Алєкссєв А. В.

ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

Практикум

ВИЩИЙ НАВЧАЛЬНИЙ ПРИВАТНИЙ ЗАКЛАД
«ДНІПРОВСЬКИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ»

Алєкссєв А. В.

ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

Практикум

Частина 1

Дніпро – 2024

УДК 004.9

Ухвалено до друку Науково-методичною радою Вищого навчального приватного закладу «Дніпровський гуманітарний університет» (протокол № 10 від 20.06.2024 р.)

Рецензенти:

КОЗІН Ігор Вікторович, доктор фізико-математичних наук, професор, професор кафедри економічної кібернетики Запорізького національного університету

МИЛЬЦЕВ Олександр Михайлович, кандидатом фізико-математичних наук, доцентом кафедри програмної інженерії Запорізького національного університету

Алєксєєв А.В. Інформаційні системи та технології: Практикум. Ч. 1. Дніпро: ВНПЗ «ДГУ», 2024. 140 с.

Практикум є практичним посібником, призначеним для студентів гуманітарних спеціальностей, які вивчають дисципліну «Інформаційні системи та технології». Розроблений з урахуванням потреб сучасного ринку праці, де цифрова грамотність стає ключовим фактором успіху в багатьох сферах діяльності. Практикум може використовуватись як для самостійного вивчення матеріалу, так і в межах аудиторних занять. Він стане цінним доповненням до лекцій та сприятиме формуванню практичних компетенцій, необхідних для успішної подальшої кар'єри у гуманітарних сферах.

Рекомендовано для підготовки здобувачів вищої освіти гуманітарних спеціальностей та для викладачів закладів вищої освіти.

ЗМІСТ

ПЕРЕДМОВА …….. 5

ТЕМА 1. ОСНОВНІ ПОНЯТТЯ, ПРИНЦИПИ РОБОТИ ТА ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ ……..…. 6
Теоретичні рекомендації до теми 1 …….. 6
1.1. Що таке комп'ютерна мережа? Класифікація мереж ……..… 6
1.2. Типи мереж: локальні, місткові, глобальні ……... 7
1.3. Основні компоненти комп'ютерної мережі …….. 9
1.4. Протоколи мереж: TCP/IP, HTTP, FTP …… 10
1.5. Використання мереж для обміну даними та спільної роботи …… 11
Практичні завдання …….. 13
Тести ……..…… 33
Питання для підсумкового контролю ……...…….. 40

ТЕМА 2. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ……...….. 42
Теоретичні рекомендації до теми 2 ……..….. 42
2.1. Що таке інформаційна безпека? Поняття та терміни …… 42
2.2. Загрози інформаційній безпеці ……...…….. 44
2.3. Методи захисту інформації ……..…… 45
2.4. Правила безпечної роботи з інформацією ……... 46
2.5. Захист особистої інформації в мережі …….. 48
Практичні завдання …….. 50
Тести ……...……... 69
Питання для підсумкового контролю …… 76

ТЕМА 3. ОБРОБЛЕННЯ ЗОБРАЖЕНЬ ЗАСОБАМИ КОМП'ЮТЕРНОЇ ГРАФІКИ ……..……... 78
Теоретичні рекомендації до теми 3 ……..….. 78
3.1. Основи комп'ютерної графіки …….. 78
3.2. Використання програми GIMP ……...…….. 80
3.3. Редагування зображень …… 82
3.4. Створення простих зображень ……..…… 84
3.5. Редагування та покращання фотографії ……... 86
Практичні завдання …….. 87
Тести ……...…… 100
Питання для підсумкового контролю ……...…… 107

ТЕМА 4. КОМП'ЮТЕРНІ ПУБЛІКАЦІЇ ……...…. 109
Теоретичні рекомендації до теми 4 ……...……..….. 109
4.1. Основи верстки …… 109
4.2. Використання редактора LaTeX для створення наукових публікацій …… 111
4.3. Підготовка рукопису до набору в журнал: покрокова інструкція …….. 114
Практичні завдання ……..... 116
Тести ……..……...… 129
Питання для підсумкового контролю ……...… 136

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ……..…… 138

ПЕРЕДМОВА

Сучасний світ неможливо уявити без інформаційних технологій. Вони проникають у всі сфери нашого життя – від бізнесу та медицини до освіти та розваг. Інформаційні системи та технології (ІСТ) є основою економіки, науки та культури, і їх роль продовжує зростати з кожним днем.

Практикум розроблено з метою надати вам необхідні знання та практичні навички для успішної роботи в цій динамічній та перспективній галузі. Відбулося прагнення створити посібник, який не лише роз'яснює теоретичні концепції, але й дає можливість одразу застосувати їх на практиці.

Посібник охоплює широкий спектр тем, що стосуються сучасних ІСТ, починаючи від основних принципів роботи інформаційних систем та закінчуючи актуальними технологіями, такими як хмарні обчислення, аналіз даних та веб-розробка. Він написаний простою та зрозумілою мовою, з прикладами та практичними завданнями, які допоможуть вам засвоїти матеріал.

Актуальність навчального посібника-практикуму зумовлена необхідністю врахування специфіки вивчення матеріалу з дисципліни «Інформаційні системи і технології» для здобувачів вищої освіти різноманітних спеціальностей.

Навчальний посібник-практикум присвячено вивченню основних понять та термінів із дисципліни, практичні вправи та завдання спрямовані на вироблення вмінь та навичок роботи з інформаційними системами, технологіями та програмними комплексами.

Кожна тема містить практичні вправи та завдання, матеріали для самоперевірки, які можуть слугувати опорою при підготовці до заліку. Додатковий матеріал викладено українською та англійською мовами, з опорою на методичну літературу, що робить посібник цінним як у теоретичному, так і в практичному плані.

Навчальний посібник рекомендовано для здобувачів вищої освіти гуманітарних спеціальностей. Практикум стане корисним джерелом знань, оскільки дозволяє глибше зрозуміти практичне застосування інформаційних систем і технологій у професійній діяльності.

ТЕМА 1. ОСНОВНІ ПОНЯТТЯ, ПРИНЦИПИ РОБОТИ ТА ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Мета: усвідомлювати основні критерії та поняття щодо інформаційних наук, володіти термінологією щодо інформації та її оброблення, напрацювати навички роботи з комп'ютерною технікою, вміти використовувати довідкову інформацію, вміти орієнтуватися в операційних системах.

ТЕОРЕТИЧНІ РЕКОМЕНДАЦІЇ ДО ТЕМИ 1

1.1. Що таке комп'ютерна мережа? Класифікація мереж

Зверніть увагу на основні положення теми:

1. **Комп'ютерна мережа** – це група комп'ютерів (або інших пристроїв, таких як принтери, смартфони, сервери тощо), які з'єднані між собою для обміну даними, ресурсами та послугами. Це дозволяє користувачам спільно працювати, ділитися інформацією та використовувати різні пристрої, що знаходяться в мережі. Сприймаємо комп'ютерну мережу як дорогу, по якій дані пересуваються між комп'ютерами.

2. **Основні компоненти комп'ютерної мережі:**

Комп'ютери та пристрої: учасники мережі, які обмінюються даними.

З'єднувальні кабелі/інтерфейси: фізичні (кабелі) або бездротові (Wi-Fi, Bluetooth) канали зв'язку.

Мережеве обладнання: пристрої, що забезпечують передавання даних, такі як: маршрутизатори, комутатори, модеми тощо.

Програмне забезпечення: програми, які керують мережею та дозволяють користувачам взаємодіяти з нею (операційні системи, програмне забезпечення для обміну файлами, веббраузери).

3. **Класифікація мереж:**

Існує багато способів класифікувати комп'ютерні мережі. Ось деякі з основних:

За масштабом (розміром):

Персональна мережа (PAN): найменша мережа, зазвичай використовується для підключення пристроїв, що знаходяться поруч, наприклад, Bluetooth-навушники до смартфона.

Домашня мережа (LAN - Local Area Network): мережа, яка з'єднує комп'ютери та інші пристрої в одному приміщенні (будинку, офісі).

Міжвидова мережа (MAN – Metropolitan Area Network): більша за LAN, але менша за WAN, що охоплює місто або великий район.

Глобальна мережа (WAN – Wide Area Network): найбільша мережа, що з'єднує мережі в різних географічних регіонах, наприклад, Інтернет.

За архітектурою:

Ключова мережа (Client-Server): один або декілька серверів надають ресурси та послуги клієнтам (комп'ютерам); клієнти запитують ресурси у сервера.

Мережа peer-to-peer (P2P): Усі комп'ютери в мережі мають рівні права та можуть обмінюватися файлами та ресурсами безпосередньо один з одним.

За топологією (фізичним розташуванням):

Зіркова (Star): всі пристрої з'єднані з центральним вузлом (комутатором або маршрутизатором).

Шинна (Bus): всі пристрої з'єднані одним кабелем.

Кільцева (Ring): пристрої з'єднані в кільце.

Деревоподібна (Tree): складний варіант зіркової топології, що розширюється в багато рівнів.

Змішана (Mesh): комбінація різних топологій.

За використанням частотного діапазону:

Провідні мережі: використовують фізичні кабелі для передавання даних (Ethernet, DSL).

Бездротові мережі: використовують радіохвилі для передавання даних (Wi-Fi, Bluetooth).

За призначенням:

Інтернет: глобальна мережа, що з'єднує мільярди пристроїв у всьому світі.

