyber threats
 - C) They replace operating systems
 - D) They create malware

Exercise 20. Fill in the Blanks

Use the words: *firewall, encryption, IDS, IPS, VPN, authentication, authorization, backup, antivirus, security patch*

1. A _____ filters incoming and outgoing network traffic.
2. _____ protects data by converting it into a secure form.
3. An _____ detects suspicious activity in a network.
4. An _____ can automatically block attacks.
5. A _____ creates a secure connection over public networks.
6. _____ verifies the identity of a user.
7. _____ controls what users are allowed to do.
8. A _____ helps restore lost data.
9. _____ software detects and removes malware.
10. A _____ fixes vulnerabilities in software.

Exercise 21. Read the text and choose the correct answer (A, B, C or D).

Network protection services are used to secure computer systems from cyber threats. A firewall is a key mechanism that filters network traffic and blocks unauthorized connections. It is considered the first line of defense in network security.

Intrusion Detection Systems (IDS) monitor network activity and detect suspicious behavior. If a threat is found, alerts are sent to administrators. Intrusion Prevention Systems (IPS) go further by automatically blocking malicious actions.

Encryption is used to protect sensitive data by converting it into unreadable form. VPN services also use encryption to secure internet connections, especially on public networks.

Authentication and authorization ensure that only verified users can access resources. Access control defines what actions users can perform in a system.

Security patches are released to fix vulnerabilities in software, while antivirus programs help detect malware. Backup systems are important because they allow data recovery after cyberattacks or system failures.

Together, these mechanisms create a strong defense system against modern cyber threats.

Questions 1-10

1. What is the main role of a firewall?
 - A) Encrypt data
 - B) Filter network traffic
 - C) Store files
 - D) Delete malware
2. IDS is used to:
 - A) Detect suspicious activity
 - B) Create backups
 - C) Speed up internet
 - D) Block VPN
3. IPS can:
 - A) Monitor only
 - B) Block attacks
 - C) Encrypt passwords
 - D) Remove firewalls
4. Encryption helps to:
 - A) Make data unreadable to unauthorized users
 - B) Delete data
 - C) Share passwords
 - D) Increase traffic
5. VPN is mainly used for:
 - A) Security connections
 - B) Creating malware
 - C) Hardware repair
 - D) File deletion
6. Authentication verifies:
 - A) Network speed
 - B) User identity
 - C) Software updates
 - D) IP addresses
7. Authorization controls:
 - A) User permissions
 - B) Antivirus updates
 - C) Network cables
 - D) Hardware devices
8. Security patches are used to:
 - A) Create vulnerabilities
 - B) Fix vulnerabilities
 - C) Increase malware
 - D) Block users

9. Antivirus software helps to:
- A) Detect malware
 - B) Create viruses
 - C) Break networks
 - D) Hack systems
10. Backup systems are used for:
- A) Data recovery
 - B) Data encryption
 - C) Data deletion
 - D) Network blocking

Exercise 22. Listening Task: Cyberattacks and Network Security. Listen to the text and choose the correct answer (A, B, C or D).

Cyberattacks are becoming more common in today's digital world. Hackers use different methods to break into computer systems and steal important information. One of the most common attacks is phishing. In this type of attack, people receive fake emails that look real, and they are tricked into giving away passwords or personal data.

Another dangerous type of cyberattack is malware. Malware is software designed to damage or control a computer system. It can delete files, spy on users, or lock data for ransom. To protect against these threats, organizations use security tools such as firewalls, antivirus programs, and intrusion detection systems.

A firewall helps block unwanted network traffic, while antivirus software removes malicious programs. Intrusion Detection Systems, or IDS, monitor network activity and send alerts when something unusual is detected. Many companies also use encryption to protect sensitive data and VPNs to create secure internet connections.

Even with strong technology, human error is still a major risk. That is why security training is important. Employees must learn how to recognize suspicious emails and avoid unsafe websites.

Questions:

1. What is phishing used for?
 - A) Increasing internet speed
 - B) Stealing personal information
 - C) Updating software
 - D) Blocking viruses
2. What is malware?
 - A) A type of firewall
 - B) A secure network connection
 - C) Software that damages systems
 - D) A password manager
3. What does a firewall do?
 - A) Deletes files

- B) Blocks unwanted traffic
- C) Creates backups
- D) Sends emails
- 4. What does IDS do?
 - A) Encrypts data
 - B) Monitors network activity and sends alerts
 - C) Removes antivirus
 - D) Hacks systems
- 5. What is important besides technical protection?
 - A) Buying new computers
 - B) Human security awareness and training
 - C) Increasing internet speed
 - D) Disabling firewalls

Exercise 23. Watch the video: <https://www.youtube.com/watch?v=sdpxddDzXfE> answer the questions and choose the correct answer (Part A and B):

Questions

1. What is a cyberattack?
2. What is the main purpose of cyberattacks?
3. What is phishing?
4. What does malware do to a computer system?
5. Why do attackers use fake messages or websites?
6. What is one common goal of hackers mentioned in the video?
7. What can users do to protect themselves online?
8. Why is cybersecurity important today?

Part A: Vocabulary (Match the word to the definition)

1. **Cyberattack**
2. **Phishing**
3. **Malware**
4. **Hacker**
5. **Security tools**

Definitions:

- A) Software used to protect computers
- B) A malicious attempt to access or damage systems
- C) A person who tries to break into systems
- D) Software that harms or controls a system
- E) Fake messages used to steal information

Part B: Choose the correct answer (A, B, C or D)

6. What is the main goal of cyberattacks?

- A) To improve security
- B) To steal or damage data
- C) To fix systems
- D) To clean viruses

7. What is phishing used for?

- A) To update software
- B) To trick users into giving personal data
- C) To protect networks
- D) To create backups

8. What does malware do?

- A) Protects systems
- B) Damages or controls systems
- C) Encrypts data
- D) Increases speed

9. What is important for online safety?

- A) Ignoring updates
- B) Using weak passwords
- C) Using security tools and safe behavior
- D) Turning off antivirus

10. Why is cybersecurity important?

- A) Because computers are slow
- B) Because cyber threats are increasing
- C) Because internet is free
- D) Because systems do not need protection

FINAL TEST UNIT 5

Part 1: Multiple Choice (1–15)

Choose the correct answer (A, B, C or D).

1. What is the main goal of a cyberattack?
 - A) Improve network speed
 - B) Protect data
 - C) Steal or damage information
 - D) Update software

2. Phishing is used to:
 - A) Encrypt files
 - B) Trick users into giving data
 - C) Block networks
 - D) Repair systems
3. Malware includes:
 - A) Firewalls only
 - B) Viruses, worms, ransomware
 - C) VPNs
 - D) Passwords
4. A firewall is used to:
 - A) Create networks
 - B) Filter traffic
 - C) Store data
 - D) Hack systems
5. Encryption protects data by:
 - A) Deleting it
 - B) Making it unreadable
 - C) Sharing it
 - D) Compressing it
6. A DDoS attack:
 - A) Improves servers
 - B) Overloads a system
 - C) Encrypts traffic
 - D) Updates software
7. IDS is used to:
 - A) Detect threats
 - B) Block all websites
 - C) Store passwords
 - D) Delete malware
8. IPS can:
 - A) Only monitor
 - B) Block attacks
 - C) Increase traffic
 - D) Disable encryption
9. SQL injection targets:
 - A) Hardware
 - B) Databases
 - C) Monitors
 - D) Wi-Fi
10. A brute force attack is:
 - A) Password guessing
 - B) Encryption method

- C) Backup system
- D) Firewall rule
- 11. Social engineering targets:
 - A) Hardware
 - B) Human psychology
 - C) Servers only
 - D) Antivirus systems
- 12. VPN is used to:
 - A) Create secure connections
 - B) Delete malware
 - C) Increase attacks
 - D) Block users
- 13. Authentication means:
 - A) Hacking system
 - B) Verifying identity
 - C) Encrypting files
 - D) Deleting data
- 14. Authorization controls:
 - A) User access rights
 - B) Internet speed
 - C) Hardware power
 - D) Network cables
- 15. A data breach is:
 - A) Data backup
 - B) Unauthorized data access
 - C) Software update
 - D) Antivirus scan

Part 2: True / False (16–23)

Write T (True) or F (False).

- 16. Phishing is a technical attack only. ____
- 17. Malware can damage computer systems. ____
- 18. Firewalls filter network traffic. ____
- 19. Encryption makes data easier to read. ____
- 20. Social engineering uses manipulation. ____
- 21. IDS prevents all attacks automatically. ____
- 22. VPN increases network security. ____
- 23. SQL injection targets web databases. ____

Part 3: Fill in the Gaps (24–27)

Use the words: (*firewall, malware, encryption, phishing, VPN*)

- 24. _____ is used to trick users into revealing data.
- 25. _____ protects data by converting it into secure form.



26. _____ filters network traffic.
27. _____ includes viruses and ransomware.

Part 4: Short Answer (28–30)

28. What is a cyberattack?
29. Name two types of cyberattacks.
30. How can organizations protect against cyberattacks?

Unit 6

The basics of cryptography and steganography

Text 1. Cryptography and Steganography

Text 2. Secret-Key Cryptosystems

Text 3. Public-Key Cryptosystems

Text 4. Cryptographic Protocols

Text 5. Digital Steganography

Glossary

Cryptography - Криптографія
Steganography - Стеганографія
Encryption - Шифрування
Decryption - Розшифрування
Cipher - Шифр
Plaintext - Відкритий текст
Ciphertext - Шифртекст (зашифрований текст)
Key - Ключ
Public key - Відкритий ключ
Private key - Приватний ключ
Symmetric encryption - Симетричне шифрування
Asymmetric encryption - Асиметричне шифрування
Hash function - Хеш-функція
Digital signature - Цифровий підпис
Data concealment - Приховування даних
Secret-key cryptosystem — криптосистема з секретним ключем
Symmetric encryption — симетричне шифрування
Decryption — дешифрування
Secret key — секретний ключ
Cryptographic algorithm — криптографічний алгоритм
Data protection — захист даних
Information security — інформаційна безпека
Confidentiality — конфіденційність
Integrity — цілісність
Authentication — автентифікація
Key distribution — розповсюдження ключів
Key management — управління ключами
Secure communication — безпечний зв'язок
Data transmission — передача даних
Block cipher — блоковий шифр
Stream cipher — потоковий шифр
Advanced Encryption Standard (AES) — стандарт розширеного шифрування (AES)
Data Encryption Standard (DES) — стандарт шифрування даних (DES)
Triple DES (3DES) — потрійний DES
Brute-force attack — атака повним перебором
Cryptanalysis — криптоаналіз
Security level — рівень безпеки
Encryption key length — довжина ключа шифрування
Secure storage — безпечне зберігання
Digital information — цифрова інформація

Access control — контроль доступу
Data confidentiality — конфіденційність даних
Cryptographic protocol — криптографічний протокол
Secure system — захищена система
Data breach — витік даних
Encryption process — процес шифрування
Decryption process — процес дешифрування
Key exchange — обмін ключами
Secure channel — захищений канал
Sensitive information — конфіденційна інформація
Public-key cryptosystem — криптосистема з публічним ключем
Key pair — пара ключів
Digital signature — цифровий підпис
Non-repudiation — невідмовність
Key generation — генерація ключів
Key distribution — розповсюдження ключів
Certificate — сертифікат
Certificate Authority (CA) — центр сертифікації
Public Key Infrastructure (PKI) — інфраструктура відкритих ключів (PKI)
Cryptographic algorithm — криптографічний алгоритм
RSA algorithm — алгоритм RSA
Elliptic Curve Cryptography (ECC) — криптографія на еліптичних кривих
Secure communication — безпечний зв'язок
Secure connection — захищене з'єднання
Message authentication — автентифікація повідомлення
Identity verification — перевірка особи
Digital certificate — цифровий сертифікат
Secure transaction — безпечна транзакція
Electronic commerce (e-commerce) — електронна комерція
Cryptanalysis — криптоаналіз
Trusted third party — довірена третя сторона
Cryptographic protocol — криптографічний протокол
Secure communication — безпечний зв'язок
Handshake protocol — протокол встановлення з'єднання
Session key — сесійний ключ
Non-repudiation — невідмовність
TLS (Transport Layer Security) — протокол захисту транспортного рівня (TLS)
SSL (Secure Sockets Layer) — захищений сокетний рівень (SSL)
Protocol attack — атака на протокол
Man-in-the-middle attack — атака “людина посередині”
Secure channel — захищений канал
Public key infrastructure (PKI) — інфраструктура відкритих ключів

Certificate authority (CA) — центр сертифікації
Message authentication code (MAC) — код автентифікації повідомлення
Hash function — хеш-функція
Secure connection — захищене з'єднання
Protocol design — проектування протоколів
Cryptographic algorithm — криптографічний алгоритм
Key agreement — узгодження ключів
Forward secrecy — пряма секретність
Replay attack — атака повторного відтворення
Session management — управління сесіями
Secure handshake — безпечне встановлення з'єднання
Identity verification — перевірка особи
Secure protocol — захищений протокол
Mutual authentication — взаємна автентифікація
Security layer — рівень безпеки
Protocol vulnerability — вразливість протоколу
Trusted connection — довірене з'єднання
Digital steganography — цифрова стеганографія
Hidden message — приховане повідомлення
Cover file — носій (файл-«обкладинка»)
Payload — приховані дані
Embedding — вбудовування (даних)
Extraction — витягування (даних)
Stego file — стегофайл (файл із прихованими даними)
Image steganography — стеганографія зображень
Audio steganography — аудіостеганографія
Video steganography — відеостеганографія
Least Significant Bit (LSB) — метод найменш значущого біта
Data hiding — приховування даних
Steganalysis — стеганаліз
Detection — виявлення
Carrier medium — носій інформації
Imperceptibility — непомітність
Robustness — стійкість
Capacity — місткість
Digital watermarking — цифровий водяний знак
File format — формат файлу
Modification — модифікація
Signal processing — обробка сигналів
Covert communication — прихована комунікація
Information hiding system — система приховування інформації
Stego key — стего-ключ
Detection resistance — стійкість до виявлення

Compression — стиснення

Digital image — цифрове зображення

Security technique — техніка безпеки

Cover distortion — спотворення носія

Hidden communication channel — прихований канал зв'язку

Text: Cryptography and Steganography

Cryptography is a method of protecting information by transforming it into an unreadable format so that only authorized users can access it. The main goal of cryptography is to ensure confidentiality, integrity, and authenticity of data. Encryption converts plaintext into ciphertext using a mathematical algorithm and a key. Decryption is the reverse process that restores the original message.

There are two main types of encryption: symmetric and asymmetric. Symmetric encryption uses the same key for both encryption and decryption. Asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption. This method is widely used in secure communication systems, such as online banking and digital certificates.

Hash functions are also an important part of cryptography. They transform data into a fixed-length value that cannot be easily reversed. This is useful for verifying data integrity and storing passwords securely. Digital signatures use cryptographic techniques to confirm the identity of the sender and ensure that the message has not been changed.

Steganography is a different approach to information security. Instead of encrypting data, it hides the existence of the message itself. For example, a secret message can be hidden inside an image, audio file, or video. Unlike cryptography, which protects the content, steganography protects the existence of communication.

Both cryptography and steganography are important tools in modern cybersecurity. They are often used together to provide stronger protection of sensitive information. Cryptographic methods secure the content of data, while steganography hides the fact that communication is taking place.

Questions to the Text

1. What is cryptography?
2. What is the main goal of cryptography?
3. What is encryption?
4. What is decryption?
5. What is plaintext?
6. What is ciphertext?
7. What are the two main types of encryption?
8. How does symmetric encryption work?
9. How does asymmetric encryption work?
10. What is a cryptographic key?

11. What is a hash function used for?
12. What is a digital signature?
13. What does steganography do?
14. How is steganography different from cryptography?
15. Why are both methods important in cybersecurity?

Exercise 1. Multiple Choice

Choose the correct answer (A, B, C or D).

1. What is cryptography used for?
 - A) Speeding up networks
 - B) Protecting information
 - C) Deleting files
 - D) Creating hardware
2. Encryption converts plaintext into:
 - A) Password
 - B) Ciphertext
 - C) Virus
 - D) Backup
3. Decryption means:
 - A) Hiding data
 - B) Restoring original data
 - C) Deleting data
 - D) Compressing files
4. Steganography is used to:
 - A) Encrypt passwords
 - B) Hide the existence of data
 - C) Block networks
 - D) Update software
5. Symmetric encryption uses:
 - A) Two keys
 - B) One key
 - C) No key
 - D) Hardware key only
6. Asymmetric encryption uses:
 - A) One password
 - B) Public and private keys
 - C) Firewall rules
 - D) Antivirus
7. A hash function produces:
 - A) Random hardware
 - B) Fixed-length value
 - C) Network traffic
 - D) Images

8. A digital signature is used to:
 - A) Increase speed
 - B) Verify sender identity
 - C) Delete viruses
 - D) Encrypt hardware
9. Steganography hides:
 - A) Passwords only
 - B) The existence of a message
 - C) Internet speed
 - D) Antivirus software
10. Ciphertext is:
 - A) Original message
 - B) Encrypted message
 - C) Virus
 - D) Network error

Exercise 2. True / False. Write T (True) or F (False).

1. Cryptography protects information. ____
2. Plaintext is encrypted data. ____
3. Decryption makes data readable again. ____
4. Steganography hides the content of data. ____
5. Symmetric encryption uses two keys. ____
6. Asymmetric encryption uses public and private keys. ____
7. A hash function can be reversed easily. ____
8. Digital signatures verify identity. ____
9. Steganography hides the existence of data. ____
10. Cryptography and steganography are unrelated fields. ____

Exercise 3. Fill in the Gaps

Use the words:

cryptography, encryption, decryption, ciphertext, plaintext, key, hash, steganography, symmetric, asymmetric

1. _____ protects information by transforming it.
2. _____ converts data into unreadable form.
3. _____ restores original data.
4. _____ is readable original data.
5. _____ is encrypted data.
6. A _____ is used in encryption algorithms.
7. _____ encryption uses one key.
8. _____ encryption uses public and private keys.
9. _____ hides the existence of a message.
10. A _____ function helps verify data integrity.

Exercise 4. Read the text and answer the questions.

Text: Secret-Key Cryptosystems

Secret-key cryptosystems, also known as symmetric cryptosystems, are one of the most widely used methods of protecting digital information. In these systems, the same secret key is used for both encryption and decryption. This means that the sender and the receiver must possess the same key and keep it confidential.

The main purpose of a secret-key cryptosystem is to ensure the confidentiality of information during storage and transmission. Before sending a message, the sender uses a cryptographic algorithm and a secret key to transform the plaintext into ciphertext. The ciphertext appears unreadable to unauthorized users. When the receiver obtains the encrypted message, the same secret key is used to decrypt the ciphertext and restore the original plaintext.

Symmetric encryption is popular because it is fast and efficient. It requires less computational power than asymmetric encryption, making it suitable for encrypting large amounts of data. For this reason, symmetric algorithms are commonly used in secure communication systems, virtual private networks, databases, and cloud storage services.

There are two main types of symmetric encryption algorithms: block ciphers and stream ciphers. Block ciphers encrypt data in fixed-size blocks, while stream ciphers encrypt data one bit or one byte at a time. Some of the most well-known symmetric encryption algorithms include AES, DES, and 3DES. Today, AES is considered the most secure and widely used standard for protecting sensitive information.

Despite their advantages, secret-key cryptosystems also have challenges. One of the main problems is key distribution. The secret key must be shared between communicating parties through a secure channel. If an attacker obtains the key, the confidentiality of the encrypted information is compromised. Therefore, effective key management is essential for maintaining a high level of security.

Secret-key cryptosystems play a crucial role in modern cybersecurity. They protect personal data, financial transactions, government information, and corporate communications. As cyber threats continue to evolve, the development and implementation of strong symmetric encryption algorithms remain an important aspect of information security.

Questions to the Text

1. What is another name for a secret-key cryptosystem?
2. How many keys are used in symmetric encryption?
3. What is the main purpose of a secret-key cryptosystem?
4. What happens to plaintext during the encryption process?
5. Why is ciphertext difficult for unauthorized users to read?
6. What key is used to decrypt the encrypted message?
7. Why is symmetric encryption considered efficient?

8. Where are symmetric encryption algorithms commonly used?
9. What are the two main types of symmetric encryption algorithms?
10. How do block ciphers differ from stream ciphers?
11. Which symmetric encryption standard is considered the most secure today?
12. What was the purpose of DES?
13. Why is key distribution a challenge in secret-key cryptosystems?
14. What can happen if an attacker obtains the secret key?
15. Why is key management important?
16. How do secret-key cryptosystems contribute to cybersecurity?
17. What types of information do these cryptosystems protect?
18. Why must communicating parties keep the key confidential?
19. What is the difference between plaintext and ciphertext?
20. Why will symmetric encryption remain important in the future?

***Exercise 5. Match the Words with their Meanings. Match the terms (1–10) with the definitions (A–J).**

1	Encryption	A. The original readable form of data.
2	Decryption	B. The process of converting ciphertext back into plaintext.
3	Secret key	C. A method of encrypting data block by block.
4	Plaintext	D. Protection of information from unauthorized access.
5	Ciphertext	E. The process of converting readable data into an unreadable form.
6	Block cipher	F. A cryptographic key known only to authorized parties.
7	Stream cipher	G. A method of trying all possible keys until the correct one is found.
8	Key management	H. The encrypted form of information.
9	Confidentiality	I. The administration and protection of cryptographic keys.
10	Brute-force attack	J. A method of encrypting data continuously, one bit or byte at a time.

***Exercise 6. Translation. Translate the following terms into Ukrainian.**

1. Secret-key cryptosystem – _____
2. Symmetric encryption – _____
3. Encryption algorithm – _____
4. Data confidentiality – _____
5. Cryptographic protocol – _____
6. Secure communication – _____
7. Access control – _____
8. Key exchange – _____
9. Network security – _____
10. Sensitive information – _____

***Exercise 7. Put the Words in the Correct Order. Make correct sentences.**

1. same / encryption / key / and / for / uses / decryption / the / symmetric / encryption
2. plaintext / ciphertext / transforms / encryption / into
3. information / confidentiality / protects / sensitive / of / encryption / the
4. cryptographic / a / uses / algorithm / encryption / process / the
5. secure / key / management / for / communication / is / important
6. data / encrypt / ciphers / in / blocks / fixed-size / block
7. secret / parties / must / the / authorized / keep / key
8. used / is / AES / widely / cybersecurity / in
9. obtain / attackers / key / the / should / not / secret
10. communication / secure / cryptosystems / support / secret-key

Exercise 8. Read the text and answer the questions.

Text: Public-Key Cryptosystems

Public-key cryptosystems, also known as asymmetric cryptosystems, are an essential part of modern information security. Unlike symmetric cryptosystems, which use the same key for encryption and decryption, public-key cryptosystems use two different but mathematically related keys: a public key and a private key.

The public key can be freely distributed and shared with anyone. It is used to encrypt information or verify a digital signature. The private key, on the other hand, is kept secret and is used to decrypt information or create a digital signature. This separation of keys increases security and eliminates the need to exchange secret keys through secure channels.

When a sender wants to send a confidential message, the message is encrypted using the recipient's public key. Once encrypted, the message becomes ciphertext and can only be decrypted using the recipient's private key. Even if an attacker intercepts the ciphertext, the information remains protected because the private key is not publicly available.

Public-key cryptography also supports digital signatures. A digital signature is created using the sender's private key and can be verified using the corresponding public key. Digital signatures provide authentication, integrity, and non-repudiation. They allow the recipient to verify the sender's identity and ensure that the message has not been altered during transmission.

One of the most widely known public-key algorithms is RSA. Another important technology is Elliptic Curve Cryptography (ECC), which offers strong security with smaller key sizes. These algorithms are widely used in secure web browsing, electronic commerce, email protection, and online banking.

Public-key cryptosystems are often used together with symmetric encryption. In many secure communication protocols, asymmetric encryption is used to exchange keys securely, while symmetric encryption is used to encrypt large amounts of data efficiently. This combination provides both security and high performance.

Public Key Infrastructure (PKI) is an important framework that supports public-key cryptography. PKI uses digital certificates issued by Certificate Authorities (CAs) to verify the ownership of public keys. This helps users establish trust and communicate securely over the Internet.

Today, public-key cryptography plays a crucial role in cybersecurity. It protects sensitive information, secures online transactions, enables digital signatures, and supports authentication systems used worldwide.

Questions to the Text

1. What is another name for a public-key cryptosystem?
2. How many keys are used in asymmetric encryption?
3. What are the two keys called?
4. Which key can be shared publicly?
5. Which key must remain secret?
6. What is the public key used for?
7. What is the private key used for?
8. How does asymmetric encryption differ from symmetric encryption?
9. How is a confidential message encrypted?
10. Which key is required to decrypt the ciphertext?
11. Why is intercepted ciphertext usually safe from attackers?
12. What is a digital signature?
13. Which key is used to create a digital signature?
14. Which key is used to verify a digital signature?
15. What three security services do digital signatures provide?
16. What is the purpose of authentication?
17. What is non-repudiation?
18. What is RSA?
19. What is ECC?
20. Why is ECC considered efficient?
21. Where are public-key cryptosystems commonly used?
22. How are asymmetric and symmetric encryption often combined?
23. Why is symmetric encryption used after key exchange?
24. What does PKI stand for?
25. What is the role of a Certificate Authority?
26. What are digital certificates used for?
27. How does PKI help establish trust?
28. Why is public-key cryptography important for online banking?
29. What role does public-key cryptography play in cybersecurity?
30. What information and services are protected by public-key cryptosystems?