Корпоративна мережа: мережа, що використовується в компанії для внутрішніх комунікацій та обміну даними.

Публічна Wi-Fi мережа: мережа, доступна для широкої публіки (наприклад, у кафе, готелях).

1.2. Типи мереж: локальні, місткові, глобальні

Зверніть увагу на основні положення теми:

Розглянемо типи мереж: локальні, місткові та глобальні. Кожна з них має свої особливості, призначення та характеристики.

1. ***Локальні мережі*** (LAN – Local Area Network)

Локальна мережа – це мережа, яка об'єднує комп'ютери та інші пристрої в обмеженій фізичній сфері, наприклад, в офісі, школі, будинку або навіть у кімнаті.

Характеристики:

Невеликий радіус дії: зазвичай охоплює площу до кількох кілометрів.

Висока швидкість передавання даних: завдяки короткому прокладанню каналів.

Низька вартість: зазвичай, дешевший у розгортанні та підтримці, ніж інші типи мереж.
Приклади: мережа в офісі, домашня мережа з Wi-Fi, мережа в навчальному закладі.
Технології: Ethernet, Wi-Fi (802.11), Bluetooth.
Призначення: обмін файлами, друкування, спільне використання ресурсів, внутрішні комунікації.

2. ***Місткові мережі*** (MAN – Metropolitan Area Network)

Місткова мережа – це мережа, яка охоплює більшу територію, ніж локальна мережа, але меншу, ніж глобальна (зазвичай, це місто або великий мікрорайон).

Характеристики:

Середній радіус дії: переважно до 50 кілометрів.
Середня швидкість передавання даних: вища, ніж у локальних мережах, але нижча, ніж у глобальних.
Більш висока вартість: дорожча у розгортанні та підтримці, ніж локальні мережі.
Приклади: мережа, яка об’єднує різні офіси компанії в одному місті, мережа кабельного телебачення, мережа університетів у місті.
Технології: файбер-оптика, віртуальні приватні мережі (VPN), DSL.
Призначення: об’єднання різних локальних мереж, надання доступу до інтернету, розподіл телевізійного сигналу, внутрішні комунікації для великих організацій.

3. ***Глобальні мережі*** (WAN – Wide Area Network)

Глобальна мережа – це мережа, яка охоплює велику географічну територію, наприклад, країну, континент або весь світ.

Характеристики:

Великий радіус дії: охоплює великі відстані.
Нижня швидкість передання даних: зазвичай, найнижча швидкість серед трьох типів мереж (хоча швидкості постійно зростають).
Висока вартість: найдорожча у розгортанні та підтримці.
Приклади: інтернет, корпоративна мережа, яка об’єднує офіси компанії в різних країнах.
Технології: супутниковий зв’язок, мережі на основі пропрієтарних протоколів (наприклад, Frame Relay, ATM), MPLS.
Призначення: міжнародний обмін даними, глобальна комунікація, доступ до інформації, електронна комерція.

1.3. Основні компоненти комп’ютерної мережі

Зосередимо увагу на основних компонентах комп’ютерної мережі. До них належать: сервер, клієнт, маршрутизатор і комутатор.

1. **Сервер** – це комп’ютер або програма, яка надає ресурси, дані або послуги іншим комп’ютерам (клієнтам) у мережі. Його завдання слугувати іншим, наприклад:

Вебсервер: надає вебсторінки (наприклад, сайт Google).

Сервер електронної пошти: відправляє та отримує електронні листи.

Файловий сервер: зберігає та надає доступ до файлів.

Сервер баз даних: зберігає та управляє інформацією в базі даних.

Характеристики: сервери зазвичай мають потужніші процесори, більше пам’яті та більший обсяг дискового простору, ніж клієнтські комп’ютери.

2. **Клієнт** – це комп’ютер або пристрій, який залучається до використання ресурсів, даних або послуг, наданих сервером. Він запитує послуги, наприклад:

Ваш особистий комп’ютер: коли ви відкриваєте вебсайт, ваш комп’ютер діє як клієнт, який залучає вебсервер.

Мобільний телефон: коли ви використовуєте додаток, який з’єднується з сервером для отримання даних.

Принтер: коли комп’ютер відправляє документ на принтер, принтер діє як клієнт.

Характеристики: клієнти зазвичай мають меншу потужність, ніж сервери.

3. **Маршрутизатор** (Router) – це пристрій, який пересилає дані між мережами. Він аналізує адресу призначення даних, визначає найкращий шлях для їх доставки та з’єднує мережі.

Функції:

Маршрутизація: визначає оптимальний шлях для даних.

NAT (Network Address Translation): забезпечує перетворення IP-адрес, дозволяючи декільком пристроям у локальній мережі використовувати одну зовнішню IP-адресу.

Брандмауер: захищає мережу від несанкціонованого доступу, наприклад: Ваш домашній маршрутизатор з’єднує вашу локальну мережу з Інтернетом.

4. **Комутатор** (Switch) – це пристрій, який з’єднує пристрої в локальній мережі (LAN). Він пересилає дані тільки до того пристрою, якому вони призначені, на відміну від хаба, який просто повторює сигнал та з’єднує пристрої всередині мережі.

Функції:

Масштабування: дозволяє додавати більше пристроїв до мережі.

Підвищення швидкості: пересилає дані безпосередньо до потрібного пристрою, зменшуючи завантаження мережі.

Безпека: може забезпечувати сегментацію мережі для підвищення безпеки.

Відмінність від хаба: хаб пересилає дані на всі пристрої в мережі, тоді як комутатор направляє дані тільки на потрібний пристрій, використовуючи MAC-адреси.

1.4. Протоколи мереж: TCP/IP, HTTP, FTP

Розглянемо ці три важливі протоколи мереж: TCP/IP, HTTP та FTP. Вони є основою сучасного Інтернету та взаємодіють між собою, щоб забезпечити передавання даних.

1. **TCP/IP** (Transmission Control Protocol/Internet Protocol) – це не один протокол, а сімейство протоколів. Це основна мова Інтернету. Воно визначає, як дані повинні бути упаковані, адресовані, маршрутизовані та доставлені в мережі.

Компоненти:

IP (Internet Protocol): Відповідає за адресування та маршрутизацію пакетів даних між різними мережами. Кожний пристрій у мережі має унікальну IP-адресу.

TCP (Transmission Control Protocol): забезпечує надійну, з'єднану передавання даних. Він гарантує, що дані будуть доставлені в правильному порядку, без помилок і без втрат. TCP використовує механізм підтвердження (acknowledgment) для перевірки отримання пакетів.

UDP (User Datagram Protocol): Протокол без з'єднання. Він швидший, ніж TCP, але не гарантує надійність доставки. Використовується для додатків, де швидкість важливіша за надійність, наприклад, потокове відео або онлайн-ігри.

Дані розбиваються на пакети, кожен із яких містить IP-адресу відправника та отримувача. IP-адреси дозволяють пакетам знаходити шлях через мережу. TCP забезпечує, щоб пакети були доставлені в правильному порядку, а UDP не робить жодних гарантій. Без TCP/IP не було б Інтернету, як ми його знаємо.

2. **HTTP (Hypertext Transfer Protocol)** – це протокол, який використовується для передавання вебсторінок та інших ресурсів між вебсервером та веббраузером.

Як працює:

Client-Server Model: HTTP – це клієнт-серверна модель, наприклад: веббраузер (клієнт) надсилає запит на вебсервер.

Запит (Request): клієнт надсилає HTTP-запит, який містить інформацію про те, який ресурс потрібно отримати (наприклад, вебсторінку).

Відповідь (Response): вебсервер надсилає HTTP-відповідь, яка містить запитуваний ресурс (наприклад, HTML-код вебсторінки).

Статусні коди: HTTP-відповідь містить статусний код, який вказує на результат запиту (наприклад, 200 OK – все добре, 404 Not Found – ресурс не знайдено), наприклад: перегляд вебсайтів, завантаження зображень, відправка форм. HTTP є ключовим протоколом для взаємодії з вебсайтами.

3. **FTP (File Transfer Protocol)** – це протокол, який використовується для передавання файлів між комп'ютерами в мережі.

Як працює:

З'єднання: FTP створює два окремих з'єднання: одне для контрольних команд і інше для передавання даних.

Команди: FTP використовує команди для управління файлами такими, як: завантаження (upload), завантаження (download), перегляд каталогів тощо.

Безпека: Класичний FTP (без шифрування) не є безпечним, оскільки дані передаються у відкритому вигляді. Для безпечного передавання файлів використовують SFTP (Secure FTP) або FTPS (FTP Secure), наприклад: завантаження та завантаження файлів на вебсервери, передавання файлів між користувачами. FTP історично був важливим протоколом для передавання файлів, але зараз частіше використовуються більш сучасні протоколи, такі як SFTP та HTTPS.

1.5. Використання мереж для обміну даними та спільної роботи

Використання мереж для обміну даними та спільної роботи є критично важливим аспектом сучасних технологій та бізнесу. Вони дозволяють командам працювати разом незалежно від географічного розташування, підвищують ефективність та сприяють інноваціям. Розглянемо різні аспекти цього питання:

1. **Типи мереж**:

Локальні мережі (LAN): з'єднують пристрої в обмеженому просторі, наприклад, офісі або школі, зазвичай використовують Ethernet або Wi-Fi.

Паралельні мережі (WAN): з'єднують локальні мережі в більші географічні зони, такі як країни або континенти. Інтернет є найбільшою WAN.

Віртуальні приватні мережі (VPN): створюють зашифрований тунель через публічну мережу (наприклад, Інтернет) для безпечного обміну даними.

Хмарні мережі: надають ресурси (обчислювальні потужності, сховище, програми) через Інтернет: Google Drive, Dropbox, Microsoft OneDrive.

Бездротові мережі (Wi-Fi, Bluetooth): Дозволяють пристроям з'єднуватися без фізичних кабелів.

2. **Технології обміну даними:**

Електронна пошта (Email): традиційний метод обміну текстовими повідомленнями та файлами.

Месенджери (Slack, Microsoft Teams, WhatsApp): для швидкого обміну повідомленнями, файлами та здійснення відеодзвінків.

Файлообмінні сервіси (Google Drive, Dropbox, OneDrive): для зберігання та обміну файлами.

Системи управління контентом (CMS) (WordPress, Drupal, Joomla): для створення та управління вебконтентом, що часто вимагає спільної роботи.

Системи керування проєктами (Asana, Trello, Jira): для організації та відстеження прогресу проєктів.

Обмін даними через API (Application Programming Interface): дозволяє різним програмам та вебсервісам взаємодіяти та обмінюватися даними.

3. **Інструменти для спільної роботи:**

Інструменти для відеоконференцій (Zoom, Google Meet, Microsoft Teams): для проведення відеозв'язків та онлайн-зустрічей.

Інструменти для спільного редагування документів (Google Docs, Microsoft Office Online): дозволяють кільком користувачам одночасно працювати над одним документом.

Інструменти для спільної роботи над кодом (GitHub, GitLab): для командної розроблення програмного забезпечення.

Інструменти для спільної роботи з графікою (Adobe Creative Cloud): дозволяють кільком користувачам працювати над одним графічним файлом.

4. Переваги використання мереж для обміну даними та спільної роботи:

Підвищення продуктивності: пришвидшує процес обміну інформацією та виконання завдань.

Економія часу та ресурсів: замінює фізичні зустрічі та поштові листи.

Покращання комунікації: забезпечує миттєвий зв'язок між членами команди.

Підтримка віддаленої роботи: дозволяє працювати з будь-якої точки світу.

Збільшення можливостей для співпраці: сприяє обміну ідеями та знаннями.

5. Безпека мереж:

Шифрування даних: захищає дані від несанкціонованого доступу.

Брандмауери: захищають мережу від зовнішніх загроз.

Антивірусне програмне забезпечення: захищає пристрої від вірусів та шкідливого програмного забезпечення.

Управління доступом: обмежує доступ до даних та ресурсів лише для авторизованих користувачів.
Регулярні оновлення: забезпечують захист від нових загроз безпеки.

ПРАКТИЧНІ ЗАВДАННЯ

Завдання № 1

Створіть мережу Bluetooth та налаштуйте Bluetooth-з'єднання між двома пристроями (наприклад, смартфоном та навушниками) у такій послідовності:
1. Увімкніть Bluetooth на обох пристроях.
2. На смартфоні оберіть «Підключити пристрої» або подібну опцію.
3. У списку доступних пристроїв знайдіть та виберіть свій навушник.
4. Введіть пароль (якщо потрібно).
5. Переконайтеся, що з'єднання встановлено.

Завдання № 2

Налаштуйте домашню мережу Wi-Fi, змініть пароль Wi-Fi та перевірте наявність підключених пристроїв за схемою:
1. Відкрийте налаштування Wi-Fi на комп'ютері або смартфоні.
2. Оберіть свою мережу.
3. Змініть пароль (введіть новий та підтвердіть).
4. Перегляньте список підключених пристроїв (зазвичай у розділі «Мережа» або «Wi-Fi»).

Завдання № 3.

(LAN) Діагностика мережі (Ping): перевірка доступності іншого комп'ютера в локальній мережі. Кроки:
1. Відкрийте командний рядок (Command Prompt) на одному комп'ютері.
2. Введіть команду `ping <IP-адреса іншого комп'ютера>`.
3. Проаналізуйте результати (час відповіді, втрачені пакети).

Завдання № 4.

(MAN) Визначення IP-адреси: з'ясування IP-адреси комп'ютера в локальній мережі. Кроки:
1. Відкрийте командний рядок (Command Prompt).
2. Введіть команду `ipconfig` (Windows) або `ifconfig` (Linux/macOS).
3. Знайдіть рядок «IPv4-адреса» або «inet addr».

Завдання № 5.

(WAN) Доступ до Інтернету: перевірка можливості підключення до Інтернету. Кроки:

1. Відкрийте веббраузер.
2. Спробуйте відвідати будь-який сайт (наприклад, google.com).

Завдання № 6.

(Клієнт-Сервер) Визначення сервера: з'ясування, чи є комп'ютер у мережі сервером. Кроки:

1. Якщо комп'ютер надає файли або послуги іншим комп'ютерам, він може бути сервером.
2. Перевірте, чи є на комп'ютері запущеним серверний програмний продукт.

Завдання № 7.

(P2P) Обмін файлами через P2P програму: використання P2P програми (наприклад, BitTorrent) для завантаження або передавання файлу. Кроки:

1. Встановіть P2P програму.
2. Знайдіть файл, який потрібно завантажити або передати.
3. Виберіть файл та запустіть процес завантаження/передавання.

Завдання № 8.

(Зірка) Визначення топології мережі: з'ясувати, чи використовується зіркова топологія в мережі (за наявності центрального вузла) та чи є один центральний пристрій (наприклад, комутатор), до якого підключено всі інші пристрої.

Завдання № 9.

(Шинна) Візуалізація топології мережі: зобразити схематично топологію мережі (за наявності можливості), що показує взаємоз'єднання пристроїв у мережі.

Завдання № 10.

(Деревоподібна) Розпізнавання деревоподібної топології: визначити, чи використовується деревоподібна топологія в мережі (з кількома рівнями з'єднань). Додатково з'ясуйте: чи є пристрої, які з'єднані безпосередньо з іншими пристроями, у тому числі пристроями на вищих рівнях.

Завдання № 11.

(За використання частотного діапазону) Визначення типу мережі (провідна/бездротова): використовується провідна мережа (Ethernet) чи бездротова (Wi-Fi). Перевірте тип мережевого адаптера (в налаштуваннях комп'ютера).

Завдання № 12.

(Інтернет) Визначення IP-адреси сайту: з'ясуйте IP-адреси вебсайту (за вибором) та використайте онлайн-інструмент для перевірки IP-адреси сайту (наприклад, whatismyip.com).

Завдання № 13.

(Корпоративна мережа) Перевірка наявності мережевих ресурсів: визначте наявність спільного принтера або іншого ресурсу в корпоративній мережі. Перевірте налаштування принтера в операційній системі.

Завдання № 14.

(Публічна Wi-Fi) Аналіз безпеки публічної Wi-Fi мережі: оцінити рівень безпеки та використати програмні інструменти для перевірки безпеки.

Завдання № 15.

(Ping) Аналіз затримки мережі: вимірювання часу відповіді при використанні `ping`. Кроки:

1. Введіть команду `ping` до різних серверів.
2. Запишіть час відповіді для кожного сервера.

Завдання № 16.

(Traceroute) Визначення шляху, яким проходить пакет даних до певного сервера. Кроки:

1. Введіть команду `traceroute <IP-адреса сервера>`.
2. Запишіть послідовність хостів, через які проходить пакет.

Завдання № 17.

(Мережевий аналізатор) Аналіз мережевого трафіку за допомогою Wireshark. Кроки:

1. Встановіть Wireshark.
2. Запустіть Wireshark та виберіть мережевий інтерфейс.
3. Захопіть трафік.

4. Проаналізуйте захоплений трафік.

Завдання № 18.

(Мережева діагностика) Визначення та усунення проблем із підключенням до мережі. Кроки:

1. Використовуйте інструменти діагностики мережі (наприклад, `ping`, `traceroute`).
2. Проаналізуйте результати та визначте причину проблеми.

Завдання № 19.

(Мережева безпека) Налаштування брандмауера для захисту комп'ютера від несанкціонованого доступу. Кроки:

1. Відкрийте налаштування брандмауера (Windows Firewall або подібне).
2. Додайте правила для дозволу або блокування певних програм або портів.

Завдання № 20.

(Створення мережі) Розроблення схеми мережі для невеликого офісу, враховуючи потреби користувачів та необхідний рівень безпеки. Кроки:

1. Визначте кількість комп'ютерів, принтерів та інших пристроїв.
2. Визначте необхідну пропускну здатність.
3. Створіть схему мережі з використанням відповідного обладнання.

Завдання № 21.

(Складність: легка): Сконфігурувати домашню Wi-Fi мережу (роутер) з надійним паролем та назвою (SSID). Кроки:

1. Підключитися до роутера через веб-інтерфейс (відкрити браузер і ввести IP-адресу роутера).
2. Змінити ім'я мережі (SSID).
3. Встановити надійний пароль для захисту Wi-Fi мережі.
4. Переконатися, що роутер оновлено до останньої версії прошивки.

Завдання № 22.

(Складність: легка): Правильно розташувати Ethernet-кабель від роутера до комп'ютера для оптимального сигналу. Кроки:

1. Перевірити наявність перешкод (стіни, металеві предмети) між роутером та комп'ютером.
2. Розмістити роутер та комп'ютер таким чином, щоб між ними було пряме видиме простір.