Exercise 9. Fill in the blanks with the correct term

Word Bank:

public key, private key, asymmetric encryption, digital signature, RSA, PKI,
--

certificate authority, ciphertext, authentication, integrity
--

1. _____ uses two different keys for encryption and decryption.
2. A message encrypted with a public key becomes _____.
3. The _____ must be kept secret by its owner.
4. The _____ can be distributed openly to anyone.
5. A _____ helps verify the sender's identity.
6. _____ ensures that a message has not been modified.
7. _____ confirms the identity of a user or system.
8. _____ is one of the most widely used public-key algorithms.
9. _____ stands for Public Key Infrastructure.
10. A _____ issues and manages digital certificates.

Exercise 10. Match the English Terms (1–10) with their Ukrainian Equivalents (A–J)

1	Public key	A. Цілісність
2	Private key	В. Пара ключів
3	Digital signature	С. Шифротекст
4	Authentication	Д. Автентифікація
5	Integrity	Е. Публічний ключ
6	Certificate Authority	Ф. Інфраструктура відкритих ключів
7	Public Key Infrastructure	Г. Центр сертифікації
8	Key pair	Н. Безпечний зв'язок
9	Secure communication	І. Цифровий підпис
10	Ciphertext	Ж. Приватний ключ

Exercise 11. Read the Texts Below. Match Choices (A–H) to Texts (1–5). There are three choices you do not need to use.

Text 1

This key can be shared openly with other users. It is commonly used to encrypt messages and verify digital signatures. Anyone can obtain this key without compromising the security of the system. In public-key cryptography, the public key is mathematically related to a private key. However, it is computationally infeasible to derive the private key from the public key. Public keys are often distributed through digital certificates.

Text 2

This key is known only to its owner. It is used to decrypt encrypted information and create digital signatures. The security of an asymmetric cryptosystem depends on keeping this key secret. If an attacker gains access to it, confidential information may be exposed. Private keys are usually stored in secure hardware devices or protected software environments. Users should never share this key with others.

Text 3

This technology allows users to confirm the authenticity of electronic documents and verify the sender's identity. It is created using a private key and verified using a public key. This technology helps ensure that a message has not been modified during transmission. It also provides non-repudiation, meaning that the sender cannot deny having signed the document. Digital signatures are widely used in e-commerce, online banking, and electronic document management systems.

Text 4

This organization issues digital certificates and helps establish trust between users communicating over the Internet. It verifies the identity of individuals, organizations, and websites before issuing certificates. These certificates link a public key to a specific entity. Browsers and operating systems rely on trusted authorities to validate secure connections. Without such organizations, users would have difficulty determining whether a public key truly belongs to the claimed owner.

Text 5

This cryptographic algorithm is widely used for secure data transmission and is based on mathematical operations involving large prime numbers. It was developed in 1977 and remains one of the most well-known public-key algorithms. The algorithm supports both encryption and digital signatures. Its security relies on the difficulty of factoring very large integers. RSA is commonly used in secure email systems, digital certificates, and Internet security protocols.

Choices

- A. RSA Algorithm
- B. Public Key
- C. Data Breach
- D. Digital Signature
- E. Certificate Authority
- F. Symmetric Encryption
- G. Private Key
- H. Firewall

***Exercise 12. Read the text and answer the questions.**

Text: Cryptographic Protocols

Cryptographic protocols are sets of rules that define how secure communication is performed between two or more parties. They use cryptographic algorithms to ensure confidentiality, integrity, and authentication of data transmitted over insecure networks such as the Internet.

One of the main purposes of cryptographic protocols is to establish a secure communication channel between users who may have never interacted before. To achieve this, protocols often begin with a process called a handshake, during which the participants agree on encryption methods and exchange cryptographic keys.

Modern protocols, such as TLS (Transport Layer Security), are widely used to protect online communication. TLS ensures that data transmitted between a client and a server remains encrypted and cannot be read or modified by attackers. It also provides authentication, allowing users to verify the identity of the server they are connecting to.

Cryptographic protocols rely heavily on key exchange mechanisms. During key exchange, parties securely generate or share a session key that will be used for symmetric encryption. This approach combines the efficiency of symmetric encryption with the security of asymmetric methods used during the exchange process.

Another important feature of cryptographic protocols is the use of digital certificates issued by Certificate Authorities (CAs). These certificates help verify the identity of users, websites, and servers. This prevents attacks such as man-in-the-middle, where an attacker tries to intercept or modify communication between two parties.

Security protocols also include mechanisms for detecting tampering and ensuring message integrity. Hash functions and message authentication codes (MACs) are commonly used to verify that data has not been altered during transmission.

Despite their effectiveness, cryptographic protocols can still be vulnerable if they are poorly designed or incorrectly implemented. Common attacks include replay attacks, protocol manipulation, and exploitation of weak encryption settings.

Overall, cryptographic protocols play a crucial role in cybersecurity. They are used in secure web browsing, online banking, email communication, and many other applications that require safe and reliable data exchange.

Questions to the Text

1. What are cryptographic protocols?
2. What is the main purpose of cryptographic protocols?
3. What does a handshake process do in a protocol?
4. Which protocol is most commonly used for secure Internet communication?
5. What does TLS protect during communication?
6. Why is authentication important in cryptographic protocols?
7. What is a secure communication channel?
8. How is a session key used in protocols?
9. What is key exchange?
10. Why are asymmetric and symmetric encryption often combined?
11. What role do Certificate Authorities play?
12. What are digital certificates used for?
13. What is a man-in-the-middle attack?
14. How do protocols protect against interception?
15. What is message integrity?
16. How do hash functions help in security protocols?

17. What is a MAC (Message Authentication Code)?
18. What can happen if a protocol is poorly designed?
19. What is a replay attack?
20. Where are cryptographic protocols commonly used?

***Exercise 13. Fill in the Gaps**

Word bank:

TLS, authentication, handshake, encryption, decryption, session key, key exchange, certificate authority, digital certificate, integrity, confidentiality, man-in-the-middle, hash function, MAC, secure channel

1. _____ ensures that data cannot be read by unauthorized users.
2. _____ is the process of converting ciphertext back into plaintext.
3. _____ is used to establish a secure connection between two parties.
4. _____ guarantees that data has not been modified during transmission.
5. _____ confirms the identity of a user or system.
6. _____ is a temporary key used for secure communication sessions.
7. _____ is a process of securely sharing cryptographic keys.
8. _____ is an organization that issues digital certificates.
9. A _____ is used to verify the identity of a website or user.
10. A _____ attack intercepts communication between two parties.
11. _____ protects data during transmission over the Internet.
12. A _____ is a cryptographic tool used to verify data integrity.
13. _____ ensures that information remains secret from unauthorized users.
14. A _____ is used to check whether a message has been altered.
15. A _____ provides a protected communication path between systems.

***Exercise 14. Multiple Choice**

1. What is the main purpose of a cryptographic protocol?

- A. Store data permanently
- B. Secure communication between parties
- C. Increase internet speed
- D. Delete encrypted data

2. What does TLS stand for?

- A. Total Link System
- B. Transport Layer Security
- C. Transfer Logic Service
- D. Trusted Login System

3. What is encryption?

- A. Deleting data
- B. Converting plaintext into ciphertext
- C. Copying files
- D. Compressing files

4.What is decryption?

- A. Converting ciphertext into plaintext
- B. Encrypting files
- C. Breaking passwords
- D. Sending emails

5.What is a handshake in cryptography?

- A. A greeting message
- B. A process of establishing a secure connection
- C. A type of malware
- D. A file format

6.What is a session key used for?

- A. Long-term storage
- B. Single communication session encryption
- C. Deleting data
- D. Password recovery

7.What does a Certificate Authority do?

- A. Deletes viruses
- B. Issues digital certificates
- C. Stores passwords
- D. Encrypts messages

8.What is a digital certificate used for?

- A. Increasing speed
- B. Verifying identity
- C. Compressing files
- D. Blocking websites

9.What is a man-in-the-middle attack?

- A. Software update
- B. Interception of communication
- C. Antivirus tool
- D. Encryption method

10.What ensures data integrity?

- A. Hash function
- B. Keyboard
- C. Browser
- D. Monitor

11.What does authentication do?

- A. Deletes files
- B. Verifies identity
- C. Encrypts data
- D. Compresses data

12.What is a MAC?

- A. Message Authentication Code
- B. Machine Access Control

- C. Mobile Application Code
- D. Memory Allocation Code

13. What is confidentiality?

- A. Data visibility to everyone
- B. Protection from unauthorized access
- C. Data deletion
- D. File backup

14. What is a secure channel?

- A. Unsafe network
- B. Protected communication path
- C. Open Wi-Fi
- D. Public website

15. What is key exchange?

- A. Sharing files
- B. Securely sharing encryption keys
- C. Deleting keys
- D. Creating passwords

***Exercise 15. True / False. Write T (True) or F (False).**

1. TLS is used to secure Internet communication.
2. Encryption converts ciphertext into plaintext.
3. Authentication verifies the identity of a user.
4. A session key is used for long-term encryption only.
5. A certificate authority issues digital certificates.
6. A man-in-the-middle attack is a type of secure protocol.
7. Integrity ensures data is not modified during transmission.
8. A handshake helps establish a secure connection.
9. A hash function is used to compress images only.
10. Confidentiality means data is kept secret from unauthorized users.
11. MAC is used to verify message integrity.
12. Decryption makes data unreadable.
13. Digital certificates help verify identity.
14. A secure channel protects transmitted data.
15. Key exchange is used to destroy encryption keys.

Exercise 16. Read the text and answer the questions.

Text: Digital Steganography

Digital steganography is a technique used to hide secret information inside digital media such as images, audio files, video files, or text documents. Unlike cryptography, which focuses on making data unreadable, steganography focuses on hiding the existence of the data itself.

In a typical steganographic system, a secret message (payload) is embedded into a cover file using a special embedding algorithm. The result is called a stego file,

which appears normal to users who do not know that hidden information exists inside it. This makes steganography a powerful tool for covert communication.

One of the most common techniques used in digital steganography is the Least Significant Bit (LSB) method. This method modifies the smallest bits of digital data in an image or audio file, so the changes are not noticeable to the human eye or ear. As a result, the cover file retains its original appearance or sound while carrying hidden information.

Digital steganography is widely used in image, audio, and video files. Image steganography hides data inside pixels of pictures, while audio steganography embeds information in sound signals. Video steganography combines both methods and can hide large amounts of data in multimedia content.

Security in steganography is based on imperceptibility and detection resistance. The main goal is to ensure that no one suspects the presence of hidden data. However, attackers may use steganalysis techniques to detect or extract hidden messages from stego files.

Another important concept is the stego key, which controls the embedding and extraction process. Without the correct key, it is difficult to recover the hidden message even if the steganographic method is known.

Digital steganography is often combined with cryptography for higher security. First, the message is encrypted, and then it is hidden inside a cover file. This double protection ensures both confidentiality and secrecy of communication.

Today, steganography is used in digital watermarking, secure communication, and data protection systems. It is also studied in cybersecurity for both defensive and offensive purposes.

Questions to the Text

1. What is digital steganography?
2. How is steganography different from cryptography?
3. What is a payload in steganography?
4. What is a cover file?
5. What is a stego file?
6. How is a hidden message embedded into a file?
7. What is the Least Significant Bit (LSB) method?
8. Why are changes in LSB usually not noticeable?
9. In which types of media can steganography be used?
10. What is image steganography?
11. What is audio steganography?
12. What is video steganography?
13. What is the main goal of steganography security?
14. What is steganalysis?
15. What is a stego key used for?
16. Why is steganography often combined with cryptography?
17. What happens before data is hidden in secure systems?

18. What is digital watermarking?
19. Where is steganography used today?
20. Why is steganography important in cybersecurity?

Exercise 17. Correct the Mistakes. Find and correct the mistake in each sentence.

1. Steganography makes data readable instead of hiding it.
2. A cover file is the hidden message inside the system.
3. The payload is the file that carries hidden information.
4. LSB method changes the most significant bits of data.
5. A stego file looks suspicious to users.
6. Cryptography focuses on hiding the existence of data.
7. Steganalysis is used to create hidden messages.
8. A stego key is not used in steganography systems.
9. Audio steganography hides data in images only.
10. Video steganography cannot store large amounts of data.
11. Imperceptibility means the hidden data is easily visible.
12. Steganography is never used with cryptography.
13. A hidden message is called a cover file.
14. LSB method modifies large parts of digital data.
15. Steganography is used only for illegal activities.

Exercise 18. Translate the Sentences. Translate into Ukrainian.

1. Digital steganography hides information inside digital media.
2. A stego file looks like a normal image or audio file.
3. The payload contains the secret message.
4. The cover file carries hidden data.
5. LSB method modifies the smallest bits of data.
6. Steganalysis is used to detect hidden information.
7. Audio steganography hides messages in sound files.
8. Video steganography combines image and audio techniques.
9. Imperceptibility is a key feature of steganography.
10. Robustness means resistance to attacks.
11. Capacity defines how much data can be hidden.
12. Stego key controls embedding and extraction.
13. Cryptography is often combined with steganography.
14. A hidden communication channel is difficult to detect.
15. Digital watermarking is a form of steganography.

Exercise 19: Modern Cybersecurity & Cryptography

Read the text below. For questions (1–10) choose the correct answer (A, B, C or D).

DIGITAL SECURITY SYSTEMS

In today's digital world, organizations depend on secure communication systems to protect sensitive information. As cyber threats continue to grow, (1) _____ plays a key role in ensuring the safety of data and networks.

One of the main foundations of secure communication is (2) _____, which hides information by converting it into unreadable form for unauthorized users. In more advanced systems, (3) _____ is used, where two different but related keys are applied for encryption and decryption.

To verify identity and ensure trust between users, systems rely on (4) _____, which confirms that a message or user is authentic. Many secure systems also use (5) _____ to ensure that transmitted data has not been altered during communication.

Modern applications often include (6) _____ to provide a secure communication channel over public networks, especially for remote users connecting to company systems.

Another important technology is (7) _____, which is responsible for detecting suspicious activity and monitoring system behavior in real time. When threats are detected, administrators may use (8) _____ to fix system vulnerabilities and improve protection.

To control system usage, organizations implement (9) _____, which determines who can access specific resources and under what conditions. Finally, all these technologies together support (10) _____, ensuring that data, systems, and communication remain safe from cyberattacks.

Answers:

No.	A	B	C	D
1	Cybersecurity	Encryption	Firewall	Malware
2	Encryption	Network	Password	Database
3	Asymmetric encryption	Firewall	VPN	Virus
4	Authentication	Encryption	Steganography	Compression
5	Integrity	Malware	Traffic	Database
6	VPN	Antivirus	IDS	Patch
7	Network monitoring	Password attack	Encryption key	Firewall rule
8	Patch management	Data loss	Stego file	Traffic load
9	Access control	Malware	Encryption key	Network speed
10	Information security	Virus attack	Database error	Password reuse

Exercise 20 Listening. Listen to the recording and complete the notes below.

Text

Cryptography is a method used to protect information by converting it into an unreadable form called ciphertext. To access the original message, a special key is required for decryption. There are two main types of cryptography: symmetric encryption, which uses one shared key, and asymmetric encryption, which uses a public key and a private key.

Steganography is a different technique. Instead of making information unreadable, it hides the existence of the message inside digital files such as images, audio, or video. The hidden message cannot be seen without special knowledge or tools.

In modern cybersecurity, both methods are often combined. First, the message is encrypted using cryptography. Then, it is hidden inside another file using steganography. This provides an extra layer of security.

Cryptography

- Purpose: to make information _____ (1)
- Encrypted data is called _____ (2)
- Symmetric encryption uses _____ key (3)
- Asymmetric encryption uses public and _____ key (4)

Steganography

- Purpose: to hide _____ of a message (5)
- Hidden data is placed inside digital _____ (6)
- Examples include images, audio, and _____ files (7)

Combined methods

- First step: _____ the message (8)
- Second step: hide it using steganography for extra _____ (9)

Exercise 21 Video.

Part A: Watch the videos in the section “Introduction to Cryptography”

<https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/intro-to-cryptography> and answer the questions.

Cryptography Basics

1. What is cryptography used for?
2. What is plaintext?
3. What is ciphertext?

Encryption Types

4. What is the difference between symmetric and asymmetric encryption?
5. How many keys are used in symmetric encryption?
6. What keys are used in asymmetric encryption?

Security Concept

7. Why is encryption important in communication?
8. What problem does cryptography solve?

Real-world use

9. Where is cryptography used in real life? (name 2 examples)
10. Why must encryption keys be kept secure?

*** Part B: Watch the video: <https://www.youtube.com/watch?v=Kf9KjCKmDcU> and answer the questions below:**

Basic Understanding

1. What is cryptography mainly used for?
2. What does encryption do to information?
3. What must someone have to decode a message?

Key Concepts

4. What is the role of a key in encryption?
5. Why is encrypted data safe during transmission?
6. What happens if the key is incorrect?

Application

7. Where is cryptography used in real life? (name one example)
8. Why is encryption important for online communication?

Higher Thinking

9. What problem does cryptography solve in digital communication?
10. How does cryptography help protect privacy?

FINAL TEST UNIT 6

Part I. Multiple Choice

Choose the correct answer (A, B, C or D).

1. What is the main goal of cryptography?
 - A. Hide the existence of data
 - B. Protect information from unauthorized access
 - C. Delete files automatically
 - D. Increase network speed
2. What is encryption?
 - A. Converting ciphertext into plaintext
 - B. Converting plaintext into ciphertext
 - C. Copying files
 - D. Compressing data

3. What is decryption?
 - A. Hiding data
 - B. Breaking networks
 - C. Converting ciphertext into plaintext
 - D. Deleting messages
4. What is a secret key used for?
 - A. Only encryption
 - B. Only decryption
 - C. Both encryption and decryption
 - D. File storage
5. What is asymmetric encryption?
 - A. One key system
 - B. Two-key system
 - C. No-key system
 - D. Random key system
6. What is a public key?
 - A. A secret key
 - B. A key used only for decryption
 - C. A key that can be shared openly
 - D. A hardware device
7. What is a private key?
 - A. A shared key
 - B. A secret key used by the owner
 - C. A public password
 - D. A network protocol
8. What is a digital signature used for?
 - A. File compression
 - B. Authentication and integrity
 - C. Increasing speed
 - D. Data deletion
9. What is steganography?
 - A. Encrypting data
 - B. Hiding the existence of data
 - C. Deleting files
 - D. Copying networks
10. What is a payload in steganography?
 - A. A network
 - B. Hidden message
 - C. Firewall
 - D. Virus
11. What is a cover file?
 - A. A file that contains hidden data
 - B. A virus file

- C. A password file
 - D. A system update
12. What is a stego file?
- A. A corrupted file
 - B. A file with hidden data
 - C. A backup file
 - D. A network file
13. What does LSB stand for?
- A. Least Significant Bit
 - B. Large System Backup
 - C. Low Security Block
 - D. Logical Signal Base
14. What is steganalysis?
- A. Creating hidden messages
 - B. Detecting hidden data
 - C. Encrypting files
 - D. Compressing images
15. What is TLS used for?
- A. File deletion
 - B. Secure communication over networks
 - C. Password generation
 - D. Data storage
16. What is a handshake in cryptography?
- A. File transfer
 - B. Establishing a secure connection
 - C. Data compression
 - D. Virus scan
17. What is a session key?
- A. Permanent key
 - B. Temporary encryption key
 - C. Public key
 - D. Password
18. What does integrity mean?
- A. Data is readable
 - B. Data is unchanged
 - C. Data is deleted
 - D. Data is copied
19. What is a man-in-the-middle attack?
- A. Secure protocol
 - B. Interception of communication
 - C. Encryption method
 - D. Firewall type

20. What is PKI?

- A. Public Key Infrastructure
- B. Private Key Internet
- C. Protocol Key Interface
- D. Protected Knowledge Index

Part II. Fill in the Gaps

Use the word bank:

encryption, decryption, steganography, payload, cover file, stego file, public key, private key, authentication, integrity, TLS, VPN, LSB, hash function, digital signature

1. _____ converts plaintext into ciphertext.
2. _____ converts ciphertext into plaintext.
3. _____ hides the existence of data.
4. A _____ contains hidden information.
5. A _____ is the original file used for hiding data.
6. A _____ is the final file with hidden data.
7. A _____ can be shared openly.
8. A _____ must remain secret.
9. _____ verifies the identity of a user or system.
10. _____ ensures data is not changed.
11. _____ secures communication over the Internet.
12. _____ provides a secure connection for remote users.
13. _____ is the smallest bit modification method.
14. A _____ helps verify data integrity.
15. A _____ confirms message authenticity.

Part III. True / False

Write **T (True)** or **F (False)**.

1. Cryptography hides the existence of data.
2. Steganography hides the existence of data.
3. Encryption makes data readable.
4. Decryption restores original data.
5. A public key must be kept secret.
6. A private key is secret.
7. LSB modifies the least significant bits.
8. Stego file looks normal.
9. Steganalysis creates hidden data.
10. TLS protects online communication.
11. VPN creates a secure tunnel.
12. Integrity means data is unchanged.
13. A digital signature provides authentication.
14. A payload is a type of firewall.
15. PKI manages digital certificates.



Unit 7

Introduction to Digital Forensics and Cyber Investigations

Text 1. Digital Forensics and Combating Cybercrime in Information Systems

Text 5. Fundamental Principles of Combating Cybercrime and Law Enforcement Tools in Cyberspace

Text 3. Electronic (Digital) Evidence

Text 4. Process of Initial Digital Forensic Investigations

Physical HDD, File Systems & Logical Structure

Text 5. Data Acquisition and Imaging in Digital Forensics

Techniques for Obstructing Digital Investigations

Text 6. The Digital Footprints Inside an OS

Text 7. Introduction to Network Forensics

Text 8. Web Application Forensics

Glossary

Digital forensics — цифрова криміналістика
Cybercrime — кіберзлочинність
Information system — інформаційна система
Evidence — доказ
Digital evidence — цифрові докази
Incident response — реагування на інциденти
Cyber investigation — кіберрозслідування
Data recovery — відновлення даних
File system — файлова система
Metadata — метадані
Log file — журнал подій
Chain of custody — ланцюг збереження доказів
Forensic analysis — криміналістичний аналіз
Malware analysis — аналіз шкідливого ПЗ
Intrusion detection — виявлення вторгнень
Unauthorized access — несанкціонований доступ
Encryption — шифрування
Data breach — витік даних
System compromise — компрометація системи
Network traffic analysis — аналіз мережевого трафіку
Firewall logs — журнали брандмауера
Disk imaging — створення образу диска
Hash value — хеш-значення
Cybersecurity tools — інструменти кібербезпеки
Evidence preservation — збереження доказів
Malicious activity — шкідлива активність
Digital artifact — цифровий артефакт
Security breach — порушення безпеки
Root cause analysis — аналіз першопричини
Attack vector — вектор атаки
System logs — системні журнали
Cyber defense — кіберзахист
Threat actor — зловмисник
Phishing attack — фішинг-атака
Ransomware — програма-вимагач
Endpoint security — захист кінцевих пристроїв
Forensic toolkit — набір криміналістичних інструментів
Data integrity — цілісність даних
Security audit — аудит безпеки

Digital Forensics and Combating Cybercrime in Information Systems

Digital forensics is a key area of modern cybersecurity that focuses on the identification, preservation, analysis, and presentation of digital evidence. It plays an essential role in combating cybercrime and investigating security incidents in information systems.

When a cyber incident occurs, forensic specialists begin by collecting digital evidence from computers, servers, mobile devices, and network systems. This evidence may include files, log files, metadata, and network traffic data. One of the most important principles in digital forensics is maintaining the chain of custody to ensure that evidence remains authentic and legally admissible.

Forensic analysis involves examining system artifacts such as deleted files, system logs, and disk images. Tools for data recovery are often used to restore lost or deleted information. Investigators also perform malware analysis to understand how malicious software infected the system and what damage it caused.

Network traffic analysis is another important technique used in cyber investigations. It helps experts identify attack vectors, unauthorized access attempts, and suspicious communication patterns. Firewall logs and intrusion detection systems provide additional information about malicious activity.

Cybercrime includes a wide range of illegal activities such as phishing attacks, ransomware distribution, identity theft, and data breaches. To combat these threats, organizations use cybersecurity tools, endpoint security systems, and continuous monitoring of their information systems.

Incident response teams play a crucial role in minimizing damage after a security breach. They perform root cause analysis to determine how the attack occurred and implement measures to prevent similar incidents in the future. Security audits and digital investigations help strengthen overall cyber defense strategies.

Digital forensics is not only used for solving cybercrimes but also for supporting legal proceedings. Properly collected and analyzed digital evidence can be presented in court to identify threat actors and prove malicious activity.

As cyber threats continue to evolve, digital forensics remains a vital discipline for protecting information systems and ensuring justice in the digital world.

Questions to the Text

1. What is digital forensics?
2. What is the main purpose of digital forensics?
3. What types of evidence are collected in cyber investigations?
4. Why is the chain of custody important?
5. What is forensic analysis?
6. What is data recovery used for?
7. What is analyzed during malware analysis?
8. What is network traffic analysis used for?

9. What information do firewall logs provide?
10. What is an attack vector?
11. What is cybercrime?
12. Name three examples of cybercrime mentioned in the text.
13. What is a phishing attack?
14. What is ransomware?
15. What is endpoint security?
16. What is incident response?
17. What is root cause analysis?
18. Why are security audits important?
19. How is digital forensics used in court?
20. Why is digital forensics important in modern cybersecurity?

Exercise 1. Multiple Choice. Choose the correct answer (A, B, C or D).