3. Використовувати Ethernet-кабель достатньої довжини.

Завдання № 23.

(Складність: середня): Налаштувати спільний доступ до принтера в локальній мережі, щоб всі комп'ютери могли його використовувати. Кроки:
1. Увійти в налаштування принтера.
2. Увімкнути спільний доступ до принтера.
3. На комп'ютерах, які повинні використовувати принтер, додати принтер у список доступних принтерів.

Завдання № 24.

(Складність: середня): Проаналізувати трафік у містковій мережі (наприклад, за допомогою інструмента моніторингу мережі) для виявлення проблемних місць. Кроки:
1. Встановити інструмент моніторингу мережі.
2. Збирати дані про трафік в різних частинах MAN.
3. Проаналізувати зібрані дані, шукаючи піки завантаження, затримки або інші аномалії.

Завдання № 25.

(Складність: середня): Налаштувати VPN-з'єднання для безпечного доступу до ресурсів в містковій мережі. Кроки:
1. Отримати облікові дані VPN від адміністратора MAN.
2. Встановити VPN-клієнт.
3. Налаштувати VPN-з'єднання з використанням облікових даних та параметрів, наданих адміністратором.

Завдання № 26.

(Складність: складна): Створити мережеве рішення, яке забезпечує стабільний та якісний зв'язок для відеоконференцій у межах MAN. Кроки:
1. Оцінити необхідну пропускну здатність.
2. Вибрати відповідне обладнання (камери, мікрофони, комутатори).
3. Налаштувати мережеві параметри (QoS).

Завдання № 27.

(Складність: легка): Виміряти швидкість інтернет-з'єднання (завантаження, вивантаження, ping). Кроки:
1. Використати онлайн-сервіс для тестування швидкості (наприклад, Speedtest).

2. Записати результати тестування.

Завдання № 28.

(Складність: середня): Вивчити, як дані маршрутизуються через різні мережі у глобальній мережі (наприклад, через маршрутизатор). Кроки:
1. Використати інструмент для перевірки маршрутів (traceroute).
2. Проаналізувати отримані результати, щоб зрозуміти, через які мережі проходять дані.

Завдання № 29.

(Складність: середня): Налаштувати власний DNS-сервер для швидшого доступу до вебсайтів. Кроки:
1. Отримати IP-адресу DNS-сервера.
2. Увійти в налаштування операційної системи та встановити DNS-сервер.

Завдання № 30.

(Складність: легка): Виміряти час відправлення та отримання пакета даних до різних серверів в Інтернеті. Кроки:
1. Відкрити командний рядок.
2. Використати команду `ping` (наприклад, `ping google.com`).
3. Записати час відповіді (latency).

Завдання № 31.

(Складність: легка): Визначити IP-адресу комп’ютера в мережі за допомогою командного рядка або графічного інтерфейсу.

Завдання № 32.

(Складність: легка): Перевірити, чи комп’ютер правильно підключений до мережі та має доступ до інтернету.

Завдання № 33.

(Складність: середня): Вивчити основні протоколи TCP/IP (IP, TCP, UDP) та їх роль у мережевій комунікації.

Завдання № 34.

(Складність: середня): Налаштувати файрвол для захисту комп’ютера від несанкціонованого доступу з мережі.

Завдання № 35.

(Складність: середня): Створити схематичне зображення мережі, включаючи всі пристрої та їх взаємозв’язки.

Завдання № 36.

(Складність: складна): Діагностувати та усунути проблему з підключенням до мережі.

Завдання № 37.

(Складність: складна): Змінити налаштування мережі для покращення продуктивності та безпеки.

Завдання № 38.

(Складність: середня): Описати, що таке NAT (Network Address Translation) та як воно працює.

Завдання № 39.

(Складність: середня): Вивчити основні заходи захисту мережі від несанкціонованого доступу та шкідливого програмного забезпечення.

Завдання № 40.

(Складність: складна): Порівняти різні мережеві технології (Ethernet, Wi-Fi, оптика) за різними критеріями (швидкість, вартість, надійність).

Завдання № 41.

Опишіть покроково, як налаштувати Wi-Fi мережу в домашньому роутері.

Перевірка: Чи описано всі необхідні кроки – зміна SSID, налаштування пароля, оновлення прошивки?

Завдання № 42.

Опишіть, яка роль відіграє сервер у комп’ютерній мережі. Наведіть три конкретні приклади серверів та їх функції. Кроки:

1. Визначте поняття «сервер».
2. Перерахуйте три приклади серверів.
3. Опишіть функцію кожного з них.

Завдання № 43.

Поясніть різницю між клієнтом і сервером. Наведіть приклад взаємодії клієнта та сервера. Кроки:

1. Розберіть визначення «клієнт» та «сервер».
2. Наведіть приклад (наприклад, завантаження вебсторінки).
3. Поясніть, як клієнт і сервер взаємодіють у цьому прикладі.

Завдання № 44.

(Складність: середня): Що таке маршрутизатор? Поясніть, яку функцію виконує маршрутизатор у комп'ютерній мережі. Кроки:

1. Визначте, що таке маршрутизатор.
2. Поясніть його роль у перенаправленні даних.
3. Опишіть коротко, як він визначає шлях даних.

Завдання № 45.

(Складність: середня): Налаштуйте простий домашній Wi-Fi роутер (якщо можливо). Змініть ім'я мережі (SSID) та пароль. Кроки:

1. Увійдіть в інтерфейс роутера (через веббраузер за IP-адресою, яку можна знайти в документації).
2. Змініть SSID.
3. Змініть пароль.
4. Переконайтеся, що зміни збережені.

Завдання № 46.

(Складність: середня): Перевірте швидкість інтернет-з'єднання за допомогою онлайн-сервісів тестування швидкості (наприклад, speedtest.net). Кроки:

1. Відкрийте веббраузер.
2. Перейдіть на сайт speedtest.net.
3. Запустіть тест.
4. Запишіть результати (швидкість завантаження та вивантаження).

Завдання № 47.

(Складність: середня): Дізнайтеся свою IP-адресу за допомогою команди в командному рядку (Windows) або терміналі (Linux/macOS): `ipconfig` (Windows) або `ifconfig` (Linux/macOS). Кроки:

1. Відкрийте командний рядок/термінал.

2. Введіть відповідну команду.
3. Запишіть отриману IP-адресу.

Завдання № 48.

(Складність: середня): Використовуйте інструмент сканування мережі (наприклад, Advanced IP Scanner) для виявлення пристроїв, підключених до вашої локальної мережі. Кроки:
1. Завантажте та встановіть інструмент сканування.
2. Запустіть сканування.
3. Запишіть список пристроїв, виявлених у мережі.

Завдання № 49.

(Складність: середня): З'єднайте два комп'ютери за допомогою комутатора. Перевірте, чи можуть вони спілкуватися між собою. Кроки:
1. Підключіть обидва комп'ютери до комутатора.
2. Переконайтеся, що обидва комп'ютери підключені до мережі.
3. Перевірте, чи можуть вони розпізнати один одного (наприклад, за допомогою команд ping).

Завдання № 50.

(Складність: середня): Створіть просте правило в налаштуваннях маршрутизатора для перенаправлення трафіку на певний вебсайт (наприклад, Google). Кроки:
1. Увійдіть в інтерфейс маршрутизатора.
2. Знайдіть розділ «Правила перенаправлення» або «URL-перенаправлення».
3. Створіть правило для перенаправлення трафіку на Google.
4. Переконайтеся, що правило збережене.

Завдання № 51.

(Складність: середня): Знайдіть MAC-адресу свого комп'ютера. Зрозумійте, як вона використовується для ідентифікації пристроїв у мережі. Кроки:
1. Визначте спосіб отримання MAC-адреси (залежить від ОС).
2. Запишіть MAC-адресу.
3. Поясніть, як MAC-адреса використовується для ідентифікації пристроїв.

Завдання № 52.

(Складність: складна): Виникла проблема з підключенням до Інтернету. Проаналізуйте можливі причини та знайдіть рішення (наприклад, перезавантаження роутера, перевірка кабелів). Кроки:

1. Зберіть інформацію про проблему.
2. Визначте можливі причини.
3. Спробуйте різні рішення.

Завдання № 53.

(Складність: складна): Використовуйте інструмент аналізу трафіку (наприклад, Wireshark) для перегляду даних, що передаються у вашій мережі. Кроки:

1. Завантажте та встановіть Wireshark.
2. Запустіть Wireshark та почніть збір трафіку.
3. Проаналізуйте зібрані дані.

Завдання № 54.

(Складність: складна): Проаналізуйте швидкість роботи мережі та знайдіть способи її оптимізації (наприклад, вимкнення непотрібних програм, оновлення драйверів). Кроки:

1. Виміряйте швидкість роботи мережі.
2. Визначте, які програми можуть впливати на швидкість.
3. Зробіть зміни та перевірте, чи покращилася швидкість.

Завдання № 55.

(Складність: складна): Спроєктуйте просту мережу для дому або офісу, включаючи маршрутизатор, комутатор та інші необхідні пристрої. Кроки:

1. Визначте потреби мережі.
2. Виберіть необхідні пристрої.
3. Складіть схему мережі.

Завдання № 56.

(Складність: складна): Встановіть та налаштуйте простий вебсервер (наприклад, Apache) на комп’ютері. Кроки:

1. Встановіть вебсервер.
2. Налаштуйте вебсервер.
3. Запустіть вебсервер.

Завдання № 57.