1. What is digital forensics?
 - A. Data encryption method
 - B. Investigation of digital evidence
 - C. Antivirus software
 - D. Network design
2. What is cybercrime?
 - A. Legal online activity
 - B. Illegal activity using computers
 - C. Software update
 - D. Data backup
3. What is digital evidence?
 - A. Printed documents
 - B. Evidence stored electronically
 - C. Hardware only
 - D. Internet speed
4. What is chain of custody?
 - A. File compression method
 - B. Process of preserving evidence integrity
 - C. Password system
 - D. Encryption algorithm
5. What is malware analysis?
 - A. Software development
 - B. Study of malicious software
 - C. Network installation
 - D. Data deletion
6. What is data recovery?
 - A. Deleting files
 - B. Restoring lost data

- C. Encrypting files
 - D. Blocking websites
7. What is network traffic analysis used for?
 - A. Designing websites
 - B. Monitoring data flow and detecting attacks
 - C. Printing documents
 - D. Increasing storage
 8. What is a firewall log?
 - A. Game file
 - B. Record of network activity
 - C. Antivirus program
 - D. Image file
 9. What is ransomware?
 - A. Backup tool
 - B. Malicious software that demands payment
 - C. Browser extension
 - D. Encryption key
 10. What is phishing?
 - A. Network upgrade
 - B. Fraudulent attempt to steal data
 - C. Antivirus scan
 - D. File transfer
 11. What is incident response?
 - A. Software design
 - B. Reaction to cyber attacks
 - C. Data compression
 - D. File creation
 12. What is root cause analysis?
 - A. Increasing speed
 - B. Finding the reason of an incident
 - C. Encrypting files
 - D. Blocking users
 13. What is endpoint security?
 - A. Protection of devices like laptops and phones
 - B. Internet speed control
 - C. File storage
 - D. Email service
 14. What is a security audit?
 - A. System cleaning
 - B. Evaluation of security systems
 - C. Password reset
 - D. File deletion

15. What is a threat actor?
- A. System administrator
 - B. Person who causes cyber attacks
 - C. Software update
 - D. Firewall system

Exercise 2. True / False. Write **T (True)** or **F (False)**.

1. Digital forensics studies physical documents only.
2. Cybercrime involves illegal activities using computers.
3. Digital evidence can include log files and metadata.
4. Chain of custody ensures evidence is protected and unchanged.
5. Malware analysis studies hardware performance.
6. Data recovery restores lost or deleted files.
7. Network traffic analysis detects suspicious activity.
8. Firewall logs show network events.
9. Ransomware steals passwords only.
10. Phishing is a type of cyber attack.
11. Incident response happens before an attack.
12. Root cause analysis finds why an incident happened.
13. Endpoint security protects devices like smartphones.
14. Security audits reduce system protection.
15. Digital forensics is used in legal investigations.

Exercise 3. Fill in the Blanks

Word bank:

digital forensics, cybercrime, evidence, chain of custody, malware analysis, data recovery, network traffic analysis, firewall logs, ransomware, phishing, incident response, root cause analysis, endpoint security, security audit, digital evidence

1. _____ is the investigation of digital information in cyber incidents.
2. _____ refers to illegal activities using computers.
3. _____ is information used in investigations or court cases.
4. _____ ensures evidence is properly preserved and documented.
5. _____ studies malicious software behavior.
6. _____ restores lost or deleted information.
7. _____ monitors data flow in a network.
8. _____ record network activities and events.
9. _____ is malware that encrypts files and demands payment.
10. _____ is a fraudulent attempt to steal sensitive data.
11. _____ is the process of reacting to security incidents.
12. _____ identifies the cause of a cyber incident.
13. _____ protects devices like computers and mobile phones.
14. _____ evaluates the security of a system.

15. _____ must be collected carefully in investigations.

Exercise 4. Read the text and answer the questions.

Text: Fundamental Principles of Combating Cybercrime and Law Enforcement Tools in Cyberspace

The rapid development of digital technologies has led to an increase in cybercrime, making effective countermeasures a priority for governments and law enforcement agencies. Combating cybercrime requires a combination of legal, technical, and organizational approaches aimed at protecting information systems and ensuring public safety in cyberspace.

One of the fundamental principles of cybercrime prevention is legality, which means that all investigative actions must be carried out in accordance with national and international laws. Another key principle is respect for human rights and privacy, ensuring that investigations do not violate fundamental freedoms while collecting digital evidence.

A third important principle is cooperation. Cybercrime often crosses national borders, so police agencies, cybersecurity organizations, and international institutions must work together. Information sharing between countries and agencies plays a crucial role in identifying and stopping cybercriminals.

Law enforcement agencies use a wide range of cyber tools and technologies to investigate digital crimes. One of the most important tools is digital forensics software, which helps collect and analyze electronic evidence from computers, mobile devices, and cloud systems.

Another important instrument is network monitoring systems, which allow police to analyze traffic and detect suspicious activity in real time. These systems help identify attack sources, malware distribution, and unauthorized access attempts.

Police also use intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor and block malicious activities. In addition, data recovery tools are used to restore deleted or hidden information that may serve as evidence in investigations.

Modern cyber police units also rely on artificial intelligence and machine learning systems to detect patterns of cybercrime, identify fraud, and predict potential attacks. These technologies improve the speed and accuracy of investigations.

Finally, international cooperation platforms such as INTERPOL and Europol cyber units play an essential role in coordinating global efforts against cybercrime. Through joint operations, training programs, and intelligence sharing, law enforcement agencies strengthen global cyber defense.

Overall, combating cybercrime requires strict adherence to legal principles and the effective use of advanced technological tools. Together, these measures help protect individuals, organizations, and governments from growing cyber threats.

Questions to the Text

1. What are the main goals of combating cybercrime?
2. What does the principle of legality mean in cyber investigations?
3. Why is respect for privacy important in cybercrime investigations?
4. What is the role of cooperation in combating cybercrime?
5. Why is international cooperation necessary in cybercrime cases?
6. What is digital forensics software used for?
7. What types of devices can be analyzed using forensic tools?
8. What is the purpose of network monitoring systems?
9. What types of threats can network monitoring detect?
10. What are IDS and IPS used for?
11. What is the difference between IDS and IPS (according to context)?
12. What are data recovery tools used for?
13. How is artificial intelligence used in cybercrime investigations?
14. What organizations support international cybercrime prevention?
15. What is the role of Europol and INTERPOL in cybersecurity?
16. Why is technology important in modern policing?
17. What challenges make cybercrime difficult to combat?
18. How do law enforcement agencies collect digital evidence?
19. What is the benefit of information sharing between countries?
20. Why is a combined legal and technological approach necessary in cyberspace?

***Exercise 5. Error Correction. Find the mistake in each sentence and correct it.**

1. Cybercrime prevention ignores legal rules.
2. Legality means breaking national laws during investigations.
3. Privacy violations are encouraged in cyber investigations.
4. Cooperation is not needed in cybercrime cases.
5. Cybercrime always stays within one country.
6. Digital forensics software destroys electronic evidence.
7. Network monitoring hides suspicious activity.
8. IDS and IPS are used to encourage cyberattacks.
9. Data recovery tools permanently delete information.
10. Artificial intelligence is never used in cyber investigations.
11. Europol and INTERPOL work independently without cooperation.
12. Cyber police do not use technology tools.
13. Law enforcement ignores digital evidence.
14. Cybercrime can be investigated without legal principles.
15. International cooperation has no role in cybersecurity.

***Exercise 6. Match the English Terms (1–18) with their Ukrainian Equivalents (A–R)**

1	Cybercrime	A. Кіберзлочинність
2	Cybersecurity	B. Кібербезпека
3	Legality	C. Законність

4	Privacy	D. Приватність
5	Cooperation	E. Співпраця
6	Digital forensics	F. Цифрова криміналістика
7	Network monitoring	G. Моніторинг мережі
8	Intrusion detection system (IDS)	H. Система виявлення вторгнень
9	Intrusion prevention system (IPS)	I. Система запобігання вторгненням
10	Data recovery	J. Відновлення даних
11	Artificial intelligence	K. Штучний інтелект
12	Machine learning	L. Машинне навчання
13	Digital evidence	M. Цифрові докази
14	Law enforcement	N. Правоохоронні органи
15	Cyber investigation	O. Кіберрозслідування
16	Information sharing	P. Обмін інформацією
17	Cyber threat	Q. Кіберзагроза
18	International cooperation	R. Міжнародна співпраця

***Exercise 7. Read the text and answer the questions.**

Text: Electronic (Digital) Evidence

Electronic or digital evidence refers to any information stored or transmitted in digital form that can be used in a court of law. It plays a crucial role in modern criminal investigations, especially in cases involving cybercrime, fraud, data breaches, and other technology-related offenses.

Digital evidence can exist in many forms, including emails, text messages, documents, images, videos, system logs, metadata, and records from cloud services. It can also include data collected from mobile devices, computers, servers, and network equipment. Because of its variety, electronic evidence is often complex and requires special methods for collection and analysis.

One of the key principles in handling digital evidence is **preservation of integrity**. This means that the evidence must not be changed or damaged during collection, storage, or analysis. Investigators often use tools such as disk imaging and hashing algorithms to ensure that original data remains unchanged.

Another important concept is the **chain of custody**, which documents every step of evidence handling. It records who collected the evidence, when it was collected, how it was stored, and who accessed it. Maintaining a clear chain of custody is essential for ensuring that digital evidence is admissible in court.

Law enforcement agencies use **digital forensic techniques** to extract and analyze electronic evidence. These techniques help recover deleted files, examine hidden data, and reconstruct user activity. Network analysis and log file examination are also commonly used to track suspicious behavior and identify attackers.

However, digital evidence also presents challenges. It can be easily modified, deleted, or encrypted by attackers. In addition, large volumes of data make analysis

time-consuming and technically demanding. Cross-border data storage in cloud systems can also complicate investigations.

Despite these challenges, electronic evidence remains one of the most powerful tools in modern justice systems. It helps investigators prove criminal activity, identify suspects, and support legal proceedings in both national and international cases.

Questions to the Text

1. What is electronic (digital) evidence?
2. In what types of cases is digital evidence commonly used?
3. What are some examples of digital evidence?
4. Why is digital evidence considered complex?
5. What does preservation of integrity mean?
6. Why is hashing used in digital investigations?
7. What is the chain of custody?
8. Why is chain of custody important in court?
9. What do forensic investigators do with digital evidence?
10. What types of data can be recovered during investigations?
11. How is network analysis used in digital forensics?
12. What challenges are associated with digital evidence?
13. Why can digital evidence be easily manipulated?
14. How does cloud storage complicate investigations?
15. What makes digital evidence powerful in legal systems?
16. How does digital evidence help identify suspects?
17. Why is large data volume a problem in investigations?
18. What tools are used to ensure evidence integrity?
19. Can digital evidence be used in international cases? Why?
20. What is the overall importance of electronic evidence in modern justice systems?

Exercise 8. Fill in the Blanks

Word bank:

digital evidence, chain of custody, integrity, hashing, disk imaging, metadata, cloud storage, forensic analysis, deleted files, log files, cybercrime, court, investigation, encryption, network analysis

1. _____ is information stored in digital form that can be used in legal cases.
2. _____ ensures that evidence is properly documented and tracked.
3. _____ means that data has not been altered.
4. _____ is used to verify that evidence has not been changed.
5. _____ creates an exact copy of a storage device.
6. _____ contains information about data such as time and author.
7. _____ allows storing data on remote servers over the Internet.

8. _____ is the scientific examination of digital information.
9. _____ are files that have been removed from a system.
10. _____ record system or network events.
11. _____ refers to illegal activities using computers.
12. Evidence must be presented in _____ to be legally valid.
13. A digital _____ collects facts during a cyber incident.
14. _____ protects data by converting it into unreadable form.
15. _____ is used to examine communication traffic in networks.

Exercise 9. Find the mistake and correct it.

1. Digital evidence is always physical paper documents.
2. Chain of custody is not important in investigations.
3. Integrity means that data has been changed during analysis.
4. Hashing is used to modify digital evidence.
5. Disk imaging destroys original data.
6. Metadata contains information about file content only.
7. Cloud storage means data is stored locally only.
8. Forensic analysis is used to create cybercrime.
9. Deleted files cannot be recovered in any case.
10. Log files hide system activity from investigators.
11. Cybercrime is legal online activity.
12. Network analysis is used to ignore traffic data.
13. Encryption makes data easier to read.
14. Courts do not accept digital evidence.
15. Digital evidence is useless in investigations.

Exercise 10. Match the English Terms (1–18) with Ukrainian Equivalents (A–R)

1	Digital evidence	A. Цифрова криміналістика
2	Chain of custody	B. Цифрові докази
3	Integrity	C. Ланцюг збереження доказів
4	Hashing	C. Цілісність
5	Disk imaging	D. Хешування
6	Metadata	E. Створення образу диска
7	Cloud storage	F. Метадані
8	Forensic analysis	G. Хмарне зберігання
9	Deleted files	H. Криміналістичний аналіз
10	Log files	I. Видалені файли
11	Cybercrime	J. Журнали подій
12	Investigation	K. Кіберзлочинність
13	Court	L. Розслідування
14	Encryption	M. Суд
15	Network analysis	N. Шифрування
16	Data recovery	O. Аналіз мережі

17	Security breach	Р. Відновлення даних
18	Digital forensics	Q. Порушення безпеки

Exercise 11. Read the text below. Match choices (A–H) to (1–5). There are three choices you don’t need to use.

Process of Initial Digital Forensic Investigations

(1) When a cyber incident is first reported, investigators must immediately **identify and secure the affected devices**. This stage involves isolating computers, mobile phones, or servers to prevent further data loss or tampering. All actions are carefully documented to ensure evidence integrity.

(2) After securing the environment, specialists perform a **preliminary assessment of the system**. They determine what type of incident occurred, whether it is malware infection, unauthorized access, or data leakage, and define the scope of the investigation.

(3) The next step is **evidence collection**, where investigators gather digital traces such as log files, system memory, emails, and network activity records. Special forensic tools are used to avoid modifying original data during acquisition.

(4) Once data is collected, analysts proceed to **data preservation and imaging**. A bit-by-bit copy of storage devices is created to ensure that the original evidence remains unchanged while analysis is performed on the duplicate copy.

(5) Finally, investigators conduct a **basic analysis of collected evidence**, searching for indicators of compromise, suspicious user activity, and possible attack vectors. The results of this stage help determine whether a full forensic investigation is required.

Choices

- A. Evidence preservation and imaging
- B. Initial system assessment
- C. Celebrity investigation case
- D. Legal court procedure
- E. Evidence collection stage
- F. Cybercrime prevention training
- G. Device isolation and securing
- H. Financial fraud analysis

***Exercise 12. Translate the following sentences into English.**

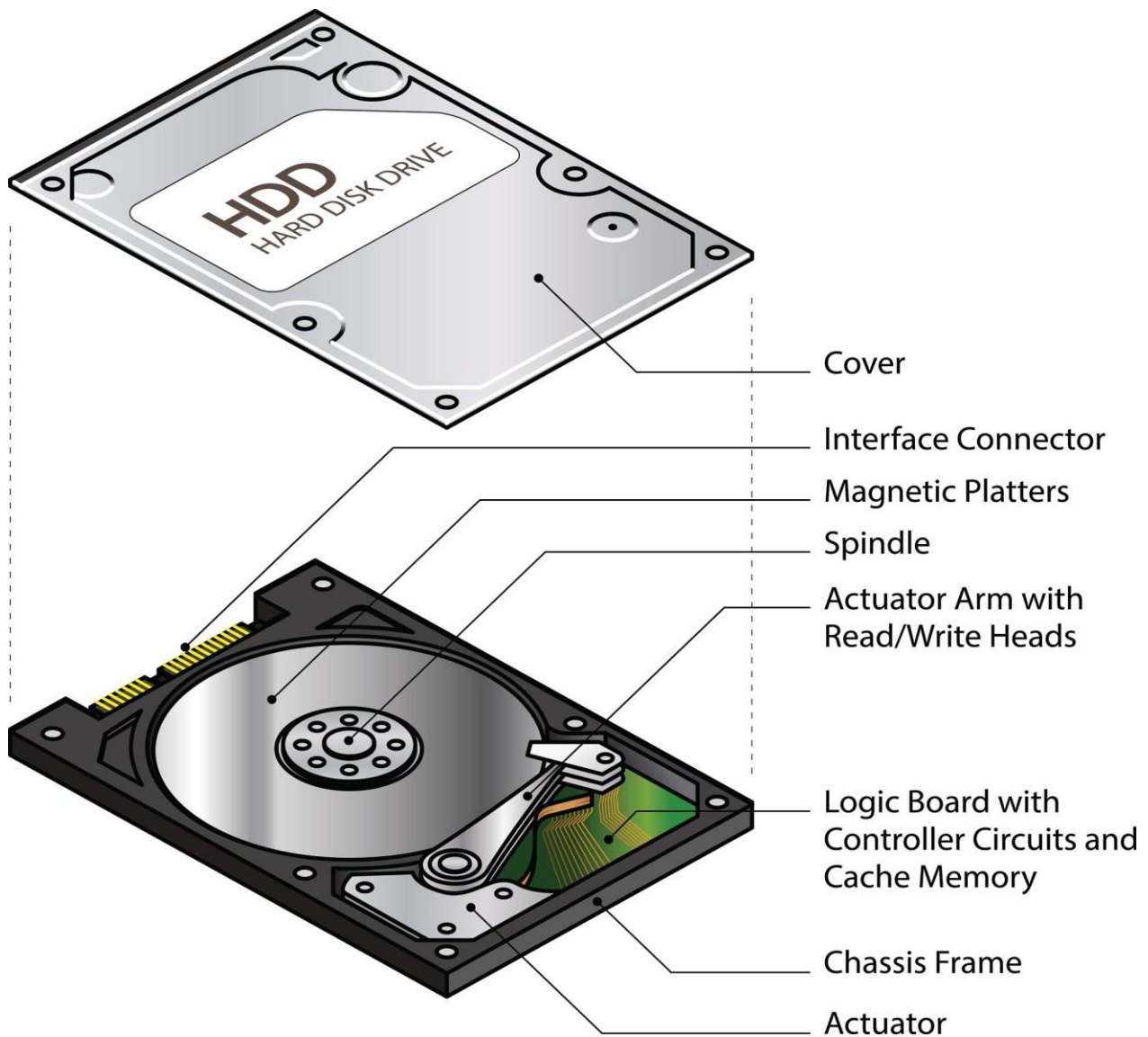
1. Під час інциденту кібербезпеки пристрої необхідно негайно ізолювати.
2. Дослідники збирають цифрові докази з комп’ютерів і серверів.
3. Важливо зберегти цілісність електронних доказів.
4. Первинний аналіз системи допомагає визначити тип інциденту.
5. Фахівці перевіряють журнали подій і мережевий трафік.
6. Дані можуть включати електронні листи та метадані.
7. Створення образу диска використовується для збереження даних.
8. Оригінальні файли не повинні бути змінені під час розслідування.

9. Збір доказів є ключовим етапом цифрової криміналістики.
10. Аналітики шукають ознаки компрометації системи.
11. Мережевий аналіз допомагає виявити підозрілу активність.
12. Дані з хмарних сервісів також можуть бути використані як докази.
13. Суд може прийняти цифрові докази у кримінальних справах.
14. Фахівці визначають можливі вектори атаки.
15. Результати розслідування використовуються для подальшого аналізу.

***Exercise 13. Write T (True) or F (False).**

1. During a cyber incident, devices should be isolated immediately.
2. Digital evidence can be collected without any special tools.
3. Preserving the integrity of evidence is an important principle in digital forensics.
4. Preliminary system analysis helps determine the type of cyber incident.
5. Investigators ignore log files during forensic analysis.
6. Network traffic can provide useful information for investigations.
7. Email and metadata can be considered digital evidence.
8. Disk imaging creates a copy of original data for analysis.
9. Original files are modified during forensic investigation to speed up the process.
10. Evidence collection is an optional step in digital forensics.
11. Analysts search for signs of system compromise during investigation.
12. Cloud data cannot be used as digital evidence.
13. Courts may accept properly collected digital evidence.
14. Attack vectors help investigators understand how the system was compromised.
15. Results of initial analysis are not useful for further investigation.

Physical HDD, File Systems & Logical Structure



1. Physical HDD Structure (Фізична структура жорсткого диску)

English Term	Український еквівалент	Визначення / Контекст
Platter	Пластина	Круглий диск, покритий магнітним шаром, на якому фізично зберігаються дані.
Spindle	Шпиндель	Оборотний вал по центру диска, що утримує пластини та обертає їх із заданою швидкістю (наприклад, 7200 RPM).
Read/Write Head	Головка читання/запису	Магнітний елемент на кінці кронштейна, що зчитує або змінює

English Term	Український еквівалент	Визначення / Контекст
		полярність мікроскопічних ділянок на пластині.
Actuator Arm	Кронштейн головки (актуатор)	Механічний важіль, який переміщує головки читання/запису по радіусу пластин.
Track	Доріжка	Одне з концентричних кіл на поверхні пластини, уздовж якого записуються дані.
Sector	Сектор	Мінімальна фізична ділянка на доріжці. Традиційно вміщує 512 байт, у сучасних дисках (Advanced Format) — 4 кілобайти.
Cylinder	Циліндр	Сукупність усіх доріжок, що розташовані на однаковій відстані від центру на всіх пластинах накопичувача.
Cluster (Allocation Unit)	Кластер (одиниця розподілу даних)	Логічне об'єднання кількох секторів, яке файлова система використовує як мінімальну одиницю для запису файлу.
Bad Sector	Пошкоджений сектор («битий» сектор)	Сектор диска, який неможливо використовувати через фізичне пошкодження або розмагнічування.

2. File Systems & Logical Structure (Файлові системи та логічна структура)

English Term	Український еквівалент	Визначення / Контекст
File System	Файлова система	Порядок і правила, що визначають спосіб організації, зберігання та іменування даних на носії.
Partition	Розділ диска	Логічна частина фізичного

English Term	Український еквівалент	Визначення / Контекст
		диска (наприклад, диск C: чи D:), яка операційною системою сприймається як окремий накопичувач.
MBR (Master Boot Record)	Головний завантажувальний запис	Старий стандарт розмітки диска, що зберігає інформацію про розділи та завантажувач ОС. Підтримує диски розміром до 2 терабайт.
GPT (GUID Partition Table)	Таблиця розділів GUID	Сучасний стандарт розмітки, що замінив MBR. Знімає обмеження на об'єм накопичувача та кількість розділів.
File Allocation Table (FAT)	Таблиця розподілу файлів	Проста і сумісна файлова система (FAT32, exFAT), де інформація про розташування файлів зберігається у спеціальній таблиці.
NTFS (New Technology File System)	Стандартна файлова система для ОС Windows, що підтримує безпеку (права доступу), великі файли та журналювання.	
Journaling	Журналювання	Технологія, при якій ФС записує зміни у спеціальний лог (журнал) перед їх виконанням. Це запобігає пошкодженню даних при раптовому вимкненні світла.
Root Directory	Кореневий каталог	Найвищий за ієрархією

English Term	Український еквівалент	Визначення / Контекст
		каталог у файловій системі (наприклад, / у Linux або C:\ у Windows).
Metadata	Метадані	Службова інформація про файли (дата створення, розмір, права доступу, атрибути), яка не є самим вмістом файлу.
Defragmentation	Дефрагментація	Процес збирання «розкиданих» по диску частин одного файлу (фрагментів) до купи для прискорення читання на HDD.

***Exercise 14: Technical Term Matching.** Match the English technical term with its correct definition or description. Write the correct letter (A–O) next to each number.

1. Platter _____ 2. Read/Write Head _____ 3. Track _____ 4. Sector _____ 5. Cluster _____ 6. Bad Sector _____ 7. Partition _____ 8. MBR _____ 9. GPT _____ 10. NTFS _____ 11. Journaling _____ 12. Metadata _____ 13. Defragmentation _____ 14. Root Directory _____ 15. Spindle _____	A. The smallest physical storage unit on a track, traditionally holding 512 bytes or 4KB. B. A logical division of a hard drive that the operating system treats as an independent unit (like Drive C:). C. The process of reorganizing scattered fragments of files into contiguous blocks to speed up HDD performance. D. A modern partitioning standard that supports drives larger than 2TB and allows almost unlimited partitions. E. A circular, magnetic disk inside an HDD where data is physically written. F. Information about files (such as file size, creation date, and permissions) rather than the content itself. G. A concentric circle on the surface of a platter where data is recorded. H. A physical component that flies microscopic distances above the platter to read or change its magnetic state.
---	--

	<p>I. A feature that logs file changes before they are actually made, protecting the drive against data corruption during crashes.</p> <p>J. A logical group of several sectors; the file system's minimum allocation unit for file storage.</p> <p>K. The central rotating shaft that holds the platters and spins them at high speeds.</p> <p>L. A damaged or demagnetized area of a drive that can no longer be used to read or write data.</p> <p>M. An older, traditional partitioning system limited to four primary partitions and 2TB drives.</p> <p>N. The top-level folder of a file system hierarchy (e.g., C:\ or /).</p> <p>O. The standard, robust file system for Windows that includes built-in security permissions and journaling.</p>
--	---

***Exercise 15: Sentence Completion.** Complete the sentences by choosing the correct word from the box. Each word is used exactly once.

Box:

Actuator Arm, Bad Sectors, Block, Cylinder, Defragmentation, FAT32, File System, GPT, Journaling, Metadata, MBR, NTFS, Platters, Root Directory, Sectors

1. A hard drive cannot store any data until it is formatted with a specific _____.
2. The mechanical _____ moves the read/write heads across the disk surfaces.
3. High-capacity external drives over 2 Terabytes require the _____ layout to fully utilize their space.
4. When you turn on your PC, the system looks at the _____ to find out how the drive is divided and where the OS is located.
5. If you cannot store a large 4GB video file on a flash drive, it is likely formatted in the old _____ system.
6. Operating systems read and write data in _____, which combine multiple physical sectors.
7. Advanced Format HDDs use physical _____ that are 4 Kilobytes in size instead of 512 bytes.
8. Modern HDDs contain multiple magnetic _____ stacked on top of each other.
9. A _____ represents all the tracks that sit directly above one another across all disk surfaces.

10. The file system uses a feature called _____ to recover quickly if the computer suddenly loses power.
11. Windows stores file attributes, permissions, and creation dates as _____ inside the Master File Table.
12. If a hard drive starts making clicking noises, it might be trying to read data from _____.
13. To access any file on a storage drive, the operating system must start searching from the _____.
14. Performing a _____ on a Solid-State Drive (SSD) is completely unnecessary and can even reduce its lifespan.
15. Traditional spinning hard disks store files in _____ mode, whereas flash drives process data electronically.

Exercise 16: Error Correction & Grammar. *Each sentence contains ONE technical or grammatical error related to the topic. Find the error and write the corrected word.*

1. A hard drive has several **platter** that rotate together on a spindle. -> *Correct:* _____
2. Sector is the smallest logical unit of data allocation used by a file system. -> *Correct:* _____
3. NTFS is more secure **then** FAT32 because it supports file permissions. -> *Correct:* _____
4. Defragmentation **reorganize** files to make the hard drive read data faster. -> *Correct:* _____
5. Old MBR systems cannot supporting partitions larger than 2 Terabytes. -> *Correct:* _____
6. The read/write head **do not** touch the platter surface during normal operation. -> *Correct:* _____
7. Modern operating systems can use GPT tables to handle **much** partitions than MBR. -> *Correct:* _____
8. Metadata include information about a file, such as its size and format. -> *Correct:* _____
9. When a computer crashes, a **journaled** file system can prevents data loss. -> *Correct:* _____
10. The actuator arm move very quickly to position the heads over the correct track. -> *Correct:* _____
11. Solid-state drives don't have any moving parts, so they don't need **defragmenting**. -> *Correct:* _____
12. A file system is responsible for **organize** how data is stored on a drive. -> *Correct:* _____
13. If a hard drive has too **much** bad sectors, it will eventually fail completely. -> *Correct:* _____

14. Every file on a partition is located somewhere under the **routing** directory. -> *Correct:* _____
15. Tracks are the **concentrate** circles written onto the magnetic surfaces of platters. -> *Correct:* _____

Exercise 17. Reading Task: Data Acquisition and Imaging in Digital Forensics
Read the text below. For questions (1–5), choose the correct answer (A, B, C or D).

In digital forensics, the initial phase of an investigation is critical, specifically the processes of **data acquisition** and **imaging**. When a digital device is seized as evidence, forensic investigators never work directly on the original media to prevent accidental data modification or destruction. Instead, they must create an exact, bit-stream duplicate of the storage drive—a process known as **forensic imaging**.

Before any data is transferred, investigators use a hardware or software tool called a **write-blocker**. This device is essential because it allows data to be read from the suspect's drive but strictly prevents the operating system from writing any new metadata or temporary files back to it, thereby maintaining **evidentiary integrity**. Once the write-blocker is active, the investigator performs a **bit-stream copy** (or forensic image), which replicates every single bit of data, including hidden files, unallocated space, and deleted fragments, unlike a standard "copy-paste" operation that only transfers active user files.

To legally prove that the forensic duplicate is identical to the original drive, investigators rely on **hashing algorithms**, such as MD5 or SHA-256. A hash function generates a unique alphanumeric string (a digital fingerprint) based on the drive's contents. The hash value of the original drive is calculated before acquisition, and the hash of the newly created image is calculated immediately after. If both values match perfectly, it verifies that no data was altered during the cloning process. Any discrepancy in the hashes renders the evidence inadmissible in a court of law.

Questions:

1. Why do forensic investigators avoid working directly on the original digital device?

- A** Because original devices are often physically damaged and fragile.
- B** To avoid accidental modification or destruction of the evidence.
- C** Because copying files manually is faster than analyzing the original drive.
- D** To allow the suspect to keep using their device during the investigation.

2. What is the primary function of a write-blocker during data acquisition?

- A** It speeds up the bit-stream copying process.
- B** It encrypts the data so that hackers cannot steal it.
- C** It permits data to be read while blocking any data from being written.
- D** It automatically deletes temporary files from the target drive.

3. How does a forensic bit-stream image differ from a regular file copy?

- A** It only copies visible user files to save storage space.

- B** It can only be performed on Solid-State Drives (SSDs).
- C** It requires a password from the suspect to access the drive.
- D** It replicates every single bit, including deleted fragments and hidden spaces.

4. What role do hashing algorithms play in the cloning process?

- A** They verify that the forensic duplicate is identical to the original media.
- B** They help investigators guess the suspect's passwords.
- C** They compress the disk image to make it easier to transfer.
- D** They repair bad sectors on the original hard drive.

5. What happens if the hash value of the original drive and the forensic image do not match?

- A** The investigator must use a different operating system.
- B** The evidence becomes invalid and cannot be used in court.
- C** The imaging software automatically fixes the error.
- D** The suspect is automatically proven guilty.

Exercise 18: Match the English terms with their Ukrainian equivalents. *Match the English technical terms (1–18) with their correct Ukrainian translations (A–R).*

1. Data Acquisition _____	A. Цілісність речових доказів
2. Forensic Imaging _____	B. Оригінальний носій (даних)
3. Bit-Stream Copy _____	C. Криміналістичний дублікат (точна копія)
4. Write-Blocker _____	D. Порозрядне (побітове) копіювання
5. Evidentiary Integrity _____	E. Алгоритм хешування
6. Hashing Algorithm _____	F. Нерозподілений простір (на диску)
7. Digital Forensics _____	G. Здобуття (збір) даних
8. Unallocated Space _____	H. Комп'ютерна криміналістика
9. Original Media _____	I. Хеш-значення (цифровий відбиток)
10. Forensic Duplicate _____	J. Створення криміналістичного образу (образу диска)
11. Data Modification _____	K. Неприпустимий у суді (не може бути доказом)
12. Hash Value _____	L. Блокатор запису (апаратний чи програмний)
13. Inadmissible in Court _____	M. Модифікація (зміна) даних
14. To Seize Evidence _____	N. Вилучати докази
15. Target Drive _____	O. Цільовий накопичувач (диск, на який пишуть копію)
16. Discrepancy _____	P. Розбіжність / невідповідність
17. Chain of Custody _____	Q. Безперервність протоколювання доказів (ланцюжок зберігання)
18. Live Acquisition _____	R. Здобуття даних у «живому» режимі (з увімкненої системи)

Exercise:19 Fill in the Blanks. *Complete the sentences using the words from the box. Change the form of the verb if necessary. Each option is used exactly once.*

Box:

bit-stream copy, chain of custody, data acquisition, digital forensics, discrepancy, evidentiary integrity, forensic image, hash value, hashing algorithm, inadmissible, live acquisition, original media, seize, target drive, write-blocker

1. During the raid, the police officers managed to _____ five laptops and three external hard drives.
2. In _____, working on a live system carries the risk of altering volatile data like RAM.
3. A hardware _____ physically intercepts commands and drops any write requests from the OS.
4. If you want to capture deleted files, a standard backup is useless; you need a perfect _____.
5. The investigator connected the suspect's drive to a clean _____ to save the cloned data.
6. To preserve _____, the device must be kept in an anti-static evidence bag.
7. SHA-256 is a widely used _____ that generates a fixed-length 64-character string.
8. If the file has been altered by even one single byte, its final _____ will change completely.
9. Any _____ between the initial and final calculations proves that data modification occurred.
10. The defense attorney argued that the evidence was _____ because it was collected without a warrant.
11. Keeping a strict _____ log ensures that every person who handled the evidence is documented.
12. Never run analysis software directly on the _____; always use a forensic duplicate.
13. The process of _____ must be done carefully to ensure the data is legally valid.
14. A _____ is usually saved as a raw .dd or an expert witness format .E01 file.
15. When a server cannot be shut down, investigators must perform a _____ to capture active network connections.

Glossary: Anti-Forensics Techniques

English Term	Український еквівалент	Визначення / Контекст
Anti-Forensics	Протидія	Набір методів та інструментів,

English Term	Український еквівалент	Визначення / Контекст
	криміналістичному дослідженню (антикриміналістика)	спрямованих на перешкоджання, уповільнення або унеможливлення цифрового розслідування.
Data Wiping (Sanitization)	Гарантоване знищення даних (затирання)	Процес повного видалення даних шляхом перезапису секцій носія випадковими символами (на відміну від звичайного видалення).
Steganography	Стеганографія	Приховування факту існування секретного повідомлення всередині іншого файлу (наприклад, картинки чи аудіо).
Data Obfuscation	Обфускація (заплутування) даних	Зміна вигляду коду або даних так, щоб вони залишалися робочими, але стали абсолютно нечитаскими для аналітиків.
Encryption	Шифрування	Перетворення інформації на нечитасимий код за допомогою алгоритмів для обмеження несанкціонованого доступу.
Artifact Destruction	Знищення артефактів	Видалення цифрових слідів (логів, історії браузера, реєстру), які залишаються в системі після дій користувача.
Trail Obfuscation	Заплутування слідів	Навмисне спотворення цифрових доказів з метою дезорієнтації слідства (наприклад, зміна часових міток).
Timestomping	Таймстемпінг (підробка	Техніка протидії, що полягає у

English Term	Український еквівалент	Визначення / Контекст
	часових міток)	зміні дати та часу створення, модифікації чи доступу до файлу (MAC times).
Volatile Data Overwriting	Перезапис тимчасових даних	Швидке очищення або заповнення випадковими даними оперативної пам'яті (RAM) перед вимкненням або під час виявлення загрози.
File Header Manipulation	Маніпуляція із заголовком файлу	Зміна службових байтів на початку файлу, щоб обдурити криміналістичний софт щодо реального типу цього файлу (наприклад, маскування .exe під .jpg).

Exercise 20. Reading Task: Anti-Forensics in Action

Read the texts below. Match choices (A–H) to paragraphs (1–6). There are two choices you don't need to use.

Techniques for Obstructing Digital Investigations

1. _____

Modern operating systems and forensic suites rely heavily on file signatures to identify data types. To counter this, sophisticated actors often alter the magic bytes at the very beginning of an executable or sensitive file. By changing these specific markers, a malicious script might be identified by automated security scanners as a harmless image or a text document, causing investigators to overlook vital evidence.

2. _____

When cybercriminals infiltrate a system, they leave a digital path behind. To mislead the response teams, they can employ tools that modify the Metadata logs—specifically the Modified, Accessed, and Created (MAC) timestamps. By backdating a file's creation time to five years in the past, the file disappears from the investigator's timeline analysis of the actual security breach window.

3. _____

Standard file deletion simply marks storage clusters as available without physically erasing the underlying binary code. Anti-forensics practitioners circumvent recovery efforts by utilizing specialized software that overwrites these sectors multiple times with zeros or random noise. Once this process is finalized,

retrieving the original information through magnetic properties or software utilities becomes physically impossible.

4. _____

While transforming a text document into unreadable ciphertext immediately signals to an investigator that something is being hidden, this method takes a more deceptive approach. It embeds confidential data directly inside legitimate, everyday carrier files, such as a family photograph or an MP3 track. To the naked eye and traditional forensic filters, the carrier file appears completely authentic and unaltered.

5. _____

Digital forensic analysts frequently perform live memory triage to extract active cryptographic keys, network connections, and passwords directly from the RAM. To defend against this, certain malware strains execute a routine that immediately floods the system's volatile memory or triggers an abrupt hardware reset the moment an administrator opens a forensic console or terminal window.

6. _____

This methodology focuses on making code or structural information highly intricate and difficult for human analysts or reverse-engineers to comprehend. Software developers and threat actors alike use packing, stripping of debugging symbols, and variable renaming. Although the application executes perfectly on the hardware level, the logic behind the program becomes an indecipherable maze during static analysis.

Choices:

- A Data Wiping (Sanitization)
- B Symmetric Encryption
- C Timestomping
- D Steganography
- E Data Obfuscation
- F File Header Manipulation
- G Brute-Force Defense
- H Volatile Data Overwriting

Exercise 21. Multiple Choice. Choose the correct answer (A, B, C or D) to complete each sentence or answer the question.

1. What is the primary goal of anti-forensics techniques?

- A To speed up the process of digital data acquisition.
- B To manipulate, hide, or erase digital evidence to block investigations.
- C To recover deleted partitions and files from corrupted target drives.
- D To automatically generate cryptographic hash values for court trials.

2. When a suspect changes a file's "magic bytes" to trick forensic software into thinking an executable (.exe) is a picture (.jpg), they are practicing...

- A data wiping.
- B timestomping.

- C file header manipulation.
- D steganography.

3. Why is standard file deletion ineffective against professional forensic software?

- A It automatically encrypts the file instead of removing it.
- B It only removes the file pointer, leaving the actual binary data intact on the drive.
- C It changes the file extension to a random string of alphanumeric characters.
- D It sends a copy of the deleted file directly to the cloud.

4. A tool that completely overwrites storage sectors with random data or zeros to ensure files can never be recovered is performing...

- A volatile data overwriting.
- B data wiping (sanitization).
- C trail obfuscation.
- D data compression.

5. Which anti-forensics method hides a secret text file inside a normal audio or image carrier file without changing its appearance?

- A Steganography
- B Symmetric Encryption
- C Metadata extraction
- D Data obfuscation

6. Timestomping specifically targets which type of forensic evidence?

- A The physical alignment of platters on a hard drive.
- B RAM data logs containing network connections.
- C The file signature and magic bytes.
- D The MAC (Modified, Accessed, Created) timestamps of a file.

7. If an intruder modifies the system event logs to make it look like a security breach happened three years ago instead of yesterday, they are using...

- A data wiping.
- B timestomping.
- C steganography.
- D file carving.

8. Malware that detects a live forensic extraction tool and immediately purges or overwrites the RAM is utilizing...

- A volatile data overwriting.
- B artifact destruction.
- C block cipher encryption.
- D hardware write-blocking.

9. Data obfuscation is typically used by threat actors to make their source code...

- A run much faster on older computers.
- B incredibly difficult for human analysts to read and reverse-engineer.
- C automatically compatible with multiple operating systems.
- D invisible to the hard drive's read/write heads.

- 10. When an investigator performs "live memory triage," what are they trying to extract before volatile data overwriting occurs?**
- A Data from physical bad sectors on the platter.
 - B Temporary information, encryption keys, and active connections from the RAM.
 - C The Master Boot Record (MBR) from the target drive.
 - D The GUID Partition Table (GPT) geometry.
- 11. The deliberate removal of registry keys, browser history, and temporary log files to leave no traces of user activity is called...**
- A file header manipulation.
 - B artifact destruction.
 - C steganography.
 - D bit-stream copying.
- 12. What makes encryption an effective anti-forensics tool?**
- A It converts plaintext into unreadable ciphertext that cannot be unlocked without the correct key.
 - B It physically destroys the hard drive's magnetic layer.
 - C It hides the fact that a file even exists on the partition.
 - D It automatically formats the root directory if an analyst opens it.
- 13. If an automated forensic tool incorrectly flags a dangerous script as a harmless image, which technique was likely used?**
- A Steganography
 - B File header manipulation
 - C Volatile data overwriting
 - D Data wiping
- 14. Packing, variable renaming, and removing debugging symbols from a program are all examples of...**
- A encryption.
 - B artifact destruction.
 - C data obfuscation.
 - D timestomping.
- 15. If a suspect successfully uses a military-grade data wiping tool on their hard drive, what will a forensic investigator see when creating a bit-stream copy?**
- A The original files, but with altered names and timestamps.
 - B A drive filled completely with zeros or random noise, with zero recoverable data.
 - C A hidden partition containing all the original metadata.
 - D A prompt asking for the MD5 hashing algorithm password.

OS Forensics - Криміналістичне дослідження ОС. Процес збору, аналізу та збереження доказів, що містяться в операційній системі (артефактів користувача та системи).

Registry Artifacts - Артефакти реєстру. Записи у базі даних конфігурації ОС (наприклад, Windows Registry), що містять інформацію про підключені пристрої, запущені програми та дії користувача.

Event Logs - Журнали подій (логи). Файли, куди операційна система автоматично записує інформацію про системні помилки, входи в систему, запуск служб та інші події безпеки.

Volatile Data - Тимчасові (летучі) дані. Дані, які втрачаються у разі вимкнення живлення комп'ютера (наприклад, вміст RAM, поточні мережеві з'єднання).

Pagefile / Swap File - Файл підкачки. Прихований системний файл на жорсткому диску, куди ОС скидає дані з RAM, якщо фізичної пам'яті не вистачає. Може містити фрагменти паролів та видалених файлів.

Hibernation File (hiberfil.sys) - Файл гібернації. Файл, у який скидається повний знімок оперативної пам'яті (RAM) під час переходу комп'ютера в режим гібернації. Справжня «золота жила» для слідчого.

Artifact – Артефакт. Будь-який цифровий слід або залишок активності в операційній системі (історія браузера, тимчасові файли, мітки часу).

Prefetch Files - Файли префетчу (попередньої вибірки) Файли ОС Windows, створені для прискорення запуску програм. Зберігають інформацію про те, які програми запускалися і коли саме.

User Profile Analysis - Аналіз профілю користувача. Дослідження папок та налаштувань конкретного користувача (історія пошуку, нещодавні документи, кошик).

File System Metadata - Метадані файлової системи Службова інформація про файли (часові мітки створення, права доступу, власник файлу), вбудована у саму файлову систему (наприклад, MFT в NTFS).

Exercise 22. Reading Task. *Read the text below. Choose from (A–H) the one which best fits each space (1–6). There are two choices you don't need to use.*

The Digital Footprints Inside an OS

Digital investigators often face clever cybercriminals who try to hide their tracks. However, the operating system (OS) acts like a permanent witness, constantly recording everything behind the scenes. When a computer is seized during an investigation, an expert's first step is to perform live memory triaging to capture (1) _____ before the machine loses power. This volatile RAM contains current network connections, running processes, and active encryption keys.

Once the temporary data is safely secured, the system is turned off, and a bit-stream copy of the hard drive is made for offline analysis. The investigator then digs deep into the Windows Registry, looking for specific (2) _____ that can prove a corporate spy plugged in an unauthorized USB drive. The Registry

remembers serial numbers, installation dates, and even the last files that were opened by a specific user profile.

To build a chronological timeline of the security incident, the expert must parse (3) _____ stored within the operating system. These system logs act as an automated diary, documenting every successful login attempt, critical software crash, or unauthorized privilege escalation. Even if a smart attacker attempts to delete these files, digital forensics utilities can often recover deleted fragments from (4) _____ on the storage drive.

Furthermore, artifacts like Prefetch files are examined because they automatically maintain (5) _____ of every application executed on the computer. This makes it impossible for a suspect to claim they "never installed or opened" a malicious hacking tool. Finally, if the computer dropped into a low-power mode shortly before the raid, the investigator will scan the root directory for (6) _____, which essentially holds a snapshot of everything that was running in the computer's memory at that exact millisecond.

Choices:

- A** a detailed history
- B** the hibernation file
- C** volatile data from RAM
- D** encrypted cloud storage
- E** crucial event logs
- F** the pagefile or unallocated space
- G** physical destruction of media
- H** registry artifacts

Exercise 23. Fill in the Blanks

Complete the sentences using the correct terms from the box. Change the form of the words if grammatically necessary. Each option is used exactly once.

Box:

Artifacts, Event Logs, File System Metadata, Hibernation File, Live Memory Triaging, OS Forensics, Pagefile, Parse, Prefetch Files, Registry Artifacts, System Logs, Timeline, User Profile Analysis, Volatile Data, Windows Registry

1. When a suspect's computer is found running, investigators must perform _____ immediately to capture active processes.
2. The specialized field of digital forensics that focuses on recovering evidence from the operating system itself is called _____.
3. In a Windows environment, the _____ acts as a massive central database storing system configuration and user activity data.
4. Analyzing the _____ can reveal a list of recently plugged-in USB devices and their unique serial numbers.

5. RAM contains _____ that will disappear forever if the computer is turned off or loses power.
6. To see exactly when a specific hacking program was executed, an analyst will examine the _____, which are designed to speed up application loading.
7. Automated operating system diaries, known as _____, record critical security events such as successful or failed user logins.
8. If the target machine went into a deep sleep before being seized, the investigator can extract a full snapshot of the RAM from the _____ (hiberfil.sys).
9. When the physical RAM is full, Windows moves temporary data to a hidden storage space on the hard drive called the _____.
10. Digital _____ are any leftovers, traces, or pieces of data created by the operating system or user activity.
11. To reconstruct the exact order of events during a data breach, investigators build a detailed chronological _____.
12. Security experts need specialized tools to _____ raw log files into a readable, human-analyzable format.
13. Timestamps, file sizes, and ownership permissions are all examples of _____ embedded within the NTFS structure.
14. Conducting a _____ allows investigators to check a specific user's browser history, recent documents, and Recycle Bin contents.
15. Attackers often try to clear the Microsoft _____ to hide their unauthorized privilege escalation attempts.

Glossary

Англійський термін	Український еквівалент	Визначення / Контекст
Network Forensics	Криміналістичне дослідження комп'ютерних мереж	Субдисципліна цифрової криміналістики, що займається моніторингом та аналізом мережевого трафіку.
Volatile Data	Летючі (непостійні) дані	Дані, які втрачаються при вимкненні живлення пристрою (наприклад, оперативна пам'ять, поточні мережеві підключення).
Packet Sniffing	Перехоплення (сніфінг) пакетів	Процес захоплення та логування мережевих пакетів, що проходять через мережу.

Англійський термін	Український еквівалент	Визначення / Контекст
Intrusion Detection System (IDS)	Система виявлення вторгнень	Програмне або апаратне забезпечення, яке моніторить мережу на предмет підозрілої активності.
Log Analysis	Аналіз журналів подій (логів)	Дослідження записів, створених серверами, брандмауерами та іншими пристроями, для відстеження хронології подій.
Evidentiary Value	Доказова цінність	Юридична вартість та придатність зібраних цифрових даних для використання у суді.
Chain of Custody	Ланцюжок збереження доказів	Хронологічна документація, яка фіксує процес вилучення, контролю, передачі та аналізу цифрових доказів.
Traffic Metadata	Метадані трафіку	Інформація про передачу даних (IP-адреси, порти, час, обсяг), без урахування самого вмісту (payload) повідомлень.

Exercise 24. Read the text and answer the questions:

Introduction to Network Forensics

Network forensics is a critical sub-branch of digital forensics that focuses on the monitoring, capture, storing, and analysis of network activities. Unlike computer forensics, which typically deals with data at rest (such as files stored on hard drives), network forensics deals with **data in motion**. It is an essential tool for identifying cyber threats, understanding how a security breach occurred, and gathering digital evidence that can stand in a court of law.

The primary challenge in network forensics is the **volatile nature** of network data. Network packets travel across cables and wireless waves in milliseconds; if they are not captured in real time, they are gone forever. To tackle this, investigators use two main approaches: the "Catch-it-as-you-can" method, where all packets passing through a traffic point are intercepted and saved, and the "Stop, look, and listen" method, where systems look for specific anomalies using an Intrusion Detection System (IDS) and only log suspicious traffic.

During an investigation, analysts rely heavily on **log analysis** and **packet sniffing** tools (like Wireshark). They examine traffic metadata to determine the source and destination IP addresses, the protocols used, and the exact timestamp of the attack. However, the widespread use of encryption (like HTTPS and VPNs) poses a significant obstacle, as it hides the actual content of the communication, forcing investigators to rely more on traffic patterns and metadata. Modern attackers often use sophisticated techniques like IP spoofing to disguise their identity or Distributed Denial of Service (DDoS) attacks to overwhelm systems and mask their true intentions. Furthermore, sophisticated malware may establish hidden communication lines, known as Command and Control (C2) channels, to silently exfiltrate sensitive corporate data.

To detect these hidden threats, forensic specialists must look beyond individual packets and perform comprehensive network flow analysis. They reconstruct fragmented data streams to understand the full narrative of how a hacker penetrated the defensive perimeter. Security Information and Event Management (SIEM) systems are also deployed to automatically aggregate logs from routers, firewalls, and servers worldwide. This automated correlation helps investigators connect seemingly unrelated network events into a single timeline of an attack. Ultimately, maintaining a strict **chain of custody** is paramount throughout this entire process. Every step of the network data collection must be meticulously documented to prevent any claims of evidence modification. If an investigator cannot prove that the captured network logs were protected from tampering from the moment of seizure to the courtroom presentation, the evidence will lose its evidentiary value and be dismissed.

Comprehension Questions

1. What is the primary focus of network forensics according to the text?
2. How does the concept of "data in motion" differ from "data at rest"?
3. Why is the volatile nature of network data considered a major challenge for investigators?
4. What happens if network packets are not captured in real time?
5. How does the "Catch-it-as-you-can" approach operate?
6. What is the core mechanism of the "Stop, look, and listen" method?
7. Which specific tool is mentioned as a common choice for packet sniffing?
8. What kind of information can investigators extract from traffic metadata?
9. Why do encryption technologies like VPNs present a problem for forensic analysts?
10. What is the purpose of IP spoofing when used by cybercriminals?
11. How do attackers use DDoS attacks as a tactical distraction?
12. What are Command and Control (C2) channels used for?
13. Why do forensic specialists reconstruct fragmented data streams?
14. What role do SIEM systems play in a modern network investigation?
15. What are the legal consequences of failing to maintain a proper chain of custody?

Exercise 25. True / False

1. Network forensics and traditional computer forensics focus on the exact same types of data storage.
2. Network packets remain permanently accessible on network cables even if they are not logged immediately.
3. The "Stop, look, and listen" method logs absolutely every single packet regardless of its nature.
4. An Intrusion Detection System (IDS) is used to flag anomalies in network traffic.
5. Wireshark can be used by analysts to perform packet sniffing during an investigation.
6. Traffic metadata includes the exact source and destination IP addresses of network packets.
7. Encryption completely prevents investigators from seeing traffic patterns or timestamps.
8. Attackers use IP spoofing to make their malicious traffic appear as if it comes from a trusted source.
9. DDoS attacks are strictly used to steal corporate files and data.
10. Command and Control (C2) channels allow malware to communicate with an attacker's external server.
11. Reconstructing fragmented data streams helps specialists understand the chronological flow of an attack.
12. SIEM systems are manual tools that require human analysts to type in every network log individually.
13. Firewalls and routers are among the devices that generate logs used in forensic analysis.
14. The chain of custody is only important during the courtroom presentation, not during data collection.
15. Evidence can be completely dismissed in a court of law if there is proof of data tampering or poor documentation.