(Складність: складна): Напишіть простий скрипт (наприклад, на Python) для автоматизації певного завдання в мережі (наприклад, перевірка наявності з'єднання).

Завдання № 58.

Намалюйте схему, що показує взаємозв'язок між сервером, клієнтом, маршрутизатором та комутатором в комп'ютерній мережі. Кроки:

1. Намалюйте схему.
2. Позначте кожен компонент.
3. Покажіть, як вони взаємодіють.

Завдання № 59.

(Складність: середня): Опишіть відмінності між локальною мережею (LAN) та глобальною мережею (WAN). Кроки:

1. Визначте, що таке LAN та WAN?
2. Опишіть їхні відмінності.

Завдання № 60.

(Складність: середня): Назвіть три способи захисту комп'ютерної мережі від несанкціонованого доступу. Кроки:

1. Перерахуйте три способи захисту.
2. Опишіть кожен спосіб.

Завдання № 61.

(Складність: середня): Узагальніть, яка основна роль кожного з представлених компонентів (сервер, клієнт, маршрутизатор, комутатор) у роботі комп'ютерної мережі. Кроки:

1. Перерахуйте компоненти.
2. Опишіть роль кожного компонента.
3. Сформулюйте загальну роль кожної групи компонентів.

Завдання № 62.

Налаштуйте IP-адресу на комп'ютері. Кроки:

1. Відкрити налаштування мережі.
2. Вибрати тип підключення (Ethernet або Wi-Fi).
3. Ввести статичну IP-адресу, маску підмережі, шлюз за замовчуванням та DNS-сервери.

4. Перевірити налаштування в командному рядку (ping шлюзу за замовчуванням).

Завдання № 63.

З’ясувати, як дані маршрутизуються між комп’ютерами. Кроки:

1. Використати команду `route print` (Windows) або `route -n` (Linux/macOS) для перегляду таблиці маршрутизації.
2. З’ясувати, як комп’ютер визначає шлях до різних мереж.

Завдання № 64.

Перевірити доступність іншого комп’ютера в мережі. Кроки:

1. Відкрити командний рядок.
2. Використати команду `ping <IP-адреса>` для відправки пакетів ICMP до вказаної IP-адреси.
3. Перевірити, чи отримано відповіді.

Завдання № 65.

Зафіксувати та проаналізувати мережевий трафік. Кроки:

1. Запустити Wireshark.
2. Вибрати мережеву карту для перехоплення трафіку.
3. Застосувати фільтр (наприклад, `http` або `ftp`) для відображення тільки потрібного трафіку.
4. Проаналізувати заголовки пакетів, щоб зрозуміти, як дані передаються.

Завдання № 66.

Створити простий HTTP-запит для отримання вебсторінки. Кроки:

1. Використати текстовий редактор для створення HTTP-запиту (наприклад, `GET /index.html HTTP/1.1`).
2. Відправити запит за допомогою `curl` або іншого інструменту для перегляду HTTP-запитів.
3. Перевірити, чи отримано відповідь з вебсторінкою.

Завдання № 67.

Підключитися до FTP-сервера та завантажити/завантажити файл. Кроки:

1. Використати FTP-клієнт (наприклад, FileZilla).
2. Ввести ім’я користувача та пароль для підключення до FTP-сервера.
3. Завантажити або завантажити файл.

Завдання № 68.

З’ясувати, чи було успішно виконано HTTP-запит. Кроки:

1. Відправити HTTP-запит.
2. Проаналізувати HTTP-відповідь та визначити статусний код.
3. Зрозуміти значення статусного коду (наприклад, 200 OK, 404 Not Found).

Завдання № 69.

Змінити DNS-сервери на комп’ютері та перевірити, чи правильно працює перевід імен. Кроки:

1. Відкрити налаштування мережі.
2. Змінити DNS-сервери на публічні сервери (наприклад, Google DNS: 8.8.8.8 та 8.8.4.4).
3. Перевірити роботу перевірки імен (ping до доменних імен).

Завдання № 70.

Проаналізувати заголовки HTTP-відповіді. Кроки:

1. Зробити HTTP-запит.
2. Проаналізувати HTTP-відповідь, звертаючи увагу на заголовки (Content-Type, Server, etc.).

Завдання № 71.

Використати `curl` для отримання HTTP-заголовків. Кроки:

1. Відкрити командний рядок.
2. Використати команду `curl -I <URL>` для отримання тільки заголовків HTTP-відповіді.

Завдання № 72.

Розбити великий файл на частини для передавання через FTP, щоб не перевищувати ліміти розміру файлу. Кроки:

1. Розбити великий файл на кілька менших.
2. Завантажити кожну частину окремо через FTP.
3. З’єднати частини в один файл на стороні клієнта.

Завдання № 73.

Підключитися до FTP-сервера без облікових даних (анонімно). Кроки:

1. Встановити FTP-клієнт.
2. Вказати анонімні облікові дані (зазвичай, пусте ім’я користувача та пароль).

Завдання № 74.

Підключитися до SFTP-сервера та передати файл. Кроки:

1. Використати SFTP-клієнт (наприклад, FileZilla з підтримкою SFTP).
2. Ввести облікові дані для SFTP-сервера.
3. Завантажити або завантажити файл.

Завдання № 75.

Виміряти швидкість передавання даних FTP. Кроки:

1. Завантажити або завантажити невеликий файл через FTP.
2. Зафіксувати час, необхідний для передавання даних.
3. Обчислити швидкість передавання даних (розмір файлу / час).

Завдання № 76.

Надіслати дані на вебсервер за допомогою HTTP-методу POST. Кроки:

1. Створити HTTP-запит методом POST, включаючи дані в тілі запиту (наприклад, в форматі JSON або URL-encoded).
2. Відправити запит за допомогою `curl` або іншого інструменту.

Завдання № 77.

Вивчити логфайли вебсервера, щоб зрозуміти, які запити надсилаються та як вебсервер реагує. Кроки:

1. Отримати доступ до логфайлів вебсервера.
2. Проаналізувати логфайли, звертаючи увагу на IP-адреси, URL-адреси, статусні коди та інші параметри.

Завдання № 78.

Налаштувати комп’ютер для використання проксі-сервера під час перегляду вебсторінок. Кроки:

1. Встановити IP-адресу та порт проксі-сервера.
2. Налаштувати налаштування проксі-сервера в веббраузері або операційній системі.

Завдання № 79.

За допомогою HTTP-запиту перевірити, чи доступний вебсайт та чи працює він коректно. Кроки:

1. Використовувати `curl` або інший інструмент для перевірки наявності вебсайту за його URL-адресою.
2. Проаналізувати HTTP-відповідь, щоб перевірити статусний код.

Завдання № 80.

Створити простий HTTP-сервер, який буде обслуговувати статичні файли. Кроки: (Потребує знання мови програмування, наприклад, Python)

1. Написати код, який буде слухати вхідні HTTP-запити.
2. Обробляти запити та повертати відповіді з вмістом файлів.

Завдання № 81.

Порівняти особливості та переваги протоколів HTTP/1.1 та HTTP/2. Кроки:

1. Ознайомитися з різними аспектами кожного протоколу (наприклад, мультиплексування, стиснення заголовків).
2. З'ясувати, як ці відмінності впливають на продуктивність вебсайтів.

Завдання № 82.

Налаштування простої локальної мережі з двома комп'ютерами, використовуючи Ethernet-кабелі та роутер. Кроки:

1. Підключіть комп'ютери до роутера.
2. Налаштуйте IP-адреси, маску підмережі, шлюз за замовчуванням та DNS-сервери на кожному комп'ютері.
3. Перевірте зв'язок за допомогою ping.

Завдання № 83.

Налаштування VPN-з'єднання для безпечного доступу до локальної мережі з віддаленого місця. Кроки:

1. Встановіть VPN-клієнт на комп'ютері.
2. Налаштуйте параметри VPN-з'єднання, використовуючи дані, надані адміністратором.
3. Перевірте зв'язок з локальною мережею.

Завдання № 84.

Створення папки, завантаження файлів та надання доступу іншим користувачам через хмарне сховище (Dropbox/Google Drive). Кроки:

1. Створіть обліковий запис на платформі хмарного сховища.
2. Створіть папку. Завантажте файли до папки.
3. Налаштуйте права доступу: читання/запис для різних користувачів.

Завдання № 85.

Створення облікового запису в сервісі електронної пошти та відправка/отримання листів. Кроки:

1. Зареєструйтеся в сервісі електронної пошти (Gmail, Outlook тощо).
2. Налаштуйте параметри поштової програми.
3. Відправте лист, перевірте отримання листа.

Завдання № 86.

Створення каналів, надсилання повідомлень, обмін файлами та здійснення відеодзвінків через месенджер для командної комунікації (Slack/Microsoft Teams). Кроки:
1. Створіть обліковий запис та канал у месенджері.
2. Відправте повідомлення до каналу.
3. Завантажте файл до каналу.
4. Заплануйте відеодзвінок.

Завдання № 87.

Створення документа в Google Docs, редагування документа кількома користувачами одночасно. Кроки:
1. Створіть новий документ в Google Docs.
2. Запросіть інших користувачів до редагування.
3. Відредагуйте документ, дивлячись на зміни в реальному часі.

Завдання № 88.

Завантаження та встановлення плагінів/розширень для браузера. Додавання функціональності в браузер через плагіни. Кроки:
1. Знайдіть та завантажте плагін/розширення для браузера.
2. Встановіть плагін/розширення.
3. Перевірте, чи працює плагін/розширення.