Exercise 26: Match the words with their meanings

1	Network forensics	A	Automated systems that aggregate and correlate logs from multiple network devices.
2	Volatile data	B	Data that moves actively across cables or wireless waves (in transit).
3	Packet sniffing	C	A technique used by hackers to fake their source IP address and disguise their identity.
4	Intrusion Detection System (IDS)	D	A sub-branch of digital forensics that deals with capturing and analyzing data in motion.
5	Log analysis	E	Information about data transmission (like IPs, timestamps) without the actual content.
6	Chain of custody	F	Data that disappears forever if not captured
7	Traffic metadata		
8	Evidentiary value		
9	Data in motion		
10	Encryption		

11	IP spoofing	in real time (e.g., temporary memory).
12	DDoS attack	Hidden communication lines used by
13	Command and Control (C2)	malware to talk to an attacker's server.
14	Data at rest	H The process of capturing and logging
15	SIEM systems	packets passing through a network.
		I A cyberattack that overwhelms network
		systems to make them unavailable.
		J Examining records created by servers and
		firewalls to trace events.
		K Software or hardware that monitors
		network traffic for suspicious activity.
		L The legal worth and suitability of digital
		data to be used as proof in court.
		M Technology (like VPN/HTTPS) that hides
		the text/content of a communication.
		N Chronological documentation showing
		who collected, handled, and analyzed the
		evidence.
		O – Data at rest — Static data stored
		permanently on physical devices like hard drives

Exercise 27: Translate into English. *Перекладіть речення англійською мовою, використовуючи професійну термінологію:*

1. Криміналістичне дослідження комп'ютерних мереж фокусується на даних у русі, а не на даних у стані спокою.
2. Головна проблема полягає в тому, що мережеві пакети є дуже летючими даними.
3. Якщо спеціалісти не перехоплять трафік у реальному часі, докази будуть втрачені назавжди.
4. Наш аналітик використовує Wireshark для перехоплення пакетів у цій локальній мережі.
5. Система виявлення вторгнень (IDS) зафіксувала підозрілу активність на сервері вчора ввечері.
6. Для відстеження хронології кібератаки експертам необхідно провести детальний аналіз журналів подій (логів).
7. Навіть якщо вміст повідомлення зашифрований, ми все одно можемо проаналізувати метадані трафіку.
8. Будь-яка помилка в документації може знизити доказову цінність зібраних цифрових даних.
9. Слідчий повинен суворо дотримуватися ланцюжка збереження доказів від моменту їх вилучення.
10. Хакери часто використовують IP-спуфінг, щоб приховати свою справжню ідентичність під час атаки.

- 11.Ця потужна DDoS-атака була використана як тактичне відволікання уваги.
- 12.Шкідливе програмне забезпечення встановило прихований командний канал (C2) для витоку корпоративних даних.
- 13.Системи SIEM допомагають автоматично збирати та пов'язувати логи з брандмауерів та маршрутизаторів.
- 14.Шифрування (таке як VPN або HTTPS) ускладнює роботу криміналістів, оскільки воно приховує вміст комунікації.
- 15.Докази будуть відхилені в суді, якщо захист доведе факт втручання в мережеві логи.

Exercise 28. Read the text below. For questions (1-10), choose the correct answer (A, B, C or D).

Web Application Forensics

As the reliance on cloud computing and e-commerce platforms grows, web applications have become the primary targets for cybercriminals. Web application forensics is a specialized branch of digital forensics dedicated to investigating attacks aimed at websites, web servers, and online services. Unlike traditional network forensics, which examines packets moving across wires, web forensics focuses on application-layer data, investigating breaches like SQL Injection (SQLi), Cross-Site Scripting (XSS), and unauthorized data exfiltration.

When a web attack occurs, the criminal leaves behind distinct digital footprints, primarily recorded in server logs. The first line of defense and investigation for a forensic specialist is analyzing the Hypertext Transfer Protocol (HTTP) server logs, such as those generated by Apache or Microsoft IIS servers. These logs document every request made to the server, including the visitor's IP address, request method (GET or POST), requested Uniform Resource Locator (URL), and the server response status code (such as a 200 OK or a 404 Not Found). By carefully inspecting these strings, investigators can pinpoint the exact moment a vulnerability was exploited.

However, modern attackers are sophisticated and rarely use their own infrastructure. They frequently employ proxy servers, the Tor network, or compromised machines to obfuscate their true location. Furthermore, skilled hackers often attempt to delete or alter server logs to impede the investigation. To counter this, forensic experts rely on centralized log management and immutable logging systems, which ensure that once a log entry is written, it cannot be modified or erased, even by an administrator with root privileges.

Another critical component of web forensics is the analysis of database logs. During an SQL Injection attack, for instance, a criminal inserts malicious database commands into a web form to steal sensitive tables. While HTTP logs might show a suspicious request, the database transaction logs reveal exactly what data was viewed, altered, or deleted. Ultimately, web forensic analysts must combine network traffic,

server logs, and database records to reconstruct the full scope of the incident and prepare a legally binding report.

Questions:

1. According to the first paragraph, what is the main reason web applications are targeted?

- A) Because traditional network forensics is too expensive.
- B) Due to the increasing reliance on cloud computing and e-commerce.
- C) Because they do not use application-layer data.
- D) Because cybercriminals prefer investigating websites over hard drives.

2. Web application forensics differs from network forensics because it focuses on:

- A) Data stored permanently on encrypted hard drives.
- B) Packets moving physically across network cables.
- C) Application-layer data and web services.
- D) Deleting malicious code from online platforms.

3. What are SQLi and XSS examples of?

- A) Types of server log management software.
- B) Specialized digital forensic tools.
- C) Common web application vulnerabilities/attacks.
- D) Server response status codes.

4. Where are a criminal's digital footprints primarily recorded during a web attack?

- A) In the user's personal web browser history.
- B) In the physical structure of the hard drive.
- C) Inside the hardware of proxy servers.
- D) Within the server logs.

5. What information can an investigator find in an HTTP server log?

- A) The hacker's real physical home address.
- B) The request method, visitor's IP, and server response code.
- C) The decrypted password of the database administrator.
- D) The source code of the anti-forensics tools used.

6. The word "obfuscate" in the third paragraph is closest in meaning to:

- A) Hide or conceal
- B) Improve or clarify
- C) Speed up
- D) Analyze or study

7. Why do skilled hackers attempt to delete or alter server logs?

- A) To save storage space on the server.
- B) To activate the database transaction logs.
- C) To hinder and obstruct the forensic investigation.
- D) To upgrade their administrative privileges to root.

8. What makes "immutable logging systems" valuable to forensic experts?

- A) They automatically block SQL Injection attacks in real time.
- B) Log entries cannot be changed or deleted once written.
- C) They reveal the real identity of users on the Tor network. D)
- They allow hackers to test their exploits safely.

9. Why are database logs crucial during an SQL Injection investigation?

- A) They track the physical location of the server hardware.
- B) They document the exact data that was viewed, altered, or stolen.
- C) They replace the need for analyzing HTTP server logs entirely.
- D) They automatically reset response codes back to 200 OK.

10. What must web forensic analysts do to understand the full scope of an incident?

- A) Rely solely on the browser history of the victim.
- B) Combine network traffic, server logs, and database records.
- C) Format the server immediately after the attack occurs.
- D) Ask the hacker to provide a legally binding report.

Exercise 29: Match the English terms (1–15) with their Ukrainian equivalents (A–O)

	English Term		Ukrainian Equivalent
1	Web application forensics	A	Приховати (заплутати) справжнє місцезнаходження
2	SQL Injection (SQLi)	B	Метод запиту
3	Cross-Site Scripting (XSS)	C	Незмінна система логування (захищена від видалення)
4	Unauthorized data exfiltration	D	Журнали транзакцій бази даних
5	Digital footprints	E	Криміналістичне дослідження веб-додатків
6	Server logs	F	Несанкціоноване вилучення (витік) даних
7	Request method	G	Права суперкористувача (root-права)
8	Response status code	H	Упровадження (ін'єкція) шкідливого SQL-коду
9	Obfuscate true location	I	Централізоване керування журналами подій
10	Immutable logging system	J	Цифрові сліди
11	Root privileges	K	Міжсайтовий скриптинг

	English Term		Ukrainian Equivalent
12	Database transaction logs	L	Юридично зобов'язуючий звіт (висновок)
13	Centralized log management	M	Компрометовані (взламані) машини
14	Legally binding report	N	Код статусу відповіді (сервера)
15	Compromised machines	O	Журнали подій сервера (серверні логи)

Exercise 30. Listen to this text and do Task 1 and Task 2

Welcome back to the "Tech & Security" podcast. Today, we are diving into the world of **Digital Forensics** and how it helps in combating cybercrime.

When a cyberattack happens — whether it's a ransomware attack on a hospital or a data breach at a tech giant — digital forensic investigators are the first ones called to the scene. Their job is a lot like traditional police forensics, but instead of looking for physical fingerprints or DNA, they hunt for digital breadcrumbs: IP addresses, altered metadata, and hidden log files.

The entire process follows a strict four-step framework. The first step is **Identification**. Investigators must pinpoint what devices were involved and what data might have been compromised. Next comes **Preservation**. This is arguably the most critical phase. Before touching any data, investigators must create a bit-stream copy — which is an exact, identical replica of the hard drive. Why? Because working on the original evidence could accidentally modify timestamps or damage files, making the evidence inadmissible in court.

The third phase is **Analysis**. This is where the real detective work begins. Analysts use specialized software to recover deleted files, reconstruct chat histories, and trace how the malware entered the information system. They look for the *artifacts* — traces left behind by the hacker. Finally, there is **Reporting**. All findings must be documented in a clear, legally sound report that can be presented to judges or corporate executives.

As cybercriminals utilize advanced tactics like AI-driven phishing and encrypted communication, digital forensics must evolve. Today, it's not just about solving crimes after they happen; it's about creating resilient information systems that can withstand the threat in real-time.

Task 1: Multiple Choice

Choose the correct answer (A, B, or C) based on the audio.

1. According to the speaker, digital forensic investigators look for:
 - A) Physical fingerprints on the server hardware.
 - B) Digital traces like altered metadata and log files.
 - C) The identity of the hacker within the first hour.

2. **Why is the "Preservation" phase considered so critical?**
 - A) It is the phase where hackers are directly identified.
 - B) It prevents the original evidence from being accidentally modified or ruined.
 - C) It helps to automatically delete the malware from the system.
3. **What does an investigator do during the "Analysis" phase?**
 - A) Presents findings to judges in a courtroom.
 - B) Pinpoints which physical devices were stolen.
 - C) Recovers deleted files and traces how the malware entered the system.

Task 2: Gap Filling

Complete the sentences below. Use **NO MORE THAN THREE WORDS** from the audio.

1. Traditional police forensics looks for DNA, while digital forensics hunts for _____.
2. Before analyzing data, investigators must create a _____ of the hard drive.
3. The final phase of the digital forensics framework is called _____.
4. Modern cybercriminals are now using advanced tactics like _____.

Exercise 31. Video

Part 1:

Watch the video <https://www.youtube.com/watch?v=w2xItujdLag> and determine whether the following statements are True or False.

1. In 2021, the number of cyberattacks per week decreased compared to 2020. [00:00:10]
2. Computer forensics originally started in the 1980s due to the rise of financial crimes using computers. [00:01:04]
3. Digital forensics experts help solve crimes like cyber terrorism, data breaches, and cyber stalking. [00:01:26]
4. Network forensics involves retrieving data from mobile devices like smartphones and tablets. [00:02:07]
5. The digital forensics market is predicted to reach over 20 billion USD by 2027. [00:02:23]

Part 2:

Watch the video <https://www.youtube.com/watch?v=w2xItujdLag> again and fill in the Branches. The video mentions three distinct branches of digital forensics. Fill in the blanks in the table according to what you heard [00:01:50]

Branch of Forensics	What it involves
---------------------	------------------

Branch of Forensics	What it involves
1. _____ forensics	Collecting and preserving data from computers, laptops, and storage devices.
2. Network forensics	Monitoring and analyzing _____ to gather evidence.
3. Mobile forensics	Retrieving data from mobile devices like _____ and tablets.

FINAL TEST UNIT 7

Digital Forensics and Combating Cybercrime in Information Systems

PART I: MULTIPLE CHOICE

Choose the single best answer (A, B, C, or D) for each question.

1. According to the Order of Volatility, which of the following evidence sources must be collected FIRST during an active incident response?

- A) Hard drive files and slack space
- B) Archival backups stored in cloud systems
- C) Routing tables, ARP cache, and RAM content
- D) Windows Registry entries and application logs

2. What is the main forensic advantage of using a "Write-Blocker" hardware device during data acquisition?

- A) It encrypts the target storage drive to prevent leaks.
- B) It intercepts and blocks any write commands from the forensic workstation to the evidence drive.
- C) It automatically bypasses the operating system's administrator password.
- D) It flags network anomalies using a built-in Intrusion Detection System (IDS).

3. If a cybercriminal uses "IP Spoofing" during a network attack on an information system, what is their primary objective?

- A) To completely encrypt the payload of the communication.
- B) To exfiltrate sensitive data without using a Command and Control (C2) channel.
- C) To disguise their true location by faking the source IP address in packet headers.
- D) To permanently delete HTTP server logs on the target web server.

4. Why should a seized mobile device be placed immediately into a Faraday bag?

- A) To keep the device's battery from draining quickly.
- B) To protect the device from physical drops or screen damage.
- C) To prevent the device from connecting to cellular networks or Wi-Fi, blocking potential remote-wipe commands.
- D) To automatically extract a bit-stream image of the mobile operating system.

5. An investigator examines database transaction logs during a web application breach. Which type of attack are they most likely investigating if they find unauthorized table modifications injected via web forms?

- A) Distributed Denial of Service (DDoS)
- B) SQL Injection (SQLi)
- C) Cross-Site Scripting (XSS)
- D) Phishing email campaigns

6. What is a unique jurisdictional challenge when conducting Cloud Forensics in modern information systems?

- A) Cloud data is strictly static and does not contain timestamps.
- B) Data is often distributed across multiple physical servers located in different countries, complicating legal warrants.
- C) Cloud service providers do not keep any server or access logs.

D) Cloud environments are immune to anti-forensics techniques.

7. Which cryptographic function is utilized to generate a unique digital fingerprint of a digital asset to verify its integrity in court?

A) Symmetric Advanced Encryption Standard (AES)

B) Public Key Infrastructure (PKI)

C) Hashing algorithms (e.g., SHA-256 or MD5)

D) Virtual Private Network (VPN) tunneling

8. What does a Security Information and Event Management (SIEM) system do to assist forensic analysts during a corporate breach investigation?

A) It physically locks down the compromised workstation hardware.

B) It automatically aggregates and correlates logs from multiple network devices to reconstruct an attack timeline.

C) It decrypts end-to-end encrypted messaging applications used by corporate insiders.

D) It deletes malicious malware files before an investigator arrives.

9. The terms "Data at Rest" and "Data in Motion" represent different states of information. Which field primarily investigates "Data in Motion"?

A) Hard drive and file system forensics

B) Operating system forensics

C) Network forensics

D) Mobile application forensics

10. What is the legal consequence if a forensic analyst fails to document the "Chain of Custody" for a hard drive seized from a crime scene?

A) The analyst will be forced to use an immutable logging system.

B) The evidentiary value of the drive is ruined, and the evidence will likely be dismissed in a court of law.

C) The data on the drive will automatically become corrupted.

D) The suspect will automatically be found guilty due to poor documentation.

PART II: TERMINOLOGY MATCHING

Match each English digital forensics term (1–10) with its correct definition or operational description (A–J).

No.	Term		Letter	Definition / Operational Description
1	Bit-stream Image		A	Automated platforms that collect, parse, and analyze logs from firewalls, routers, and endpoints.
2	Anti-forensics		B	An exact bit-for-bit copy of a storage medium, including hidden, deleted, and unallocated data sectors.
3	SIEM		C	Information about data execution, such as

No.	Term		Letter	Definition / Operational Description
	Systems			timestamps, file paths, authors, or geolocation tags.
4	Slack Space		D	Sneaking or faking network packet data to trick an information system into trusting a malicious source.
5	Metadata		E	Hidden communication lines used by malware to receive commands from an external cybercriminal server.
6	C2 Channels		F	The unused space created when a file saved to a hard drive does not completely fill the allocated sector block.
7	Immutable Log		G	Techniques used by criminals to intentionally alter, erase, or obscure digital footprints to obstruct investigators.
8	Wireshark		H	A popular software utility used for deep packet sniffing and analyzing active network traffic streams.
9	Spoofing		I	A digital log entry file that is cryptographically sealed so it can never be modified or deleted once written.
10	Exfiltration		J	The unauthorized transfer or theft of sensitive corporate or personal data from an information system.

PART III: CASE STUDY & SHORT ANSWER

Read the operational scenario below and answer the questions. Be precise and utilize professional digital forensics terminology.

Scenario:

A regional bank detects an active cyberattack inside its core information system at 2:00 AM. A security analyst notices that a server handling financial records is rapidly transferring large volumes of data to an unknown external IP address. The analyst suspects a sophisticated ransomware group has compromised an administrator

account. Out of panic, the local IT administrator walks into the server room and abruptly presses the physical power button to turn off the compromised server.

Questions:

1. The Volatility Mistake:

Explain why the local IT administrator's action (abruptly powering off the server) disrupted standard digital forensics procedures. What critical evidence types were immediately destroyed by this action?

Your answer:

2. Alternative Log Analysis:

Since the local server is now offline, what alternative network-level infrastructure components should the digital forensics team examine to track the data exfiltration path and confirm the destination IP address? (Name at least two sources).

Your answer:

3. Ensuring Admissibility:

When the forensic team clones the hard drives of the server to perform analysis in the laboratory, how do they mathematically prove to a court of law that their copy is identical to the original drive and that no data modification occurred during the investigation?

Your answer:



Unit 8

Digital Forensics in Modern Technologies *Forensic Analysis of Digital Technologies* *and the Presentation of Findings in Cyber* *Investigations*

Text 1. Forensic Analysis of Digital Technologies and the Presentation of Findings

Text 2. Key Targets and Technologies in Cybercrime Investigation

Texts 3. Database Forensics Challenges and Methods

Text 4. The Architecture and Challenges of Cloud Forensics

Text 5. Methodology and Objectives of Malware Forensics

Text 6. Email and Social Media Investigations. Digital Footprints in Communication Networks

Text 7. Mobile Device Forensics. Extracting Evidence from the Pocket

Text 8. The Art of Documentation and Presentation in Digital Forensics

Glossary

Digital forensics — цифрова криміналістика.

Forensic analysis — криміналістичний аналіз / дослідження.

Presentation of findings — представлення (презентація) результатів дослідження.

Cyber investigation — розслідування кіберзлочинів.

Admissible evidence — допустимі докази (*докази, зібрані без порушення закону, які суд приймає до розгляду*).

Data acquisition — збір (вилучення) даних.

Bit-stream image (Forensic image) — побітовий клонований образ диска (*точна копія носія інформації*).

Chain of custody — ланцюжок збереження доказів.

Data integrity — цілісність даних.

Cryptographic hashing — криптографічне хешування (*створення унікального цифрового відбитка файлу*).

Expert witness — експерт-свідок (*фахівець, який дає свідчення та роз'яснення в суді*).

Cross-examination — перехресний допит.

Tamper-evident packaging — упакування з індикацією втручання (*спеціальні сейф-пакети*).

To exculpate — виправдовувати / доводити невинуватість.

To inculpate — інкримінувати / доводити вину.

Live data triage — первинний аналіз «живих» даних (*збір інформації з увімкненого пристрою*).

Forensic workstation — криміналістична робоча станція (*захищений комп'ютер експерта*).

Text

Forensic Analysis of Digital Technologies and the Presentation of Findings

The ultimate goal of digital forensics is not just the technical extraction of data, but the collection of **admissible evidence** that can stand in a court of law. As digital technologies evolve, cyber investigations have become highly complex, requiring a structured approach that balances technical expertise with strict legal compliance. The forensic process typically follows four critical phases: preservation, **data acquisition**, analysis, and the final **presentation of findings**.

During the preservation and acquisition phases, investigators must guarantee **data integrity**. Before any analysis begins on a suspect device, a **bit-stream image** (or forensic duplicate) is created using hardware write-blockers. This ensures that the original evidence remains completely unaltered. To mathematically prove that the copy is identical to the original, investigators utilize **cryptographic hashing** algorithms, such as SHA-256. Any modification to the data, even changing a single character, would completely alter the resulting hash value. Throughout this process, every transfer of the physical or digital media must be documented in a **chain of custody** log to prevent claims of evidence tampering.

However, modern systems often require a different approach known as **live data triage**. When dealing with running servers or encrypted devices, pulling the power plug can permanently destroy volatile RAM data, such as active network connections or temporary encryption keys. Therefore, analysts must carefully extract volatile information while the system is still live, ensuring they do not inadvertently modify critical system logs.

Furthermore, the rise of cloud computing and highly integrated IoT devices has shifted the boundaries of cyber investigations. Forensic specialists can no longer rely solely on physical hard drives; they must legally negotiate multi-jurisdictional data storage and extract remote backups from cloud infrastructures. Mobile devices present another layer of difficulty, forcing experts to use **tamper-evident packaging** or Faraday bags immediately upon seizure to block remote wipe commands.

Once the data is securely captured, the analysis phase begins on a dedicated **forensic workstation**. This phase involves searching for hidden, deleted, or fragmented files, analyzing system registries, and reconstructing timelines of cybercriminal activity. This phase requires impartial objectivity; the forensic analyst looks for data that can either **inculpate** (prove guilt) or **exculpate** (prove innocence) a suspect.

The final and arguably most challenging phase is the **presentation of findings**. A brilliant technical analysis is useless if a judge, jury, or prosecutor cannot understand it. Forensic specialists must translate complex technical logs, hex values, and network architectures into a clear, jargon-free forensic report. Furthermore, digital forensics experts are frequently called into court to serve as an **expert witness**. During **cross-examination**, defense attorneys will rigorously challenge both the

expert's qualifications and the forensic methodology used. They may question the specific validation steps of the forensic software or look for minor gaps in the chain of custody to get the evidence suppressed. Therefore, the ability to clearly communicate how an exploit occurred and how the evidence was protected is just as vital as the technical skill required to find it.

Answer the questions based on the text

1. What is the ultimate goal of digital forensics according to the first paragraph?
2. Which four critical phases define the standard digital forensics process?
3. Why must investigators avoid working directly on the original suspect device?
4. How do cryptographic hashing algorithms mathematically protect digital evidence?
5. What type of documentation prevents defense claims regarding evidence tampering?
6. What is **live data triage** and when is it typically used?
7. What critical data can be permanently lost if a running server is abruptly powered off?
8. How has the rise of cloud computing complicated the legal side of cyber investigations?
9. Why should an investigator place a seized smartphone into a Faraday bag immediately?
10. What is the difference between data that *inculcates* and data that *exculpates* a suspect?
11. Why is a purely technical forensic report often insufficient for a court of law?
12. What challenges does a forensic specialist face during a **cross-examination**?

Exercise 1: Multiple Choice. Choose the correct answer (A, B, C, or D) to complete the sentence or answer the question.

1. Which phase of a cyber investigation ensures that legal guidelines are met and files are not altered during extraction?
A) Cross-examination
B) Presentation of findings
C) Data acquisition
D) Live data triage
2. If an investigator needs to mathematically guarantee that a cloned hard drive has not been modified, they use:
A) Cross-examination
B) Cryptographic hashing
C) Root privileges
D) Tamper-evident packaging
3. Evidence that is collected legally and can be formally introduced in a court of law is called:
A) Admissible evidence

- B) Volatile data
 - C) Inculpatory data
 - D) Traffic metadata
4. A forensic duplicate that represents a sector-by-sector, bit-for-bit copy of physical media is a:
 - A) Live triage report
 - B) SIEM system
 - C) Bit-stream image
 - D) Workstation backup
 5. What must an investigator continuously fill out to document who handled the digital evidence?
 - A) Forensic report
 - B) Cryptographic hash log
 - C) Chain of custody
 - D) Server log file
 6. Evidence that clears a suspect of blame and supports their innocence is said to:
 - A) Obfuscate
 - B) Inculcate
 - C) Exculpate
 - D) Exfiltrate
 7. What is a specialized, secure computer system used by specialists to perform analysis on evidence images?
 - A) Forensic workstation
 - B) Target machine
 - C) Command and control system
 - D) Proxy server
 8. When an analyst extracts temporary encryption keys from the active RAM of a running server, they are performing:
 - A) Database log analysis
 - B) Live data triage
 - C) Cloud log management
 - D) Packet sniffing
 9. A technical specialist who is called into a courtroom to explain digital evidence and answer legal questions is an:
 - A) Expert witness
 - B) Intruder analyst
 - C) Insider witness
 - D) Investigating prosecutor
 10. During a legal trial, the defense attorney asks tough questions to challenge the expert witness's methodology during:
 - A) Data acquisition
 - B) Presentation of findings
 - C) Log correlation

- D) Cross-examination
11. To protect a physical hard drive or smartphone from physical tampering after it is seized, it is placed in:
- A) Faraday workstations
 - B) Tamper-evident packaging
 - C) Multi-jurisdictional safes
 - D) Immutable logging cases
12. Evidence that directly connects a suspect to a cybercrime and points to their guilt is said to:
- A) Exculpate
 - B) Obfuscate
 - C) Inculcate
 - D) Encrypt
13. The stage of a cyber investigation where complex technical data is translated into clear facts for a judge and jury is the:
- A) Presentation of findings
 - B) Data acquisition
 - C) Forensic triage
 - D) Stream reconstruction
14. To make sure that the original hard drive cannot be modified during the cloning process, analysts connect it to a hardware:
- A) Packet sniffer
 - B) Write-blocker
 - C) SIEM system
 - D) C2 channel
15. Maintaining data integrity means ensuring that the extracted evidence remains:
- A) Completely encrypted and hidden
 - B) Accessible via the public internet
 - C) Unaltered, complete, and accurate
 - D) Obfuscated by cloud systems

Exercise 2: True or False. *State whether the following statements are True or False based on professional digital forensics standards.*

1. A bit-stream image includes deleted files and unallocated space, unlike a regular file copy. (**True / False**)
2. If an investigator changes the name of a folder on an evidence drive, the cryptographic hash value stays exactly the same. (**True / False**)
3. Legally admissible evidence must be gathered according to proper legal procedures. (**True / False**)
4. Forensic analysis must be performed directly on the original device whenever possible. (**True / False**)
5. A chain of custody document can have gaps in time as long as the evidence is eventually locked in a lab. (**True / False**)

6. Exculpating evidence is just as important to a forensic analyst as inculpatory evidence. (**True / False**)
7. Live data triage is used when turning off a computer would result in losing critical volatile memory. (**True / False**)
8. During cross-examination, defense lawyers will look for minor documentation mistakes to get digital evidence dismissed. (**True / False**)
9. An expert witness should use a lot of complex technical jargon to ensure the jury understands the depth of the case. (**True / False**)
10. Tamper-evident packaging makes it impossible for someone to open a physical piece of evidence without leaving visible marks. (**True / False**)
11. Cyber investigation processes do not require legal oversight until the evidence is brought into the courtroom. (**True / False**)
12. Data integrity can be legally proven in court by matching the original hash value with the forensic image's hash value. (**True / False**)
13. Forensic workstations should always be connected to the public internet during malware analysis. (**True / False**)
14. The presentation of findings phase is focused on writing technical reports meant exclusively for other IT specialists. (**True / False**)
15. If a single character of data inside a bit-stream image is altered, the SHA-256 hash output changes entirely. (**True / False**)

Exercise 3: Fill in the Gaps. *Fill in the gaps with the most appropriate word or phrase from the box below. Do not use the same phrase twice.*

admissible evidence, expert witness, cross-examination, data acquisition, bit-stream image, forensic workstation, cryptographic hashing, chain of custody, data integrity, presentation of findings, inculcate, exculpate, live data triage, tamper-evident packaging, cyber investigation

1. The investigator carefully placed the suspect's hard drive inside a secure bag with _____ to ensure no one could open it secretly.
2. If you want to use digital logs in a court trial, you must prove they are _____ by showing how they were collected.
3. The technician performed a _____ on the server to extract active network sockets before pulling the power cord.
4. The prosecutor used server log entries to _____ the rogue employee and tie them to the network breach.
5. The digital forensics process failed because there was a two-day gap in the _____ log.
6. Every sector of the computer's solid-state drive was duplicated into a perfect _____.
7. Algorithms like SHA-256 are used in _____ to generate unique digital fingerprints for evidence files.

8. The specialist used a high-performance _____ that was completely isolated from the local office network to run carving tools.
9. The defense attorney tried to weaken the analyst's testimony during a aggressive _____.
- 10.If an administrator modifies a file on a suspect computer after seizing it, the _____ of the evidence is broken.
- 11.The _____ team _____ discovered _____ emails _____ that _____ completely _____ the manager, proving he was out of the country when the attack occurred.
- 12.A comprehensive _____ involves not only finding malicious scripts but also documenting the entire legal process.
- 13.During the _____ stage, the technical lead presented a simplified flowchart showing how the data exfiltration happened.
- 14.The judge asked the _____ to clarify how an SQL Injection vulnerability could expose a company's database.
- 15.The extraction of raw data from a digital device into a secure forensic file format is known as _____.

Exercise 4. Multiple Choice Reading (A, B, C or D). Read the text below. For questions (1-10), choose the correct answer (A, B, C or D).

Key Targets and Technologies in Cybercrime Investigation

In the modern digital era, information systems have become both the instruments and the scenes of crime. To successfully prevent and investigate cybercrimes, law enforcement agencies and forensic specialists must identify specific objects of attention. These key targets include not only traditional physical hardware like hard drives and servers, but also transient digital assets such as volatile RAM data, cloud-based storage, network traffic logs, and encrypted communication channels. Each of these objects requires a distinct methodological approach and specialized technology to ensure that evidence is gathered legally and effectively.

When preventing cyber threats, the primary focus is on proactive monitoring and vulnerability assessment. Artificial Intelligence (AI) and Machine Learning (ML) algorithms are increasingly deployed within Security Information and Event Management (SIEM) systems. These technologies automatically scan vast infrastructure networks to detect early anomalies, such as unauthorized data exfiltration or unusual command patterns, before an actual breach occurs. Furthermore, Intrusion Detection Systems (IDS) act as automated security guards, filtering data in motion and blocking suspicious connections from known malicious IP addresses.

Once a cybercrime is committed, the investigation phase requires reactive digital forensics. Here, the immediate object of attention shifts to volatile data. Because active network connections, running processes, and temporary decryption keys reside inside the computer's Random Access Memory (RAM), they disappear

the moment a machine is powered down. Investigators utilize **live data triage** technologies to securely capture this "data in motion" while the system is still running. Turning off a compromised server abruptly is now considered a critical mistake that can permanently destroy vital evidence.

For static data, or "data at rest," investigators rely on specialized hardware like **write-blockers** to extract a perfect bit-stream image of hard drives without altering a single bit of the original media. To mathematically validate the integrity of this copied data for courtroom presentation, cryptographic hashing algorithms (such as SHA-256) are used to generate a unique digital fingerprint. Ultimately, successful combatting of cybercrime depends on the seamless integration of these automated monitoring systems and strict forensic preservation protocols, turning raw digital footprints into legally admissible evidence.

Questions 1–10

1. According to the first paragraph, what has happened to information systems in the modern era?

- A) They have completely replaced the need for legal warrants.
- B) They act as both the tools used to commit crimes and the crime scenes themselves.
- C) They are used exclusively for traditional physical hardware storage.
- D) They have made network traffic logs obsolete.

2. Which of the following is mentioned as a transient (volatile) digital asset? A) A physical hardware server.

- B) An external backup hard drive.
- C) Volatile RAM data.
- D) A hardware write-blocker device.

3. What is the main focus when trying to *prevent* cyber threats before they happen?

- A) Writing legally binding reports for the court.
- B) Proactive monitoring and vulnerability assessment.
- C) Shutting down servers to wipe the system's memory.
- D) Cross-examining suspects in a laboratory.

4. How do AI and Machine Learning algorithms assist SIEM systems?

- A) By physically capturing smartphones at a crime scene.
- B) By automatically scanning networks to detect early anomalies.
- C) By decrypting HTTPS traffic without cryptographic keys.
- D) By replacing human judges and prosecutors in court.

5. What is the primary function of an Intrusion Detection System (IDS)?

- A) To create a bit-stream image of static hard drives.
- B) To act as an automated guard that filters data in motion and blocks suspicious connections.
- C) To generate SHA-256 digital fingerprints for physical evidence.
- D) To package mobile phones inside specialized Faraday bags.

6. Why is RAM data considered a critical object of attention immediately after a crime?

- A) It contains static corporate files that never change.
- B) It stores active connections, running processes, and encryption keys that vanish when powered off.
- C) It is immune to any anti-forensics tampering techniques.
- D) It can only be extracted using a physical hardware write-blocker.

7. What technique do investigators use to extract volatile information while a server is still running?

- A) Hard drive fragmentation.
- B) Live data triage.
- C) Passive data exfiltration.
- D) Multi-jurisdictional cloud blocking.

8. What does the text describe as a "critical mistake" during an active server investigation?

- A) Using cryptographic hashing to verify data integrity.
- B) Connecting the forensic workstation to an isolated network.
- C) Abruptly turning off a compromised, running server.
- D) Deploying an IDS to monitor incoming traffic.

9. What tool is used to ensure that an original hard drive cannot be modified during the data cloning process?

- A) A proxy server.
- B) An immutable logging system.
- C) A write-blocker.
- D) A Faraday bag.

10. How do forensic specialists mathematically prove to a court that a forensic copy is identical to the original drive?

- A) By presenting a signed confession from the IT administrator.
- B) By utilizing cryptographic hashing algorithms to match digital fingerprints.
- C) By running a DDoS attack against the evidence drive.
- D) By showing that the device was placed in a tamper-evident package.

***Exercise 5. Match the Words with their Meanings.** Choose a definition (A–L) that matches the meaning of each English term (1–12).

Words

Meanings

- | | |
|------------------------|---|
| 1. Volatile data | A The absolute assurance that digital evidence has remained unaltered, complete, and accurate. |
| 2. Data exfiltration | B A unique digital code generated by an algorithm that acts as an unchangeable identity mark for a file. |
| 3. Write-blocker | C The legal and technical process of collecting temporary data from a device while it is still running. |
| 4. Admissible evidence | D Information stored in RAM that is temporary and |

Words	Meanings
	vanishes completely once the power source is disconnected.
5. Data integrity	E Automated technology that monitors network infrastructure to spot security weak points and early threats.
6. Bit-stream image	F An unauthorized transfer or theft of sensitive data from a secure corporate or institutional network.
7. Cryptographic hash	G A hardware tool that prevents a computer from making any modifications to an original evidence drive during cloning.
8. Live data triage	H Systems that act as security guards, filtering data packets in motion and blocking malicious IP connections.
9. Vulnerability assessment	I Information and digital artifacts that are legally collected and accepted by a judge to be used during a trial.
10. Intrusion Detection System (IDS)	J A sector-by-sector, bit-for-bit exact forensic duplicate of a physical storage device.
11. Incident response	K The phase where investigators search for hidden data, reconstruct timelines, and identify cybercriminal tracks.
12. Forensic analysis	L An organized, structured plan of action taken by specialists to contain, manage, and mitigate a cyberattack.

*** Exercise 6. Translate into English.** *Translate the given words, expressions and sentences into English, based on the vocabulary of the text.*

Part A: Термінологічні вирази

1. Допустимі докази — _____
2. Збір (вилучення) даних — _____
3. Побітовий клонований образ диска — _____
4. Ланцюжок збереження доказів — _____
5. Первинний аналіз «живих» даних — _____
6. Криптографічне хешування — _____
7. Упакування з індикацією втручання — _____
8. Оцінка вразливостей — _____
9. Викрадення (несанкціоноване вилучення) даних — _____
10. Експерт-свідок — _____

Part B: Професійні речення

11. Вимкнення зламаного сервера знищить критично важливі дані в оперативній пам'яті (RAM).
12. Спеціалісти використовують апаратні блокіратори запису для захисту цілісності даних.
13. Кожна зміна цифрового доказу повністю змінить кінцеве хеш-значення.
14. Головна мета цифрової криміналістики — зібрати докази, які витримають перевірку в суді.

15. Під час перехресного допиту адвокати захисту будуть ретельно перевіряти методику розслідування.

***Exercise 7.** *Read the texts below. Match choices (A–H) to the texts (1–5). There are **three** choices you do not need to use.*

Texts: Database Forensics Challenges and Methods

1. _____

Unlike traditional file system analysis, investigating an active database requires careful extraction of volatile memory structures. If a malicious user executes an unauthorized query and immediately logs out, the proof of this connection often resides exclusively in the system's transaction cache or buffer pool. Powering down the SQL server abruptly to pull a static image would flush these dynamic tables instantly, erasing critical IP footprints and temporary session keys. Investigators must perform memory carving while the engine is running.

2. _____

When auditing corporate fraud, investigators frequently encounter "data at rest" modification anomalies. Savvy insiders often execute raw UPDATE or DELETE statements directly inside the relational engine, bypass standard application logs, and then clean up the user history. To reconstruct what happened, a forensic specialist must dive into the database transaction logs (such as SQL Server's .ldf or Oracle's Redo logs). These files serve as a chronological black box, recording every single physical modification before it is permanently committed to the data files.

3. _____

A major hurdle in contemporary database forensics is identifying tampered or completely falsified entries within multi-layered environments. In financial cybercrimes, attackers might manipulate currency balances and alter database metadata to obscure the timestamp of the transaction. To establish data integrity for legal presentation, examiners run automated integrity checkers and recalculate internal page-level checksums. If a single byte within a database table block has been manipulated manually, the internal checksum will mismatch, exposing the illicit alteration.

4. _____

With companies migrating their core infrastructures to platforms like AWS RDS or Azure SQL, the physical boundaries of database investigations have faded. Forensics experts no longer have physical access to the underlying hard drives, write-blockers cannot be plugged in, and sector-by-sector cloning is impossible. Analysts must adapt by relying strictly on cloud-native logging protocols, control-plane APIs, and remote database auditing features to reconstruct malicious access, introducing complex multi-jurisdictional legal challenges.

5. _____

One of the trickiest aspects of database analysis involves identifying and reconstructing "dropped" or deleted records. When a row is removed from a database table, the database management system (DBMS) typically marks that specific storage

slot as "free" or unallocated rather than wiping the actual data bytes instantly. Using hex editors and specialized parsing tools, a forensic analyst can scan these unallocated pages to carve out deleted texts, hidden index keys, and fragments of past transactions before new data overwrites them.

Choices A–H

- A) Analyzing Transaction Logs to Reconstruct Chronological Fraud Activities
- B) Implementing Advanced Firewalls to Prevent SQL Injection Exploits
- C) Recovering Scratched and Overwritten Hard Drive Platters Physically
- D) The Volatility of Buffer Pools and the Risks of Abrupt Server Shutdowns
- E) Carving and Extracting Dropped Table Rows from Unallocated Database Pages
- F) Utilizing Cryptographic Checksums to Detect Metadata and Page Tampering
- G) Migrating Legacy Database Infrastructures to High-Speed Hybrid Storage Systems
- H) Investigating Database Incidents within Virtualized and Managed Cloud Environments

Exercise 8. Put the words in the correct order:

1. forensics / system / data / database / motion / investigates / in.
2. RAM / server / down / flushes / volatile / dynamic / tables / powering / the.
3. transactions / chronological / log / records / files / database / modifications / all.
4. specialists / transaction / audit / for / logs / examine / corporate / fraud.
5. checksums / detect / page / internal / automated / tampering / help / to.
6. unallocated / deleted / can / experts / pages / from / records / carve.
7. cloud / access / do / have / physical / servers / investigators / not / to.
8. write-blockers / original / cloning / used / protect / are / data / during / to.
9. modification / hash / any / value / database / changes / the / cryptographic.
10. chain / custody / must / documented / of / be / meticulously / every / step.
11. expert / translated / terms / witness / the / technical / complex / judge / for / the.
12. tools / forensic / tables / analyze / to / relational / used / are / logs.
13. software / integrity / legal / requirements / tools / must / formal / meet.
14. database / metadata / attackers / alter / transaction / timestamps / to / manipulate.
15. live / extraction / triage / structures / memory / active / requires / data.

Exercise 9: Match the English terms with their Ukrainian equivalents

Directions: Match the English professional term on the left (1–15) with its exact Ukrainian forensic equivalent on the right (A–O).

№	English Term	Forensic	Letter	Ukrainian Equivalent
1	Database forensics		A	Первинний аналіз «живих» даних
2	Transaction cache		B	Посторінкова контрольна сума
3	Relational engine		C	Нерозподілені сторінки бази даних
4	Chronological black box		D	Тимчасові сесійні ключі
5	Data at rest		E	Видалені (скинуті) рядки таблиці
6	Page-level checksum		F	Кеш транзакцій (буферний пул)
7	Falsified entries		G	Криміналістичне дослідження баз даних
8	Unallocated database pages		H	Реляційний механізм (двигун БД)
9	Cloud-native logging		I	Дані у стані спокою (збережені дані)
10	Dropped table rows		J	Підроблені (сфальсифіковані) записи
11	Temporary session keys		K	Хронологічна «чорна скринька»
12	Live data triage		L	Вбудоване (нативне) логування в хмарі
13	Hex editor		M	Перехресний допит (у суді)
14	Expert witness		N	Шістнадцятковий редактор (хекс-редактор)
15	Cross-examination		O	Експерт-свідок

Exercise 10. Read the text and answer the questions.

Text: The Architecture and Challenges of Cloud Forensics

The rapid migration of corporate data to remote environments has fundamentally altered the landscape of digital investigations. **Cloud forensics** — a specialized sub-discipline of digital forensics — involves the preservation, acquisition, and analysis of digital evidence stored in cloud computing infrastructures. Unlike traditional hardware forensics, where an investigator exercises complete physical control over a suspect's hard drive, cloud environments present a virtualized, multi-tenant landscape where data is distributed across dynamic, remote servers.

[Diagram mapping cloud service deployment models SaaS PaaS IaaS and forensic data access levels]

The primary obstacle in cloud investigations is the loss of physical control. When data resides in the cloud, standard protocols like connecting a physical **write-blocker** to extract a sector-by-sector **bit-stream image** are completely impossible. Instead, investigators must rely on the cooperation of Cloud Service Providers (CSPs) and utilize API-driven data acquisition. The level of forensic access depends heavily on the cloud deployment model:

- **Software as a Service (SaaS):** The investigator has the least control, relying almost entirely on logs provided by the CSP (e.g., mail server access logs).
- **Platform as a Service (PaaS):** Access is limited to application logs and database configurations.
- **Infrastructure as a Service (IaaS):** This provides the highest level of forensic control, allowing investigators to capture virtual machine (VM) snapshots and volatile RAM data from virtualized environments.

Data volatility and multi-tenancy introduce severe legal and technical risks. In a multi-tenant cloud environment, a single physical server hosts data belonging to hundreds of different companies or individuals. Extracting an entire physical hard drive from a data center would violate the privacy and human rights of innocent third parties, making the evidence inadmissible in court. Therefore, analysts must perform scoped extractions.

Furthermore, data in the cloud is highly ephemeral; logs rotate quickly, and virtual instances can be deleted permanently with a single command. To prove **data integrity** during legal presentation, investigators must immediately calculate cryptographic hashes of the extracted cloud logs and maintain a flawless **chain of custody**, documenting every digital API call and transfer of information.

Finally, **jurisdictional challenges** often complicate cloud investigations. A suspect might be located in Ukraine, while the malicious actions were executed using a SaaS platform hosted in Germany, and the actual physical server storing the encrypted data logs is located in the United States. Navigating international legal frameworks and executing cross-border data requests requires significant time, during which vital digital footprints can be completely overwritten or purged by automated cloud optimization algorithms.

Questions:

1. How does the text define the sub-discipline of **cloud forensics**?
2. What is the fundamental difference between traditional hardware forensics and cloud forensics regarding physical control?
3. Why are traditional tools like hardware write-blockers and bit-stream images ineffective in cloud investigations?
4. Which cloud deployment model (SaaS, PaaS, or IaaS) grants forensic analysts the highest level of control, and why?
5. What is a "multi-tenant environment," and what unique challenge does it present to investigators?
6. Why is traditional full-disk extraction legally problematic in a multi-tenant cloud infrastructure?
7. What does the term "ephemeral data" imply in the context of cloud logging systems?
8. How do cyber investigators mathematically validate the integrity of extracted cloud data logs?
9. Explain the multi-jurisdictional scenario described in the final paragraph of the text.
10. What can happen to vital cloud logs while investigators are waiting for international legal requests to clear?

Exercise 11. Write True if the statement matches the information in the text, or False if it contradicts the text.

1. Cloud forensics is considered a specialized sub-discipline of digital forensics. (**True / False**)
2. Investigators in cloud forensics exercise the same physical control over hard drives as they do in traditional hardware forensics. (**True / False**)
3. Standard physical write-blockers can easily be used to clone cloud infrastructure sector-by-sector. (**True / False**)
4. Cloud service deployment models significantly impact the level of forensic access available to analysts. (**True / False**)
5. The Software as a Service (SaaS) model provides investigators with the highest level of forensic control. (**True / False**)
6. Virtual machine snapshots and volatile RAM can be captured effectively within an IaaS infrastructure. (**True / False**)
7. Multi-tenancy means that a single physical server is dedicated strictly to one corporate client. (**True / False**)
8. Extracting an entire physical hard drive from a multi-tenant data center could violate human rights and privacy laws. (**True / False**)
9. Scoped extractions are used by analysts to avoid collecting data from innocent third parties. (**True / False**)
10. Data in cloud environments is long-lasting and completely safe from sudden deletion. (**True / False**)

- 11.To ensure data integrity for legal presentation, examiners immediately calculate cryptographic hashes of extracted logs. (**True / False**)
- 12.The "chain of custody" is only important for physical evidence, not for digital API calls. (**True / False**)
- 13.Physical cloud servers are always located within the same legal jurisdiction as the suspect. (**True / False**)
- 14.Automated cloud optimization algorithms can purge or overwrite vital digital footprints while legal requests are processed. (**True / False**)

***Exercise 12. Match the Words with their Meanings.** Match each English term or expression (1–14) with its correct professional definition (A–N).

	Cloud Forensics Term			Definition / Meaning
1	Cloud forensics		A	Data that is temporary, short-lived, and can be easily overwritten or deleted permanently by automated algorithms.
2	Multi-tenancy		B	A cloud model where investigators only have access to basic application logs and database setups, but no OS control.
3	Scoped extraction		C	Legal challenges that arise because digital footprints, suspects, and hardware servers are located in different countries.
4	Ephemeral data		D	A specialized sub-discipline that involves recovering and analyzing evidence from virtualized, remote environments.
5	Platform as a Service (PaaS)		E	A cloud model that grants the highest level of forensic control, including virtual machine snapshots and RAM captures.
6	Jurisdictional challenges		F	The absolute assurance that digital evidence has not been tampered with or modified since its collection.
7	Data integrity		G	A process where data is gathered remotely using system commands and endpoints rather than physical write-blockers.

	Cloud Forensics Term			Definition / Meaning
8	Infrastructure as a Service (IaaS)		H	A dynamic architectural model where a single physical server hosts data belonging to multiple independent clients.
9	Software as a Service (SaaS)		I	A certified log that records every single digital API call, access, and transfer of digital evidence during an investigation.
10	API-driven data acquisition		J	A targeted, limited extraction of specific files designed to protect the privacy rights of innocent third parties.
11	Chain of custody log		K	A virtual copy of a specific point in time that preserves the exact state of a virtual server's operating system.
12	Virtual machine snapshot		L	Companies that host remote environments (like AWS or Microsoft Azure) and must cooperate with law enforcement during a case.
13	Cloud Service Providers (CSPs)		M	The process of automatically replacing or cleaning out old log files to save space inside an information system.
14	Log rotation		N	A cloud model where investigators have the least control, relying strictly on user-level access history provided by the vendor.

*** Exercise 13. Translate into English.** *Translate the given words, professional phrases, and sentences into English using cloud forensics vocabulary.*

Part A: Спеціалізовані вирази

1. Хмарна криміналістика — _____
2. Багатоорендне середовище (спільне використання сервера) — _____
3. Обмежене (вибіркове) вилучення даних — _____
4. Мінливі / ефемерні дані — _____
5. Юрисдикційні проблеми (законодавчі перешкоди) — _____
6. Знімок віртуальної машини — _____
7. Провайдери хмарних послуг — _____

8. Збір даних через API — _____
9. Повне вилучення диска — _____
10. Ротація логів (журналів подій) — _____

Part B: Професійні речення

11. Традиційні апаратні блокіратори запису абсолютно неможливо підключити до хмарної інфраструктури.
12. Вилучення всього фізичного диска з дата-центру порушило б права людини сторонніх осіб.
13. Спеціалісти повинні негайно розрахувати криптографічні хеші для підтвердження цілісності даних.
14. Модель розгортання «Інфраструктура як сервіс» (IaaS) забезпечує найвищий рівень криміналістичного контролю.

Glossary

Malware Forensics

Malware forensics — криміналістичне дослідження шкідливого програмного забезпечення (ПЗ).

Static analysis — статичний аналіз (*дослідження коду програми без її фактичного запуску*).

Dynamic analysis (Behavioral analysis) — динамічний (поведінковий) аналіз (*спостереження за програмою під час її виконання*).

Sandboxing — ізольоване середовище («пісочниця») (*запуск шкідливого ПЗ у безпечній системі*).

Reverse engineering — зворотне проектування (реверс-інжиніринг / декомпіляція).

Disassembler — дизасемблер (*інструмент, що переводить бінарний код у текстовий формат асемблера*).

Debugger — відладчик (дебагер) (*програма для покрокового контролю виконання коду*).

Indicators of Compromise (IoCs) — індикатори компрометації (*цифрові сліди атаки, як-от IP-адреси чи хеші файлів*).

Command and Control (C2) server — сервер керування та контролю (*командний сервер хакерів*).

Obfuscation — обфускація (*навмисне заплутування коду зловмисниками для ускладнення аналізу*).

Packed malware — упаковане (стиснене) шкідливе ПЗ.

Signature matching — зіставлення сигнатур (*пошук відомих шматочків коду вірусів*).

YARA rules — правила YARA (*інструмент для ідентифікації та класифікації шкідливих файлів*).

Process injection — ін'єкція процесу (*приховане впровадження шкідливого коду в легітимну програму*).

Persistence mechanism — механізм закріплення в системі (спосіб, яким вірус виживає після перезавантаження ПК).

***Exercise 14. Read the text and answer the questions.**

Text

Methodology and Objectives of Malware Forensics

When an information system is breached, finding out *how* the malicious code operated is the job of **malware forensics**. This specialized discipline focuses on isolating, dissecting, and understanding malicious software, such as ransomware, trojans, or spyware, to determine its intent, origin, and impact on the infrastructure. To safely examine malware without threatening the production network, forensic analysts rely on two primary methodologies: **static analysis** and **dynamic analysis**.