Завдання № 89.

Встановлення WordPress на хостингу, створення базової сторінки з текстом та зображенням. Кроки:
1. Зареєструйтеся на хостингу.
2. Встановіть WordPress.
3. За допомогою адмін-панелі WordPress створіть нову сторінку, додайте текст та зображення.
4. Опублікуйте сторінку.

Завдання № 90.

Створення дошки, колонок та карток для організації проєктів. Кроки:

1. Створіть обліковий запис на Trello.
2. Створіть нову дошку.
3. Додайте колонки (наприклад, “To Do”, “In Progress”, “Done”).
4. Створіть картки та додайте їх до відповідних колонок.

Завдання № 91.

Створення простого API (за допомогою онлайн інструментів), яке повертає випадкове число. Кроки:

1. Використайте онлайн інструмент для створення API (наприклад, RapidAPI).
2. Створіть endpoint, який повертає випадкове число.
3. Перевірте роботу API за допомогою інструменту тестування API.

Завдання № 92.

Включення та налаштування правил файрволу (Windows Firewall) для блокування певного трафіку. Кроки:

1. Відкрийте налаштування Windows Firewall.
2. Включіть файрвол.
3. Додайте правило, яке блокує трафік із невідомих джерел.

Завдання № 93.

Створення зашифрованого архіву з паролем. Кроки:

1. Використовуйте 7-Zip для створення архіву.
2. Встановіть пароль для архіву.
3. Перевірте, чи можна відкрити архів тільки за правильним паролем.

Завдання № 94.

Створення резервної копії важливих файлів на зовнішній носій або в хмарне сховище. Кроки:

1. Виберіть файли для резервного копіювання.
2. Скопіюйте файли на зовнішній носій або в хмарне сховище.

Завдання № 95.

Підключення та налаштування принтера до локальної мережі. Кроки:

1. Підключіть принтер до роутера.
2. Встановіть драйвери принтера на комп’ютері.
3. Налаштуйте принтер в операційній системі.

Завдання № 96.

Перевірка IP-адреси та DNS-серверів, що використовуються комп'ютером. Кроки:

1. Відкрийте командний рядок.
2. Введіть команду `ipconfig` (Windows) або `ifconfig` (Linux/macOS).
3. Перевірте IP-адресу, маску підмережі, шлюз за замовчуванням та DNS-сервери.

Завдання № 97.

Вимірювання швидкості мережі (Speedtest) завантаження та віддавання даних. Кроки:

1. Відвідайте сайт Speedtest.
2. Запустіть тест.
3. Запишіть результати швидкості завантаження та віддавання.

Завдання № 98.

Використання інструментів для віддаленого доступу до комп'ютера (TeamViewer/AnyDesk). Кроки:

1. Встановіть TeamViewer або AnyDesk на обидва комп'ютери.
2. Запустіть програму. Введіть ідентифікатор користувача та пароль.

Завдання № 99.

Захоплення та аналіз мережевого трафіку (Wireshark). (Потребує базових знань про мережі) Кроки:

1. Встановіть Wireshark. Запустіть Wireshark.
2. Виберіть інтерфейс мережі для перехоплення трафіку.
3. Захопіть трафік.
4. Проаналізуйте захоплений трафік, фільтруючи за протоколом, джерелом або призначенням.

Завдання № 100.

Зміна налаштувань роутера (наприклад, зміна пароля, блокування певних сайтів). Кроки:

1. Увійдіть в інтерфейс адміністратора роутера (зазвичай через браузер).
2. Змініть пароль.
3. Налаштуйте батьківський контроль.

Завдання № 101.

Створення та редагування документації в Confluence, використовуючи різні формати та інтеграції. Кроки:

1. Зареєструйтесь в Confluence.
2. Створіть нову сторінку.
3. Використовуйте текстовий редактор, редактор зображень, та інші інструменти для створення контенту.
4. Додайте інтеграції з іншими інструментами.

Завдання № 102.

Опишіть, як можна налаштувати VPN-з'єднання для доступу до ресурсів у містковій мережі. Перевірка: Чи описано всі необхідні кроки – отримання облікових даних, встановлення VPN-клієнта, налаштування з'єднання?

Завдання № 103.

Виміряйте швидкість інтернет-з'єднання за допомогою онлайн-сервісу. Запишіть результати.

Завдання № 104.

Як визначити IP-адресу комп'ютера в мережі? Оцінюється здатність до використання командного рядка або графічного інтерфейсу.

Завдання № 105.

Порівняйте різні мережеві технології за критеріями: швидкість, вартість, надійність.

Завдання № 106.

Опишіть кроки налаштування простого Wi-Fi роутера (зміна SSID та пароля).

Завдання № 107.

Намалюйте схему, що показує взаємозв'язок між маршрутизатором, комутатором, сервером та клієнтом у комп'ютерній мережі.

Завдання № 108.

Створіть просту схему мережі для домашнього офісу, включаючи маршрутизатор, комутатор та комп'ютери.

Завдання № 109.

За допомогою `ping` перевірте доступність комп’ютера з IP-адресою 192.168.1.1. Проаналізуйте результати.

Завдання № 110.

Використовуйте `curl` для отримання заголовків HTTP-відповіді для вебсайту google.com.

Завдання № 111.

Завантажте файл із FTP-сервера за допомогою FTP-клієнта.

Завдання № 112.

Проаналізуйте лог-файл вебсервера та знайдіть запити до сайту, які завершились помилкою 404 (Not Found).

Завдання № 113.

Визначте IP-адресу та маску підмережі вашого комп’ютера.

Завдання № 114.

Вкажіть DNS-сервери, які використовуються вашим комп’ютером.

Завдання № 115.

Створіть обліковий запис на одному із хмарних сховищ та завантажте на нього файл.

Завдання № 116.

Відправте електронний лист з прикріпленим файлом.

Завдання № 117.

Використовуйте інструмент для спільного редагування документа (Google Docs, Microsoft Office Online) та поділіться документом з іншими користувачами.

Завдання № 118.

Встановіть антивірусне програмне забезпечення на комп’ютер та проскануйте його на наявність вірусів.

Завдання № 119.

Налаштуйте файрвол на вашому комп’ютері.

Завдання № 120.

Створіть просту локальну мережу з двома комп’ютерами та налаштуйте між ними обмін файлами.

Завдання № 121.

Налаштуйте VPN-з’єднання для доступу до локальної мережі з віддаленого місця.

Завдання № 122.

Створіть та налаштуйте вебсайт з використанням CMS (WordPress).

Завдання № 123.

Використовуйте інструмент для віддаленого доступу до комп’ютера та підключіться до нього з іншого пристрою.

Завдання № 124.

Виміряйте швидкість завантаження та віддавання даних вашого інтернет-з’єднання.

ТЕСТИ

1. Що таке комп’ютерна мережа?

а) група комп’ютерів, з’єднаних лише для гри;

б) група комп’ютерів, з’єднаних для обміну даними та ресурсами;

в) одиночний комп’ютер, який підключається до інтернету;

г) програмне забезпечення для захисту комп’ютерів.

2. Який із перелічених компонентів НЕ є частиною комп’ютерної мережі?

а) комп’ютери;

б) з’єднувальні кабелі;

в) операційна система;

г) двірний дзвінок.

3. Яка мережа зазвичай охоплює один будинок або офіс?

а) WAN;

б) MAN;

в) LAN;

г) PAN.

4. Яка з перелічених мереж є найбільшою?
а) LAN;
б) MAN;
в) WAN;
г) PAN.

5. Яка топологія мережі передбачає, що всі пристрої з'єднані з центральним вузлом?
а) кільцева;
б) шинна;
в) зіркова;
г) деревоподібна.

6. Яка архітектура мережі характеризується рівними правами та можливостями для всіх пристроїв?
а) Client-Server;
б) Peer-to-Peer;
в) зіркова;
г) кільцева.

7. Який протокол використовується для бездротового з'єднання в домашніх мережах?
а) Ethernet;
б) DSL;
в) Wi-Fi;
г) Bluetooth.

8. Який тип мережі використовує фізичні кабелі для передавання даних?
а) бездротова;
б) провідна;
в) оптична;
г) інфрачервона.

9. Що таке маршрутизатор?
а) пристрій для друку документів;
б) пристрій для з'єднання комп'ютерів у мережі;
в) пристрій для захисту комп'ютерів від вірусів;

г) пристрій для зберігання даних.

10. Яка з перелічених характеристик найкраще описує Client-Server мережу?
а) всі комп’ютери рівні за правами;
б) один або кілька серверів надають ресурси клієнтам;
в) всі комп’ютери з’єднані в кільце;
г) мережа використовує бездротове з’єднання.

11. Що означає скорочення MAN?
а) Local Area Network;
б) Metropolitan Area Network;
в) Wide Area Network;
г) Personal Area Network.

12. Яка з перелічених технологій забезпечує швидкий доступ до Інтернету за допомогою телефонної лінії?
а) Wi-Fi;
б) DSL;
в) Bluetooth;
г) Ethernet.

13. Яка з перелічених технологій використовується для бездротового з’єднання між пристроями на короткій відстані?
а) Wi-Fi;
б) Ethernet;
в) Bluetooth;
г) DSL.

14. Яка з наступних топологій забезпечує резервування даних у випадку збою одного з вузлів?
а) зіркова;
б) шинна;
в) кільцева;
г) деревоподібна.