The investigation usually begins with static analysis. Here, analysts inspect the binary file without executing it. They extract basic metadata, calculate the cryptographic hash, and search for specific text strings, such as hardcoded IP addresses or registry pathways. To dig deeper into compiled binaries, investigators use a **disassembler** to translate machine code into human-readable assembly language, or tools for **reverse engineering** to reconstruct the original logic.

However, cybercriminals frequently deploy defense mechanisms to delay investigations. They use **obfuscation** to confuse code structures or distribute **packed malware** that hides the actual malicious payload inside a compressed layer. To bypass these tricks, analysts switch to dynamic analysis, executing the file inside a heavily monitored, isolated network environment known as a **sandbox**.

During dynamic analysis, a **debugger** allows the investigator to monitor the program's behavior step-by-step. The focus shifts to discovering how the virus interacts with the operating system: Does it create a hidden **persistence mechanism** in the Windows Registry to survive reboots? Does it perform **process injection** to hide inside clean system tasks? Crucially, dynamic analysis uncovers network activities, exposing the hidden **Command and Control (C2) server** used by attackers to exfiltrate database records.

The ultimate goal of malware forensics is to extract **Indicators of Compromise (IoCs)**. By documenting unique file extensions, malicious IP addresses, and registry keys, analysts can create custom **YARA rules**. These rules act as digital alerts, enabling the security team to perform automated **signature matching** across the entire enterprise network to prevent future infections and ensure system protection.

Answer the questions based on the text

1. What is the primary objective of **malware forensics** during a system breach investigation?
2. What are the two core technical methodologies used by forensic analysts to study malicious code?

3. What specific data can investigators find during the initial static analysis phase?
4. What is the difference between how a disassembler is used and how reverse engineering is applied?
5. Why do cybercriminals use **obfuscation** and packing techniques on their software?
6. What is a **sandbox** and why is it essential for performing dynamic analysis safely?
7. What system changes do investigators look for when searching for a **persistence mechanism**?
8. How does a **process injection** attack help a virus escape detection by basic antivirus scanners?
9. Why is identifying a **Command and Control (C2) server** a major breakthrough in an investigation?

***Exercise 15. Put the words in the correct order**

1. forensics / code / how / operated / malware / discovers / malicious.
2. without / file / static / executable / analyzes / analysis / running / the.
3. reverse / logic / programming / engineering / reconstructs / original / the / software.
4. obfuscation / code / use / cybercriminals / structures / to / confuse.
5. payloads / malicious / packed / inside / malware / compression / hides / layers.
6. isolated / sandbox / execution / secure / environments / provide / malware / for.
7. debugger / code / step-by-step / interactive / execution / monitors / a / running.
8. registry / keys / hidden / mechanism / create / persistence / malware / a.
9. system / process / injects / code / injection / clean / into / malicious / tasks.
10. database / C2 / exfiltrate / servers / channels / provide / records / to.
11. custom / alerts / YARA / security / generate / rules / to / digital.
12. alerts / signature / matching / known / flags / threat / patterns / based / on.
13. workstation / forensic / network / from / production / isolated / stays / the.
14. analysts / indicators / extract / of / compromise / security / system / for.

Exercise 16. Fill in the Gaps. *Fill in the gaps in the sentences with the appropriate professional terms from the reference book. Each expression can only be used once.*

reference book

static analysis, dynamic analysis, sandbox, reverse engineering, obfuscation, packed malware, debugger, persistence mechanism, process injection, C2 server, Indicators of Compromise, YARA rules

1. To prevent the virus from spreading to the corporate network, analysts executed the sample inside an isolated _____.
2. Cybercriminals applied advanced _____ to mask the text strings and make the code unreadable.

3. Investigators check the startup registry paths to see if the trojan established a _____.
4. During _____, the specialist monitors how the running file interacts with the active operating system.
5. The security system flagged a malicious IP address and file hash, which are critical _____.
6. To inspect a binary without executing its dangerous payload, you must perform _____ first.
7. The ransomware used a technique called _____ to execute its payload inside the legitimate explorer.exe process.
8. Analysts use an interactive _____ to set breakpoints and control code execution step-by-step.
9. Because the file was distributed as _____, the static scanner could not read the compressed internal headers.
10. The team deployed custom _____ to scan the entire network infrastructure for specific malware signatures.
11. The network log analysis revealed that the compromised machine was communicating directly with an overseas _____.
12. High-level experts perform _____ to decompile binary components and reconstruct the software's original source logic.

Exercise 17. Match the English terms with their Ukrainian equivalents

	English Term	Forensic		Ukrainian Equivalent
1	Static analysis		A	Індикатори компрометації (цифрові сліди атаки)
2	Sandboxing		B	Обфускація (навмисне заплутування коду)
3	Reverse engineering		C	Статичний аналіз (дослідження без запуску)
4	Obfuscation		D	Сервер керування та контролю (командний сервер)
5	Packed malware		E	Механізм закріплення (виживання) в системі
6	Debugger		F	Ізольоване середовище («пісочниця»)

	English Forensic Term			Ukrainian Equivalent
7	Persistence mechanism		G	Зворотнє проектування (реверс-інжиніринг)
8	Process injection		H	Упаковане (стиснене) шкідливе ПЗ
9	C2 server		I	Відладчик (дебагер для покрокового контролю)
10	Indicators of Compromise		J	Ін'єкція процесу (впровадження в іншу програму)

Exercise 18. Read the text below. For questions (1–10), choose the correct answer (A, B, C or D).

Email and Social Media Investigations Digital Footprints in Communication Networks

The investigation of electronic communication platforms has become a cornerstone of modern digital forensics. When cybercriminals orchestrate phishing campaigns, corporate espionage, or online harassment, they inevitably leave footprints within email infrastructures and social media ecosystems. For forensic examiners, extracting and preserving this data requires a combination of network analysis, metadata parsing, and strict adherence to legal standards to ensure the evidence remains admissible in court.

Email forensics typically begins not with the visible text of the message, but with the hidden **email header**. While a casual user only sees the sender's name and the message body, the header contains a technical log of the email's entire journey across the Internet. Analysts parse this data to extract **MIME parameters**, unique Message-IDs, and the sequence of **Received headers**. These logs display the exact IP addresses of the mail transfer agents (MTAs) that handled the file. By tracing these routing lines backward, an investigator can discover the original outbound server used by the attacker, effectively defeating simple display-name spoofing tricks where an email pretends to come from a trusted financial institution.

However, modern email security protocols like **SPF (Sender Policy Framework)**, **DKIM (DomainKeys Identified Mail)**, and **DMARC** complicate simple deception. DKIM, for instance, attaches a unique cryptographic signature to the email header. If an attacker intercepts the email in transit and alters its text or attachments, the cryptographic verification will fail automatically. For a forensic investigator, verifying a valid DKIM signature mathematically proves **data integrity** — confirming that the evidence has remained completely unaltered since it was dispatched by the sender's server.

Investigating social media platforms (such as Meta, X, or Telegram) introduces a shift from server logs to **OSINT (Open Source Intelligence)** and API data extraction. When a suspect deletes a threatening post or a fraudulent direct message, the data often vanishes from public view, but it does not disappear instantly from the platform's underlying databases. Analysts utilize targeted web-scraping tools and legal sub-poenas to request institutional data packets directly from social media corporations.

Furthermore, social media files are rich in hidden **metadata**. For example, when a suspect uploads an image of stolen corporate documents to a social platform, the image file may still contain embedded **EXIF data**. This hidden layer can store the exact brand and model of the smartphone camera used, the precise date and time of the photo, and even the global **GPS coordinates** of the physical room where the document was photographed. Combined with a meticulously documented **chain of custody log** that notes every step of the digital collection process, this metadata provides prosecutor teams with undeniable proof linking a physical individual to a specific cyber incident.

Multiple Choice Questions:

1. According to the first paragraph, what is required to ensure that communication evidence can be used during a trial?

- A) Using open-source web-scraping applications exclusively.
- B) Complete reliance on the visible text of a message.
- C) A combination of technical analysis and strict compliance with legal frameworks.
- D) Immediately deleting the suspect's social media ecosystem.

2. Where do forensic examiners look first to trace the routing history of a suspicious email?

- A) The visible text body of the message.
- B) The hidden email header logs.
- C) The recipient's local desktop background.
- D) Public social media timelines.

3. What specific information can be uncovered by analyzing the sequence of "Received" headers?

- A) The smartphone camera brand used by the suspect.
- B) The exact physical room address of the recipient.
- C) The IP addresses of the mail transfer agents that processed the email.
- D) The deleted direct messages from a social media account.

4. Display-name spoofing is a technique where an attacker:

- A) Permanently deletes all email traffic from a corporate server.
- B) Makes an email fake its sender identity to look like a trusted entity.
- C) Attaches a valid cryptographic signature to a file.
- D) Extracts GPS coordinates from an uploaded image.

5. How does the DKIM protocol help a forensic investigator validate data integrity?

- A) It automatically deletes spam messages before they reach the user.
- B) It provides the physical location of the attacker's house.
- C) It uses a cryptographic signature that fails if the message was altered in transit.
- D) It blocks the police from accessing private mail transfer agents.

6. What happens when a suspect deletes a fraudulent message from a social media platform?

- A) It is permanently wiped from all corporate servers around the world within one millisecond.
- B) It disappears from public view but often remains stored within the platform's databases.
- C) The investigator must use a hardware write-blocker on the smartphone to see it publicly.
- D) The DMARC security protocol automatically republishes it.

7. To collect hidden institutional data packets from social media companies, law enforcement must use:

- A) Simple display-name spoofing tricks.
- B) Traditional sector-by-sector hard drive cloning tools.
- C) Legal subpoenas and API data extraction.
- D) Automated email routing protocols.

8. What type of hidden information is stored inside EXIF data layers of an uploaded photo?

- A) Mail transfer agent routing pathways and MIME parameters.
- B) Technical camera specifications, timestamps, and GPS coordinates.
- C) Automated DMARC optimization algorithms.
- D) The password history of the suspect's email account.

9. Why are GPS coordinates in image metadata highly valuable for an investigation?

- A) They automatically prove that a DKIM signature is invalid.
- B) They pinpoint the physical location where the digital photograph was taken.
- C) They allow analysts to bypass the need for a chain of custody.
- D) They convert machine code into readable assembly language.

10. What is the main purpose of a meticulously documented chain of custody log?

- A) To scrape public information from open-source intelligence websites.
- B) To ensure the email server rotates its log files more frequently.
- C) To legally prove that digital evidence was collected and handled without tampering.
- D) To encrypt the data transfer packets during cloud migration.

Exercise 19. Fill in the Gaps. Fill in the gaps in the sentences with the appropriate professional term from the box. Each term can be used only once.

email header, MIME parameters, Message-ID, Received headers, mail transfer agents, display-name spoofing, SPF, DKIM, DMARC, OSINT, web-scraping, EXIF data, GPS coordinates, chain of custody log

1. To hide their true identity, the scammer used _____ so that the email appeared to come from the official bank support.
2. The investigator parsed the hidden _____ to view the routing history of the message across the internet.
3. Every legitimate email contains a unique _____ in its metadata that acts as a digital serial number for that specific message.
4. Analysts track the chronological path of an email by reading the sequence of _____ from bottom to top.
5. In the header, the IP addresses belongs to the various _____ that forwarded the electronic file across networks.
6. The digital signature protocol known as _____ uses cryptographic keys to prove that an email was not altered in transit.
7. To verify if the sending server was actually authorized by the domain owner, examiners check the _____ records in the DNS.
8. Security frameworks like _____ help organizations set strict rules on how to handle emails that fail cryptographic authentication.
9. Information about the formatting, character sets, and file attachments of an email is defined within the _____.
10. When gathering public information from a suspect's open social media profiles, investigators rely on _____ techniques.
11. To collect thousands of public posts and comments automatically for timeline reconstruction, analysts use specialized _____ tools.
12. When a suspect uploads an original digital photograph, forensic tools can extract hidden _____ embedded inside the image file.
13. The camera metadata was so precise that it exposed the exact global _____ of the room where the documents were stolen.
14. To make sure the evidence is admitted in court, the forensic team must document every transfer of the files in a detailed _____.

Exercise 20. Match the Words (1–14) with their Meanings (A–N).

	Forensic Term			Technical / Legal Definition
1	Email header		A	A specific security protocol that attaches a verifiable cryptographic signature to an email to guarantee its integrity.
2	Display-name spoofing		B	Hidden metadata embedded within image files that contains camera details, creation time, and hardware settings.
3	Received headers		C	A technical log at the top of an email containing routing paths, timestamps, and server configuration details.
4	Mail transfer agents (MTAs)		D	Automated software-driven collection of data from web pages and social media platforms to preserve public evidence.
5	DKIM		E	A deceptive technique where an attacker changes the visible sender name to trick the victim into trusting the message.
6	SPF		F	Global satellite positioning data embedded in metadata that pinpoints the exact physical location where a file was created.
7	EXIF data		G	A chronological sequence of metadata lines showing every single server an email passed through on its journey.
8	GPS coordinates		H	Open-source intelligence methodology used to gather legally available public information from internet ecosystems.
9	Chain of custody log		I	Software applications and servers that are responsible for routing, transferring, and delivering emails between networks.
10	OSINT		J	A DNS-based authentication protocol that lists which specific IP addresses are legally allowed to send emails for a domain.

	Forensic Term			Technical / Legal Definition
11	Web-scraping		K	A strict, unalterable document that tracks who collected, accessed, and handled digital evidence from the crime scene to the courtroom.
12	Message-ID		L	A globally unique string of characters assigned to an email by the outbound mail server to differentiate it from all others.
13	MIME parameters		M	Standards that define how non-text attachments, audio, video, and different language encodings are structured within an email.
14	DMARC		N	A comprehensive protocol that links SPF and DKIM together, giving domain owners instructions on how to block unauthorized emails.

Exercise 21. Read the sentences below. Each sentence contains one professional, factual, or grammatical mistake related to digital forensics. Find the mistake and write the corrected version of the sentence.

1. Email headers is completely useless for investigators because they only show the visible text body of a message.
2. Forensic examiners check the sequence of MIME parameters to track the chronological IP routing path of an email.
3. Display-name spoofing is a cryptographic protocol that mathematically secures an email against interception.
4. The Message-ID is a unique physical address of the computer hardware that sent the original email file.
5. Mail transfer agents are human law enforcement specialists who manually carry digital logs to the courtroom.
6. If an attacker alters an email attachment in transit, the digital DKIM signature validation will pass successfully.
7. To verify if a remote server is legally authorized to send emails for a specific domain, analysts check the OSINT records.
8. Web-scraping is a hardware tool used to physically clone a suspect's smartphone inside a digital lab.
9. Delete social media posts disappear instantly from all underlying corporate databases the exact millisecond a user clicks delete.

10. EXIF data layers are stored inside email headers to define the language encoding characters of the text.
11. GPS coordinates embedded in a digital photograph can pinpoint the exact camera serial number used by the suspect.
12. A chain of custody log is only necessary for physical evidence like weapons, and it are completely ignored in digital investigations.
13. Security frameworks like DMARC are used to extract hidden location data from files uploaded to social media.
14. Investigators use OSINT methodologies to extract private, password-protected databases from encrypted cloud networks.

Exercise 22. Read the text below. Choose from (A–H) the one which best fits each space (1–6). There are two choices you do not need to use.

Mobile Device Forensics. Extracting Evidence from the Pocket

In the modern digital era, smartphones have become the primary repositories of personal and professional data. Consequently, mobile device forensics has grown into a vital branch of digital investigations, dealing with the recovery of digital evidence from smartphones, tablets, and wearable tech. Unlike traditional computer forensics, where data remains relatively static on a hard drive, mobile devices are dynamic ecosystems (1).

The extraction process always begins with a critical step: isolating the device from all wireless networks. If a seized smartphone connects to a cellular tower or Wi-Fi network, an associate of the suspect could trigger a remote-wipe command, (2). To prevent this, forensic analysts immediately place the phone into a **Faraday bag**, an enclosure that blocks all radio frequency signals, or switch the device into airplane mode if it is unlocked.

Once the device is securely isolated, investigators must choose between two primary data acquisition methodologies: logical extraction and physical extraction. A logical extraction is faster and safer; it communicates with the device's operating system to copy visible files, such as contacts, call logs, and media. However, this method cannot access modified system areas (3).

To dig deeper, experts perform a physical extraction. This advanced process bypasses the operating system entirely to create a sector-by-sector bit-stream clone of the underlying flash memory. Physical extraction is highly valued by prosecutors because (4), allowing examiners to recover deleted chat history from encrypted messengers, unallocated database fragments, and hidden system logs.

The ultimate challenge in mobile forensics is encryption. Modern smartphone operating systems utilize file-based encryption by default, meaning that without the user's passcode or biometric data, the extracted memory dump remains an unreadable scrambled mess. To crack these defenses, digital labs utilize specialized hardware-software suites (5).

Throughout this complex procedure, maintaining a flawless **chain of custody log** is mandatory. Every single action—from the second the phone is dropped into the

Faraday bag to the final compilation of the forensic report—must be documented. This level of precision ensures (6), proving to the court that the evidence was not manipulated, altered, or fabricated during the investigation.

Choices (A–H)

- A) that the digital evidence remains legally admissible during a trial
- B) which can permanently destroy all files and application databases before police can read them
- C) it allows for the recovery of bypassed hardware hardware-software suites
- D) it captures the entire flash memory including deleted data rows
- E) that constantly update, sync, and overwrite information in real time
- F) which are capable of executing automated brute-force attacks to guess the lock screen PIN
- G) or extract files that have been deleted by the user
- H) to physically clone a suspect's smartphone inside a traditional data center

Exercise 23. True or False Read the statements below. Write True if the statement is factually and technically correct based on the text, or False if it contains an error.

1. Mobile device forensics deals with recovering evidence from smartphones, tablets, and wearable tech. (**True / False**)
2. Unlike traditional computer forensics, data on mobile devices remains completely static. (**True / False**)
3. Isolating a seized smartphone from wireless networks is done to prevent a remote-wipe command. (**True / False**)
4. A Faraday bag is a special tool used to charge a smartphone's battery during a raid. (**True / False**)
5. Faraday bags work by blocking all radio frequency signals from reaching the device. (**True / False**)
6. Logical extraction is a slower and more dangerous method than physical extraction. (**True / False**)
7. A logical extraction communicates with the operating system to copy visible files like call logs and contacts. (**True / False**)
8. Logical extraction can easily recover files that have been permanently deleted by the user. (**True / False**)
9. Physical extraction creates a sector-by-sector bit-stream clone of the underlying flash memory. (**True / False**)
10. Physical extraction bypasses the operating system entirely to gather unallocated database fragments. (**True / False**)
11. Modern smartphone operating systems turn off file-based encryption by default. (**True / False**)
12. Without a user's passcode or biometric data, an encrypted memory dump looks like a scrambled mess. (**True / False**)

13. Automated brute-force attacks are used by digital labs to guess the lock screen PIN of a device. (**True / False**)
14. A chain of custody log is optional and only used if the smartphone belongs to a violent criminal. (**True / False**)

Exercise 24. Fill in the gaps in the sentences with the appropriate professional term from the box. Each term can be used only once.

mobile device forensics, dynamic ecosystems, remote-wipe, Faraday bag, radio frequency signals, logical extraction, physical extraction, bit-stream clone, flash memory, file-based encryption, memory dump, hardware-software suites, brute-force attacks, chain of custody log

1. To investigate a suspect's tablet, the detective specialized in _____ was called to the scene.
2. Smartphones are considered _____ because they constantly update, sync, and overwrite information.
3. If the phone is not isolated, an associate can send a _____ command to destroy all files.
4. The officer immediately placed the seized phone inside a _____ to block all network connections.
5. This specialized enclosure ensures that no _____ can enter or leave the device during transport.
6. A _____ is quick and safe because it extracts visible data by talking to the device's operating system.
7. To extract hidden logs and deleted chat history, investigators must perform a deep _____.
8. A physical extraction bypasses the OS to create a perfect sector-by-sector _____ of the storage.
9. This advanced process reads raw data directly from the underlying chips of the _____.
10. Cracking modern phones is difficult because _____ scrambles user files automatically.
11. Without the correct passcode, the extracted _____ remains completely unreadable to the analyst.
12. Digital forensic laboratories utilize advanced _____ to bypass mobile security systems.
13. Forensic tools use automated _____ to guess thousands of lock screen PIN combinations per minute.
14. To ensure the evidence is admissible in court, every step must be documented in the _____.

Exercise 25. Translate the sentences into English

1. Хмарна криміналістика є спеціалізованою піддисципліною цифрової криміналістики, яка досліджує віртуальні середовища.
2. Вилучення всього фізичного диска з багатоорендного дата-центру порушує права на приватність третіх осіб.
3. Модель «Інфраструктура як сервіс» (IaaS) забезпечує криміналістам найвищий рівень контролю над віртуальними машинами.
4. Статичний аналіз дозволяє експертам досліджувати шкідливий файл та обчислювати його хеш без запуску коду.
5. Зловмисники використовують обфускацію та упаковане шкідливе ПЗ, щоб заплутати структуру коду та приховати вірус.
6. Аналітики запускають підозрілі файли в ізольованому середовищі (пісочниці), щоб безпечно дослідити їхню поведінку.
7. Шкідлива програма виконала ін'єкцію процесу, щоб приховати свій код усередині легітимного системного завдання.
8. Криміналісти вивчають приховані заголовки електронних листів, щоб відстежити IP-адреси агентів передачі пошти.
9. Перевірка криптографічного підпису DKIM математично доводить цілісність даних та захищає від підробки імені відправника.
10. Метадані EXIF, що містяться у фотографіях, можуть зберігати точні GPS-координати та час створення файлу.
11. На відміну від комп'ютерів, мобільні пристрої є динамічними екосистемами, де дані постійно оновлюються в реальному часі.
12. Слідчий негайно помістив вилучений телефон у пакет Фарадея, щоб запобігти команді віддаленого очищення даних.
13. Логічне вилучення копіює лише видимі файли, тоді як фізичне вилучення створює побітовий клон усієї флеш-пам'яті.
14. Для підбору цифрових паролів на заблокованих екранах лабораторії використовують автоматизований перебір (атаки brute-force).
15. Суворе ведення ланцюжка зберігання доказів є обов'язковим для того, щоб цифрові докази були визнані допустимими в суді.

Glossary

Forensic report — експертний висновок / криміналістичний звіт.

Executive summary — стисле резюме для керівництва (*нетехнічний огляд основних знахідок для менеджерів або суддів*).

Expert testimony (Expert witness testimony) — свідчення експерта в суді.

Admissibility of evidence — допустимість доказів (*відповідність усім юридичним вимогам для представлення в суді*).

Chain of custody verification — перевірка ланцюжка зберігання доказів.

Reproducibility (Repeatability) — відтворюваність / повторюваність результатів (*можливість іншого експерта отримати ті самі результати за тією ж методикою*).

Cross-examination — перехресний допит (*допит експерта адвокатами протилежної сторони*).

Technical jargon — технічний жаргон / професійний сленг.

Layperson (Lay audience) — неспеціаліст / мирянин (*людина без технічної чи криміналістичної освіти, наприклад, присяжний*).

Corroborating evidence — підтверджувальні (підкріплювальні) докази.

Cryptographic hash validation — перевірка криптографічного хешу (*довідення відсутності змін у файлах*).

Timeline of events — хронологія (таймлайн) подій.

Standard Operating Procedures (SOPs) — стандартні операційні процедури (*суворі інструкції та правила проведення дослідження*).

Expert witness — експерт-свідок (*криміналіст, якого офіційно викликають до суду для надання професійної оцінки*).

Visual aids — наочні засоби / візуальні матеріали (*схеми, графіки, таблиці*).

Exercise 26. Answer the questions based on the text

The Art of Documentation and Presentation in Digital Forensics

The ultimate phase of any digital investigation is not digging through raw hex code or recovering deleted databases; it is documentation. A digital forensic analyst can perform a technically flawless extraction of a suspect's cloud files or mobile logs, but if those findings are not articulated clearly, the evidence may fail to impact the case. The dual objective of **forensic reporting** is to transform complex binary structures into an understandable narrative while strictly demonstrating the **admissibility of evidence** under legal frameworks.

A professional **forensic report** must satisfy two completely different audiences simultaneously. It begins with an **executive summary**, which is specifically tailored for a **layperson audience**, such as corporate executives, legal prosecutors, or juries. This section strictly avoids **technical jargon**, opting instead to deliver a clear, concise overview of *who* did *what*, *when*, and *how* it impacts the litigation. Following this overview, the document transitions into an exhaustive technical analysis. This technical segment includes standard metadata profiles, **cryptographic hash validation** logs, and a structured **timeline of events** that traces the attacker's movements step-by-step.

Crucially, every high-quality forensic report must guarantee **reproducibility**. Legal defense teams routinely hire independent analysts to scrutinize the state's evidence. Therefore, the report must document the exact software versions, hardware configurations, and **Standard Operating Procedures (SOPs)** utilized during the investigation. If an independent examiner cannot follow the report's methodology to achieve the exact same cryptographic results, the integrity of the data is compromised, and the court may declare the evidence inadmissible.

The final challenge for a digital investigator is delivering **expert testimony** in a courtroom setting. As an **expert witness**, the analyst is placed under oath and subjected to intense **cross-examination** by defense attorneys. The defense will

systematically look for gaps in the **chain of custody verification** or attempt to confuse the jury with technical complexities. To survive cross-examination, an expert must remain objective, use clear **visual aids** to explain digital networks, and bridge the gap between complex computer architecture and basic legal concepts, ensuring that justice is guided by scientific facts.

Questions:

1. Why is documentation considered the ultimate and most critical phase of a digital forensic investigation?
2. What is the dual objective of **forensic reporting** under legal frameworks?
3. What is the main purpose of an **executive summary** at the beginning of a report?
4. Who belongs to a **layperson audience** in a courtroom setting, and why must an expert avoid using **technical jargon** with them?
5. What specific technical elements must be included in the second, more detailed section of the forensic report?
6. Why is a structured **timeline of events** essential when describing an attacker's actions?
7. What role does **cryptographic hash validation** play in proving the integrity of digital evidence?
8. What does the concept of **reproducibility** mean when an independent analyst reviews a case?
9. What technical information regarding tools must be documented to guarantee repeatability?
10. What are the legal consequences if an independent examiner cannot replicate the report's exact cryptographic results?
11. What is the role and legal status of a digital investigator acting as an **expert witness** in court?
12. What happens during a **cross-examination**, and who conducts this procedure?
13. What specific weaknesses or flaws will defense attorneys systematically look for in the forensic report?
14. Why are **visual aids** highly recommended when presenting digital evidence to a jury?
15. How should an expert witness bridge the gap between complex computer architecture and basic legal concepts during a trial?

*Exercise 27. True or False:

1. The ultimate phase of a digital forensic investigation is digging through raw hex code. (**True / False**)
2. A forensic report must satisfy both technical experts and a lay audience simultaneously. (**True / False**)
3. The executive summary should be densely packed with advanced programming language and technical jargon. (**True / False**)

4. A layperson audience includes corporate executives, legal prosecutors, and juries. (**True / False**)
5. Cryptographic hash validation logs are included in the report to prove that files were not tampered with. (**True / False**)
6. A structured timeline of events traces the attacker's movements step-by-step. (**True / False**)
7. Reproducibility means that independent analysts are legally blocked from reviewing the state's evidence. (**True / False**)
8. To guarantee repeatability, a report must document the exact software versions and hardware configurations used. (**True / False**)
9. If a second examiner cannot achieve the exact same cryptographic results, the court may declare the evidence inadmissible. (**True / False**)
10. Standard Operating Procedures (SOPs) are optional guidelines that analysts can ignore during data collection. (**True / False**)
11. An expert witness is placed under oath when delivering testimony in a courtroom setting. (**True / False**)
12. Cross-examination is conducted by the prosecutor to support the forensic analyst's findings. (**True / False**)
13. Defense attorneys will systematically look for gaps in the chain of custody verification. (**True / False**)
14. Visual aids should be avoided in court because they confuse the jury. (**True / False**)
15. The main goal of an expert witness is to bridge the gap between complex computer architecture and basic legal concepts. (**True / False**)

***Exercise 28. Fill in the Gaps. Fill in the blanks with the appropriate terms from the reference (each expression is used once):**

forensic report, executive summary, expert testimony, admissibility of evidence, chain of custody verification, reproducibility, cross-examination, technical jargon, layperson, corroborating evidence, cryptographic hash validation, timeline of events, Standard Operating Procedures, expert witness, visual aids

1. The analyst prepared a detailed _____ to present all digital findings to the court.
2. Juries are considered a _____ audience because they lack formal training in cyber forensics.
3. The defense attorney began an aggressive _____ to challenge the investigator's credentials.
4. To prove the files were identical to the original drive, the expert performed a _____.
5. The judge ruled on the _____, allowing the hard drive clone to be used as a primary exhibit.

6. A clear _____ showed exactly when the suspect accessed the restricted cloud database.
7. The investigator avoided using _____ so that the judge could easily follow the narrative.
8. Every laboratory must follow strict _____ to ensure all examinations are legally compliant.
9. The prosecutor introduced a server log as _____ to support the victim's testimony.
10. The corporate managers only read the _____ to quickly understand the financial impact of the hack.
11. An independent lab was hired to test the _____ of the primary analyst's findings.
12. The specialist was called to the stand to deliver his _____ regarding the mobile malware.
13. To make complex network routing paths easy to understand, the expert used _____ like diagrams.
14. Gaps in the _____ can lead to the permanent dismissal of critical digital evidence.
15. As an _____, the specialist must remain completely objective and stick to scientific facts.

***Exercise 29. Match the words with their meanings**

1. Forensic report	A) A strict, unalterable document that tracks who collected, accessed, and handled digital evidence.
2. Executive summary	B) The status of evidence that meets all legal requirements and is allowed to be presented in a trial.
3. Expert testimony	C) A detailed document that translates complex digital findings into a legally sound narrative.
4. Admissibility of evidence	D) A brief, non-technical overview of the main findings, designed for high-level managers or judges.
5. Chain of custody verification	E) Strict, step-by-step instructions that ensure forensic tasks are performed consistently.
6. Reproducibility	F) Verbal statements delivered under oath in a courtroom by a qualified specialist.
7. Cross-examination	G) Technical language or professional slang that is difficult for non-specialists to understand.
8. Technical jargon	H) A person who does not possess specialized or professional knowledge in a specific field.
9. Layperson	I) Secondary evidence that supports, confirms, or strengthens an already existing digital finding.
10. Corroborating evidence	J) The ability of an independent examiner to achieve identical results using the same methodology
11. Cryptographic hash	K) Charts, diagrams, or tables used to make complex

validation	data scannable and clear for a jury.
12. Timeline of events	L) A chronological log that maps out the precise sequence of actions during a cyber incident.
13. Standard Operating Procedures	M) A process where an expert is systematically questioned by the opposing legal team to find flaws.
14. Expert witness	N) A professional called to court to interpret evidence based on their specialized scientific skills.
15. Visual aids	O) A mathematical process that verifies a file has remained completely unaltered since collection.

***Exercise 30. Translate into English**

1. Кінцевим етапом будь-якого цифрового розслідування є ретельне складання експертного висновку.
2. Професійний криміналістичний звіт повинен задовольняти дві абсолютно різні аудиторії одночасно.
3. Стисле резюме для керівництва спеціально розроблене для аудиторії неспеціалістів.
4. Ми повинні уникати складного технічного жаргону під час представлення доказів присяжним.
5. Технічний розділ звіту містить перевірку криптографічного хешу та хронологію подій.
6. Кожен високоякісний висновок експерта повинен гарантувати повну відтворюваність результатів.
7. Якщо інший експерт не зможе повторити методику, суд визнає докази недопустимими.
8. Слідчий задокументував версії програмного забезпечення та стандартні операційні процедури.
9. Головне завдання експерта-свідка — дати об'єктивні свідчення в залі суду.
10. Під час перехресного допиту адвокати захисту шукатимуть прогалини у ланцюжку зберігання доказів.
11. Адвокати намагатимуться заплутати суддів за допомогою складних технічних концепцій.
12. Використання наочних засобів допомагає подолати розрив між архітектурою комп'ютера та правом.
13. Підтверджувальні докази посилили позицію звинувачення під час судового процесу.
14. Перевірка ланцюжка зберігання доказів доводить, що файли не були змінені під час аналізу.
15. Правосуддя має керуватися науковими фактами, а не припущеннями чи емоціями.

***Exercise 31. Put the words in the correct order**

1. documentation / is / phase / ultimate / code / the / investigation / of / an.
2. satisfy / reports / forensic / different / simultaneously / must / audiences / two.
3. avoids / executive / summary / completely / technical / the / jargon.
4. layperson / a / jury / considered / is / audience / a / courtroom / in.
5. validation / proves / hash / cryptographic / data / integrity / mathematical.
6. movements / timeline / sequence / steps / the / attacker's / traces / of / the.
7. guarantee / forensic / reproducibility / high-quality / must / findings / all.
8. tools / exact / document / analysts / operating / standard / procedures / and.
9. declare / court / inadmissible / the / may / evidence / the / unreplicable.
10. testimony / delivered / witness / expert / under / is / always / oath.
11. intensive / cross-examination / analysts / face / from / defense / attorneys / the.
12. look / gaps / verification / custody / for / in / defense / teams / chain.
13. visual / data / networks / simplify / complex / aids / courtroom / in / the.
14. corroborating / evidence / digital / prosecutors / supports / case / the / of.
15. bridge / experts / legal / gap / concepts / technical / and / between / the.

***Exercise 32. Match the English terms with Ukrainian equivalents (1–15 / A–O)**

	English Forensic Term			Ukrainian Equivalent
1	Forensic report		A	Перехресний допит
2	Executive summary		B	Допустимість доказів
3	Expert testimony		C	Наочні засоби / візуальні матеріали
4	Admissibility of evidence		D	Технічний жаргон / професійний сленг
5	Chain of custody verification		E	Стандартні операційні процедури (СОП)
6	Reproducibility		F	Стисле резюме для керівництва (вступна частина)
7	Cross-examination		G	Криміналістичний звіт / експертний висновок
8	Technical jargon		H	Перевірка криптографічного хешу
9	Layperson		I	Хронологія (таймлайн) подій
10	Corroborating evidence		J	Перевірка ланцюжка зберігання

	English Forensic Term			Ukrainian Equivalent
				доказів
11	Cryptographic hash validation		К	Неспеціаліст / мирянин (нетехнічна аудиторія)
12	Timeline of events		L	Свідчення експерта в суді
13	Standard Operating Procedures		M	Відтворюваність / повторюваність результатів
14	Expert witness		N	Підтверджувальні (підкріплювальні) докази
15	Visual aids		O	Експерт-свідок (криміналіст у суді)

***Exercise 33. Correct the mistakes**

1. Forensic reports is only written for computer systems administrators and nobody else.
2. The executive summary must be full of advanced programming syntax to confuse laypersons.
3. Legal prosecutors are considered part of a highly trained technical coding audience.
4. Cryptographic hash validation are used to permanently delete all file metadata from a system.
5. A timeline of events lists files randomly without any chronological or time-based order.
6. Reproducibility means that a forensic process can only be executed once and never repeated.
7. To guarantee repeatability, an investigator should hide the software versions they used.
8. If an independent examiner replicates your results exactly, your evidence are declared fake.
9. Standard Operating Procedures is completely optional and ignored during cloud investigations.
10. An expert witness delivers their testimony privately in a cafe without taking an oath.
11. Cross-examination are conducted by your own legal team to praise your excellent technical report.
12. Defense attorneys systematically ignore gaps in the chain of custody verification process.

13. Visual aids are completely useless because text jargon is much easier for a jury to read.
14. The main goal of an expert witness is to hide technical data from the judge during a trial.
15. Admissibility of evidence means that anyone can bring any unverified file into a courtroom.

Exercise 34. Listening.

Part 1. Listen to the text and fill in the gaps in the sentences. USE NO MORE THAN THREE WORDS.

1. The ultimate test for a digital forensic expert is how they handle the _____.
2. According to legal frameworks, raw data is insufficient; it must be authentic, reliable, and _____.
3. Investigators use _____ like SHA-256 to prove that the digital evidence has not been altered.
4. If a single bit of data changes, the _____ will change completely.
5. In an Executive Summary, forensic investigators must avoid using _____.

Part 2: Matching (Report Types)

Which characteristics belong to a Technical Report and which to an Executive Summary? Write the corresponding letter next to it.

A — Technical Report

B — Executive Summary / Legal Report

1. Focuses on answering "who, when, and what" without deep jargon. [____]
2. Includes exact cryptographic hashes, registry paths, and specific software tools used. [____]
3. Designed primarily for judges, juries, or corporate executives. [____]
4. Created for peer review and other technical experts to verify the methodology. [____]

Listening Script

Speaker: In the realm of cybercrime investigation, performing a forensic analysis is only half the battle. The ultimate test of a digital forensic expert lies in the **presentation of findings**. Whether you are testifying in a court of law or briefing a corporate board, you must translate complex technological data into clear, legally binding evidence.

During the forensic analysis of digital technologies, investigators deal with vast amounts of raw data. They examine volatile memory, extract unallocated space to recover deleted files, and dissect system logs. However, under the **Federal Rules of**

Evidence (or equivalent international legal frameworks), raw technical data is not enough. To be admissible in court, the evidence must meet three strict criteria: it must be **authentic, reliable, and complete**.

To establish authenticity, investigators use cryptographic hashes, such as **SHA-256**. A hash function acts as a digital fingerprint for a file or a whole drive. If even a single bit of data is altered during analysis, the hash value changes completely. This proves to the court that the evidence has not been tampered with since it was seized.

The presentation phase usually involves creating two types of reports. The first is a highly detailed **Technical Report** meant for peer review and other experts. It includes specific tools used, registries analyzed, and exact time offsets. The second is the **Executive Summary** or **Legal Report**. This is where the investigator must avoid deep technical jargon. Instead of explaining *how* a specific hex editor works, the expert must clearly present the timeline of events: *who* accessed the system, *when* the data was exfiltrated, and *what* the impact was.

As a forensic expert on the witness stand, clarity and objectivity are your best tools. If a judge or jury cannot understand your findings, even the most groundbreaking digital discovery becomes useless.

Exercise 35. Video

Task 1: Vocabulary Matching (Terminology)

Watch the beginning of the video: https://www.youtube.com/watch?v=f_mx3z61P6E [00:00 - 01:40]. Match the two types of witnesses in court and their functions.

A — Fact Witness (Свідок факту)

B — Expert Witness (Свідок-експерт)

1. Can only testify about what they directly saw, heard, or experienced. [____]
2. Is allowed to offer professional opinions and draw conclusions based on specialized training and analysis. [____]
3. Might be an investigator who simply states: "I found this hard drive on the desk." [____]
4. Can explain to the jury what the presence of specific metadata implies about a user's intent. [____]

Task 2: Multiple Choice (Courtroom Challenges)

Watch to the part of the video: https://www.youtube.com/watch?v=f_mx3z61P6E about courtroom challenges [01:40 - 03:40] and choose the correct answer.

1. **What is the primary role of an expert's CV (Curriculum Vitae) during the *voir dire* process?**
 - A) To show how much money the expert earns.
 - B) To legally qualify and prove the expert's authority, credentials, and experience to the court.
 - C) To summarize the timeline of the cybercrime.

2. **When presenting digital evidence to a non-technical jury, a forensic expert should:**
 - A) Use as many complex programming terms and hex codes as possible to look smart.
 - B) Demystify technology by using clear, concise definitions for jargon (like file slack or unallocated space).
 - C) Avoid using any text and show only raw data code.
3. **According to the video, what is crucial when facing cross-examination by the defense lawyer?**
 - A) Changing your findings if the pressure is too high.
 - B) Maintaining professionalism, ethics, strict honesty, and relying on clear documentation.
 - C) Arguing emotionally with the lawyer.

FINAL TEST UNIT 8
PART I: MULTIPLE CHOICE

Choose the correct answer (A, B, C, or D) for each question.

1. Which type of data disappears immediately when a suspect smartphone or computer is powered off?

- A) Persistent data
- B) Volatile data
- C) Encrypted data at rest
- D) Metadata

2. What is the primary purpose of maintaining a strict "Chain of Custody" during a cybercrime investigation?

- A) To speed up the decryption of hard drives.
- B) To automatically generate a legally binding report.
- C) To prove that digital evidence has not been altered or tampered with since its seizure.
- D) To hide the investigator's methods from the defense.

3. In mobile device forensics, what is the main risk of failing to place a seized smartphone into a Faraday bag?

- A) The battery will drain twice as fast.
- B) The phone might receive a remote wipe command over the cellular network or Wi-Fi.
- C) The device will automatically encrypt its entire file system.
- D) The dynamic RAM (volatile data) will instantly overwrite itself.

4. During a Cloud Forensics investigation, what is a major legal and technical challenge that investigators face?

- A) Data is completely static and never changes.
- B) Multi-tenancy, meaning the suspect's data is physically co-located on the same servers as innocent users' data.
- C) Cloud servers do not generate any HTTP or server logs.
- D) Cloud architecture relies entirely on physical hard drives that cannot be imaged.

5. What type of cyberattack is an investigator analyzing if the server logs show thousands of malicious SQL commands injected directly into an online web form?

- A) Cross-Site Scripting (XSS)
- B) Ransomware Deployment
- C) SQL Injection (SQLi)
- D) Distributed Denial of Service (DDoS)

6. Which artifact is most useful to a forensic specialist trying to determine which external USB drives were plugged into a Windows machine?

- A) Windows Registry
- B) The Master Boot Record (MBR)
- C) Database transaction logs
- D) Router configuration tables

7. Why do modern hackers use "IP spoofing" during a network attack?

- A) To legally protect their intellectual property.
- B) To encrypt the payload of their communication.
- C) To disguise their true identity by faking the source IP address.
- D) To establish a direct connection with the database.

8. What does a "Write-Blocker" do when connected to a suspect's hard drive during the acquisition phase?

- A) It decrypts secret-key cryptosystems on the fly.
- B) It physically prevents the forensic workstation from writing any data to the evidence drive.
- C) It automatically flags anomalies using an Intrusion Detection System (IDS).
- D) It compresses the target media to save storage space.

9. In Internet of Things (IoT) forensics, smart home devices (like smart refrigerators or voice assistants) are often investigated because:

- A) They contain high-capacity solid-state drives (SSDs).
- B) They act as a local timeline of physical events and user presence via sensor data and local caches.
- C) They are completely immune to anti-forensics techniques.
- D) They use the exact same operating system forensics as standard Linux servers.

10. What is the main objective of anti-forensics techniques used by sophisticated criminals?

- A) To improve the evidentiary value of digital assets.
- B) To automatically aggregate logs into a SIEM system.
- C) To manipulate, erase, or obscure digital evidence to frustrate forensic analysts.
- D) To build hidden Command and Control (C2) communication lines.

PART II: TERMINOLOGY MATCHING

Match the English digital forensics terms on the left (1–10) with their correct definitions or descriptions on the right (A–J).

No.	Term		Letter	Definition / Description
1	Bit-stream Image		A	Automated systems that aggregate and correlate logs from across an entire network to find threats.
2	Metadata		B	An attack that uses compromised machines to overwhelm network services, masking other malicious actions.
3	SIEM Systems		C	Hidden communication paths used by malware to receive orders from an external malicious server.

No.	Term		Letter	Definition / Description
4	DDoS Attack		D	Data about data (e.g., timestamps, file author, file size, or GPS coordinates embedded in a photo).
5	C2 Channels		E	A cryptographic function used to verify data integrity by creating a unique digital fingerprint (e.g., SHA-256).
6	Hash Value		F	A sector-by-sector, exact physical duplicate of a storage media, including unallocated space and slack space.
7	Slack Space		G	A specialized software tool used by analysts for packet sniffing and deep network traffic analysis.
8	Wireshark		H	The unused space left over on a hard drive sector when a file does not take up the entire allocated block.
9	Data at Rest		I	A logging architecture that guarantees entries cannot be modified or deleted once they are written.
10	Immutable Logging		J	Static digital assets stored permanently on physical hardware like hard drives or solid-state drives.

PART III: CASE STUDY & SHORT ANSWER

Read the scenario below and answer the questions briefly but precisely. Use appropriate professional terminology.

Scenario:

A large e-commerce company suspects that an insider (a rogue employee with administrative privileges) has stolen a sensitive database containing customer credit card details. The security team noticed unusual outbound data traffic late at night. When the suspect noticed the security team investigating, they abruptly shut down their corporate laptop by pulling out the power cord.

Questions:

1. Evidence Prioritization:

Because the laptop was abruptly forced to shut down, what critical category of evidence was likely lost or modified in this scenario? Explain why this complicates the investigation of the network connections.

Your

answer:

—

—

2. **Alternative Sources of Evidence:**

Since the local computer was shut down, name **two alternative infrastructure-level sources** where the forensic team can look to prove that "unauthorized data exfiltration" occurred.

Your

answer:

—

—

3. **Data Integrity Assurance:**

Once the forensic team extracts the hard drive from the corporate laptop to create a copy, what steps must they take to legally guarantee that the data analyzed in the lab exactly matches the state of the drive when it was seized?

Your

answer:

—

—

REFERENCES

1. Anthropic. (2026). *Claude Mythos and the future of AI-powered vulnerability discovery*. Anthropic. Available at: <https://www.anthropic.com/>
2. CISA. (2023). *#StopRansomware Guide*. Cybersecurity and Infrastructure Security Agency. Available at: [#StopRansomware Guide](#)
3. Cybersecurity and Infrastructure Security Agency (CISA). *Cybersecurity resources and best practices*. Available at: [CISA Cybersecurity Resources](#)
4. ENISA. (2025). *ENISA Threat Landscape 2025*. European Union Agency for Cybersecurity. Available at: [ENISA Threat Landscape 2025](#)
5. Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Publications Office of the European Union. Available at: [Internet Organised Crime Threat Assessment \(IOCTA\) 2024](#)
6. Europol. (2025). *The changing DNA of serious and organised crime: EU Serious and Organised Crime Threat Assessment 2025*. Publications Office of the European Union. Available at: [EU-SOCTA 2025](#)
7. Kovacs, E. (2026, May 25). *Anthropic: Mythos Detected 23,000 Potential Vulnerabilities Across 1,000 OSS Projects*. SecurityWeek. Available at: [SecurityWeek article](#)
8. National Cyber Security Centre. (2022). *Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion*. UK Government. Available at: [NCSC – Russia behind cyber attack with Europe-wide impact](#)
9. National Institute of Standards and Technology. (2024). Pascoe, C., Quinn, S., & Scarfone, K. *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper 29. Available at: [NIST Cybersecurity Framework \(CSF\) 2.0](#)
10. National Institute of Standards and Technology. (2024). Rigopoulos, K., Quinn, S., Pascoe, C., Marron, J., Mahn, A., & Topper, D. *NIST Cybersecurity Framework 2.0: Resource & Overview Guide*. NIST Special Publication 1299. Available at: [NIST CSF 2.0 Resource & Overview Guide](#)
11. OWASP Foundation. (2025). *OWASP Top 10: The Ten Most Critical Web Application Security Risks*. Available at: [OWASP Top 10](#)
12. OWASP Foundation. *OWASP Web Security Testing Guide*. Available at: [OWASP Web Security Testing Guide](#)
13. MITRE. *ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge*. Available at: [MITRE ATT&CK](#)
14. MITRE. *Common Vulnerabilities and Exposures (CVE)*. Available at: [MITRE CVE](#)
15. FIRST. *Common Vulnerability Scoring System (CVSS)*. Forum of Incident Response and Security Teams. Available at: [FIRST CVSS](#)
16. IBM. *What is cybersecurity?* IBM. Available at: [IBM Cybersecurity](#)
17. Microsoft. *Microsoft Security*. Available at: [Microsoft Security](#)
18. Google. *Google Safety Center: Security*. Available at: [Google Security](#)

19. Cloudflare. *Learning Center: Cybersecurity*. Cloudflare. Available at: [Cloudflare Learning Center](#)
20. Cisco. *Cybersecurity*. Cisco. Available at: [Cisco Cybersecurity](#)
21. International Telecommunication Union. *Global Cybersecurity Index*. ITU. Available at: [ITU Global Cybersecurity Index](#)
22. European Union Agency for Cybersecurity (ENISA). *Cybersecurity*. Available at: [ENISA](#)
23. INTERPOL. *Cybercrime*. International Criminal Police Organization. Available at: [INTERPOL Cybercrime](#)
24. Council of Europe. *Cybercrime Programme Office (C-PROC)*. Available at: [Council of Europe – Cybercrime Programme Office](#)
25. United Nations Office on Drugs and Crime. *Cybercrime*. UNODC. Available at: [UNODC Cybercrime](#)
26. National Police of Ukraine. *Cyber Police Department*. Available at: [Cyber Police of Ukraine](#)
27. Computer History Museum. *Computer History Museum*. Available at: [Computer History Museum](#)
28. Encyclopaedia Britannica. *Artificial Intelligence*. Available at: [Encyclopaedia Britannica – Artificial Intelligence](#)
29. Encyclopaedia Britannica. *Computer*. Available at: [Encyclopaedia Britannica – Computer](#)
30. National Institute of Standards and Technology. *Post-Quantum Cryptography*. NIST. Available at: [NIST Post-Quantum Cryptography](#)
31. National Institute of Standards and Technology. *Computer Security Resource Center (CSRC)*. Available at: [NIST Computer Security Resource Center](#)
32. Internet Engineering Task Force. *RFCs – Internet Engineering Task Force*. Available at: [IETF RFCs](#)
33. National Cyber Security Centre. *Guidance and resources*. UK Government. Available at: [NCSC Guidance](#)
34. Verizon. (2025). *2025 Data Breach Investigations Report*. Verizon. Available at: [Verizon Data Breach Investigations Report](#)
35. Mandiant. *M-Trends: Cybersecurity insights and threat intelligence*. Google Cloud. Available at: [Mandiant M-Trends](#)
36. Microsoft. *Microsoft Digital Defense Report*. Available at: [Microsoft Digital Defense Report](#)
37. Google Cloud. *Threat Horizons*. Available at: [Google Cloud Threat Horizons](#)
38. SANS Institute. *Cybersecurity Training and Resources*. Available at: [SANS Institute](#)
39. CERT-UA. *Computer Emergency Response Team of Ukraine*. State Service of Special Communications and Information Protection of Ukraine. Available at: [CERT-UA](#)

40. State Service of Special Communications and Information Protection of Ukraine. *Cybersecurity*. Available at: [SSSCIP of Ukraine](#)
41. <https://univd.edu.ua/en/video/1422>
42. <https://www.youtube.com/watch?v=VINyUsm0W4w>
43. <https://www.youtube.com/watch?v=nS8KweAV1g0>
44. https://glasp.co/youtube/NIRXtMg-0z8?utm_source
45. <https://www.youtube.com/watch?v=sdpxddDzXfE>
46. <https://www.youtube.com/watch?v=Kf9KjCKmDcU>
47. <https://www.youtube.com/watch?v=w2xItujdLag>
48. https://www.youtube.com/watch?v=f_mx3z61P6E
49. https://www.youtube.com/watch?v=f_mx3z61P6E
50. <https://recfaces.com/articles/digital-forensics>