15. Який протокол використовується для передавання електронної пошти?
а) HTTP;

б) FTP;
в) SMTP;
г) TCP.

16. Який із перелічених пристроїв використовується для перетворення даних у формат, придатний для передавання по мережі?
а) модем;
б) принтер;
в) клавіатура;
г) миша.

17. Яка з перелічених мереж забезпечує з'єднання між різними країнами та континентами?
а) LAN;
б) MAN;
в) WAN;
г) PAN.

18. Що таке IP-адреса?
а) фізична адреса комп'ютера;
б) логічна адреса комп'ютера в мережі;
в) пароль для входу в мережу;
г) назва комп'ютера.

19. Який із варіантів найкраще описує функцію комутатора в мережі?
а) передає дані між комп'ютерами в мережі;
б) перетворює дані в формат, придатний для передавання;
в) розподіляє дані між комп'ютерами в мережі;
г) захищає мережу від вірусів.

20. Який із наступних протоколів забезпечує безпечне з'єднання в Інтернеті?
а) HTTP;
б) FTP;
в) HTTPS;
г) SMTP.

21. Що таке локальна мережа?
а) офіс;

б) місто;
в) інтернет;
г) глобальна мережа.

22. Які технології зазвичай використовуються для побудови локальних мереж?
а) супутниковий зв’язок;
б) Ethernet;
в) Інтернет;
г) MPLS.

23. У чому різниця між локальною та містковою мережею?
а) радіус дії;
б) вартість;
в) швидкість;
г) всі перелічені варіанти.

24. Які технології зазвичай використовуються для побудови місткових мереж?
а) DSL;
б) Файбер-оптика;
в) Bluetooth;
г) Wi-Fi.

25. Що таке глобальна мережа?
а) офіс;
б) інтернет;
в) домашня мережа;
г) місткова мережа.

26. Які технології зазвичай використовуються для побудови глобальних мереж?
а) Ethernet;
б) супутниковий зв’язок;
в) MPLS;
г) Bluetooth.

27. Що таке IP-адреса?

а) назва комп;ютера;

б) унікальний номер комп’ютера в мережі;

в) пароль до мережі;

г) адреса роутера.

28. Які основні заходи безпеки слід вжити для захисту мережі?

а) встановити надійний пароль;

б) оновлювати програмне забезпечення;

в) використовувати файрвол;

г) усі перелічені варіанти.

30. Що таке TCP/IP?

а) один протокол для передавання даних;

б) сімейство протоколів, що забезпечує мережеву інфраструктуру;

в) протокол для передачі вебсторінок;

г) протокол для передавання файлів.

31. Яка основна функція IP-протоколу?

а) забезпечення надійного з’єднання між комп’ютерами;

б) адресація та маршрутизація пакетів даних;

в) передавання даних за допомогою http;

г) передавання даних за допомогою ftp.

32. Що таке TCP та UDP? Які їхні відмінності?

а) TCP забезпечує швидке передавання, а UDP – надійну;

б) TCP забезпечує надійне передавання з підтвердженням, а UDP – швидке без підтвердження;

в) TCP та UDP – це один і той самий протокол;

г) TCP використовується для вебсторінок, а UDP – для аудіо.

33. Що таке таблиця маршрутизації?

а) список файлів, які потрібно завантажити;

б) таблиця, що містить інформацію про те, як дані маршрутизуються між мережами;

в) список вебсайтів, які відвідані користувачем;

г) налаштування IP-адреси.

34. Що таке HTTP?

а) протокол для передавання файлів;

б) протокол для передавання вебсторінок та інших ресурсів;

в) протокол для встановлення з’єднання між комп’ютерами;

г) протокол для передавання аудіо та відео.

35. Які основні компоненти HTTP-запиту?

а) IP-адреса, порт, дані;

б) метод (GET, POST тощо), URL, заголовки;

в) розмір файлу, тип файлу, дані;

г) пароль, ім’я користувача, дані.

36. Що таке статусний код HTTP?

а) код, що вказує на тип файлу;

б) код, що вказує на результат виконання запиту (наприклад, 200 OK, 404 Not Found);

в) код, що вказує на кількість байтів, отриманих з сервера;

г) код, що вказує на час виконання запиту.

37. Як HTTP працює на основі клієнт-серверної моделі?

а) сервер надсилає дані клієнту;

б) клієнт надсилає запит на сервер, а сервер відправляє відповідь;

в) сервер та клієнт обмінюються даними безпосередньо;

г) клієнт та сервер працюють паралельно, не взаємодіючи.

38. Що таке FTP?

а) протокол для передавання вебсторінок;

б) протокол для передавання файлів між комп’ютерами;

в) протокол для встановлення з’єднання між комп’ютерами;

г) протокол для передавання аудіо та відео.

39. Які два з’єднання використовуються в FTP?

а) з’єднання для даних та з’єднання для аутентифікації;

б) з’єднання для контрольних команд та з’єднання для передавання даних;

в) з’єднання для завантаження та з’єднання для завантаження;

г) з’єднання для вебсторінок та з’єднання для файлів.

40. Що таке SFTP та FTPS? У чому їхня різниця?

а) SFTP – безпечна версія FTP, FTPS – нестабільна;

б) SFTP – безпечна версія FTP, FTPS – безпечна версія FTP з шифруванням;

в) SFTP – нестабільна версія FTP, FTPS – безпечна версія FTP;

г) SFTP та FTPS – це один і той самий протокол.

ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Що таке комп’ютерна мережа?
2. Назвіть основні компоненти комп’ютерної мережі.
3. Яка роль мережевого обладнання?
4. Назвіть функцію програмного забезпечення.
5. Прокоментуйте основну класифікацію мереж.
6. Які переваги та недоліки локальних мереж порівняно з містковими?
7. Як правильно розташувати Ethernet-кабель для забезпечення оптимального сигналу? Оцінюється здатність до практичного застосування знань.
8. Які переваги та недоліки місткових мереж порівняно з локальними?
9. Як можна проаналізувати трафік у містковій мережі за допомогою моніторингу? Оцінюється здатність до виявлення проблемних місць.
10. Які переваги та недоліки глобальних мереж порівняно з локальними та містковими?
11. Як можна визначити маршрути, якими дані проходять через глобальну мережу? Оцінюється здатність до використання інструментів та аналізу даних.
12. Що таке NAT (Network Address Translation)? Оцінюється здатність до пояснення концепції.
13. Що таке комп’ютерна мережа? Наведіть 3 приклади її застосування в повсякденному житті.
14. Яка основна роль сервера у комп’ютерній мережі? Перелічіть 3 типи серверів та коротко опишіть їх функції.
15. Що таке клієнт у комп’ютерній мережі? Наведіть 3 приклади клієнтських пристроїв.
16. Поясніть, як маршрутизатор забезпечує зв’язок між різними мережами.
17. Чим комутатор відрізняється від хаба?
18. Яку функцію виконує комутатор у локальній мережі?
19. Яка основна функція IP-адреси?
20. Як можна дізнатися свою IP-адресу?
21. Що таке MAC-адреса? Яка її роль у роботі комп’ютерної мережі?

22. Які інструменти можна використовувати для тестування швидкості інтернет-з’єднання?
23. Яка мета сканування комп’ютерної мережі?
24. Які пристрої можна виявити за допомогою сканера?
25. Як маршрутизатор визначає шлях для передавання даних?
26. Яка основна відмінність між комутацією та хабуванням даних?
27. Поясніть, що таке NAT і чому він необхідний у домашніх мережах.
28. Яку функцію виконує брандмауер у комп’ютерній мережі?
29. Опишіть 3 можливі причини проблем з підключенням до Інтернету та запропонуйте способи їх вирішення.
30. Що можна дізнатися, проаналізувавши трафік комп’ютерної мережі за допомогою інструменту, такого як Wireshark?
31. Назвіть 3 способи оптимізації швидкості роботи комп’ютерної мережі.
32. Назвіть 3 способи захисту комп’ютерної мережі від несанкціонованого доступу.
33. Узагальніть роль кожного з представлених компонентів (сервер, клієнт, маршрутизатор, комутатор) у роботі комп’ютерної мережі.
34. Поясніть різницю між локальною мережею (LAN) та глобальною мережею (WAN).
35. Які переваги використання FTP порівняно з іншими протоколами для передачі файлів?
36. Чому TCP/IP вважається основою Інтернету?
37. Яка різниця між HTTP та HTTPS?
38. Що таке «проксі-сервер» і як він може бути використаний?
39. Опишіть, як працює процес передавання файлу через FTP.
40. Яка різниця між локальною мережею (LAN) та паралельною мережею (WAN)?
41. Що таке VPN і для чого він використовується?
42. Які основні типи мереж ви знаєте? Наведіть приклади використання кожної.
43. Що таке IP-адреса та DNS-сервер? Чому вони важливі?
44. Що таке файрвол і яку роль він відіграє в безпеці мережі?
45. Наведіть приклади технологій, які використовуються для обміну даними в мережі.
46. Які переваги використання хмарних сховищ (Dropbox, Google Drive) порівняно з локальним зберіганням файлів?
47. Що таке API та як він використовується для обміну даними між програмами?
48. Які інструменти можна використовувати для спільної роботи над документами?

49. Які переваги використання месенджерів (Slack, Teams) для командної комунікації?
50. Які способи шифрування даних можна використовувати для захисту даних у мережі?
51. Що таке антивірусне програмне забезпечення та чому воно важливе?
52. Які заходи можна вжити для забезпечення безпеки локальної мережі?
53. Що таке «батьківський контроль» і як його можна налаштувати?
54. Опишіть, як використання мереж впливає на ефективність роботи команди.
55. Назвіть три переваги використання хмарних технологій для спільної роботи.
56. Які основні заходи безпеки слід вживати для захисту даних в мережі?
57. Як різні інструменти для спільної роботи можуть допомогти покращити комунікацію та співпрацю?

ТЕМА 2. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мета: формувати знання та навички щодо основ інформаційної безпеки, вивчити методи захисту інформації в комп'ютерних мережах, ознайомитися з потенційними загрозами для інформаційної системи та способами їхнього уникнення або обмеження впливу.

ТЕОРЕТИЧНІ РЕКОМЕНДАЦІЇ ДО ТЕМИ 2

2.1. Що таке інформаційна безпека? Поняття та терміни

Інформаційна безпека – це комплекс заходів, спрямованих на захист інформації від несанкціонованого доступу, використання, розголошення, модифікації або знищення. Це не просто технічний аспект, а й процес, що включає організаційні, юридичні та людські фактори.

Ключові поняття та терміни:

Аутентичність – забезпечення того, що інформація справжня та не була підроблена.

Вразливість – слабка сторона в інформаційній системі або процедурах, яка може бути використана зловмисником для здійснення атаки. Приклади: незахищені паролі, застаріле програмне забезпечення, відсутність резервного копіювання.

Доступність – забезпечення того, щоб авторизовані користувачі могли отримати доступ до інформації вчасно та без перешкод.

Загроза – потенційна можливість, яка може призвести до негативного впливу на інформаційну систему або інформаційний актив. Приклади: віруси, хакерські атаки, помилки персоналу, стихійні лиха.

Захист – заходи, спрямовані на зменшення ймовірності виникнення загрози або на мінімізацію наслідків її використання.

Інформація – будь-який значущий символ, даних, знання, що може бути закодований та переданий. Це може бути текст, зображення, аудіо, відео, код, дані бази даних тощо.

Інформаційна система – комплекс апаратних, програмних та людських ресурсів, що обробляє, зберігає та передає інформацію.

Інформаційний актив – будь-яка інформація, що має цінність для організації або особи. Це може бути комерційна таємниця, інтелектуальна власність, персональні дані, фінансова інформація тощо.

Конфіденційність – забезпечення того, щоб інформація була доступна лише авторизованим особам.

Неприпустимість – забезпечення того, що особу, яка надіслала або отримала інформацію, неможливо заперечити.

Ризик – ймовірність того, що загроза буде використана для експлуатації вразливості, і наслідки цього. (Ризик = Ймовірність + Вплив).

Цілісність – забезпечення точності та повноти інформації, а також захист від несанкціонованої модифікації.

Типи інформаційної безпеки:

Людська інформаційна безпека – забезпечення безпечної поведінки користувачів та персоналу (навчання, підвищення обізнаності про ризики).

Організаційна інформаційна безпека – заходи, що реалізуються за допомогою організаційних процедур та політик (політики безпеки, процедури управління доступом, навчання персоналу тощо).

Технічна інформаційна безпека – заходи, що реалізуються за допомогою технічних засобів (брандмауери, антивірусне програмне забезпечення, шифрування, системи виявлення вторгнень тощо).

Юридична інформаційна безпека – захист інформації відповідно до законодавства (закони про захист персональних даних, закони про авторське право тощо).

Важливо розуміти, що **інформаційна безпека** – це не статична концепція, а динамічний процес, який потребує постійного моніторингу, адаптації та вдосконалення.

2.2. Загрози інформаційній безпеці

Інформаційна безпека в сучасному світі становить значний виклик, оскільки постійно з'являються нові та ускладнюються методи атак.

Розглянемо основні типи загроз:

1. Віруси (Viruses) – це шкідливі програми, які можуть розмножуватися та поширюватися, заражаючи інші файли та системи. Вони часто прикріплюються до легітимних програм, і коли заражена програма запускається, вірус активується.

Віруси можуть пошкодити файли, викрадати дані, вимикати системи або навіть використовувати заражені комп'ютери для розповсюдження.

Способи поширення: електронна пошта, заражені вебсайти, носії інформації (USB-накопичувачі).

Захист: антивірусне програмне забезпечення, регулярні оновлення, обережне відкриття вкладок у браузері та приєднаних файлів.

2. Шкідливе програмне забезпечення (Malware - Malicious Software) – це загальний термін, який охоплює широкий спектр шкідливих програм, включаючи віруси, трояни, черв'яки, шпигунське ПЗ, рекламне ПЗ та інші.

Різновиди:

Трояни (Trojans) – маскуються під корисні програми, але при використанні виконують шкідливі дії.

Черв'яки (Worms) – самостійно поширюються по мережі, не потребуючи введення на комп'ютер користувачем.

Шпигунське ПЗ (Spyware) – збирає інформацію про користувача (звички, паролі, дані) та передає її злочинцям.

Рекламне ПЗ (Adware) – відображає небажану рекламу.

Захист – антишкідливе програмне забезпечення, брандмауер, регулярні оновлення, обережність при завантаженні та встановленні програм.

3. Фішинг (Phishing) – це метод шахрайства, коли зловмисники видають себе за легітимні організації (банки, соціальні мережі, державні установи) для отримання конфіденційної інформації, такої як логіни, паролі, номери кредитних карток.

Фішингові електронні листи, повідомлення або вебсайти імітують офіційні, щоб змусити користувачів ввести свої дані. Приклади: Електронні листи з повідомленням про проблеми з обліковим записом, пропонування виграшів, запити на внесення даних для перевірки особи.

Захист – критичне ставлення до електронних листів та повідомлень, перевірка адреси відправника, не вводити особисту інформацію на підозрілих вебсайтах, використання двофакторної аутентифікації.

4. DDoS-атаки (Distributed Denial of Service Attacks) – це спроби вивести з ладу вебсайт або сервіс, перевантажуючи його великою кількістю запитів із різних джерел.

Зловмисники використовують мережу заражених комп'ютерів (ботнетов) для одночасного відправлення великої кількості запитів на цільовий сервер.

Наслідки: недоступність вебсайту, втрата прибутку, пошкодження репутації.

Захист: використання сервісів захисту від DDoS-атак, брандмауер, моніторинг трафіку.

Важливо пам'ятати, що **інформаційна безпека** – це безперервний процес. Регулярне оновлення програмного забезпечення, використання надійних паролів, обережність в Інтернеті та використання відповідних інструментів захисту – це ключові фактори для захисту від цих та інших загроз.

2.3. Методи захисту інформації

Розглянемо кожен із цих методів більш детально:

1. Антивірусне програмне забезпечення – це програмні продукти, призначені для виявлення, запобігання та видалення шкідливого програмного забезпечення (malware), такого як віруси, трояни, черв'яки, шпигунське ПЗ та інше.

Сканування: регулярно сканує файли, програми та систему на наявність відомих шкідливих програм.

Реальний час: моніторить активність системи в режимі реального часу, блокуючи потенційно шкідливі дії.

База даних: використовує базу даних відомих шкідливих програм, що постійно оновлюється.

Хуманінг (Heuristics): виявляє нові, ще не відомі шкідливі програми, аналізуючи їхню поведінку.

Приклади програм: Norton Antivirus, McAfee, Kaspersky, Bitdefender, Avast, Windows Defender.

Важливо пам'ятати, що антивірус не є панацеєю. Необхідно дотримуватися правил безпечної поведінки в Інтернеті.

2. Брандмауер (Firewall) – це система, що контролює мережевий трафік, блокуючи несанкціонований доступ до комп'ютера або мережі.

Перевірка трафіку: брандмауер аналізує кожен пакет даних, що намагається пройти через нього, порівнюючи його з налаштованими правилами.

Фільтрація: залежно від правил, трафік може бути: *дозволений* (проходить далі) і *заблокований* (не проходить далі).

Типи брандмауерів:

Апаратні (Hardware) – фізичні пристрої, які встановлюються на мережевому обладнанні.

Програмні (Software) – програми, що встановлюються на комп'ютер. (Наприклад, Windows Firewall, iptables).

Важливо пам'ятати, що брандмауер захищає від зовнішніх загроз, але не захищає від шкідливих програм, що вже знаходяться всередині системи.

3. Шифрування (Encryption) – це процес перетворення даних у нечитабельний формат, який може бути прочитаний лише за допомогою ключа розшифрування.

Використовується алгоритм шифрування, який перетворює дані (текст) на шифротекст.

Типи шифрування:

Симетричне шифрування – використовується один і той же ключ для шифрування та розшифрування, наприклад, AES, DES.

Асиметричне шифрування – використовується пара ключів: відкритий ключ (для шифрування) та закритий ключ (для розшифрування), наприклад, RSA.

Застосування:

Шифрування файлів – захист особистої інформації та конфіденційних даних.

Шифрування електронної пошти – захист вмісту електронних листів.

Шифрування мережевого трафіку (HTTPS) – захист даних, що передаються через Інтернет.

Важливо пам'ятати, що шифрування захищає дані від несанкціонованого доступу, але не захищає від зламу самого алгоритму шифрування (хоча сучасні алгоритми дуже стійкі).

Взаємодія методів: Ці три методи працюють найкраще в комплексі. Антивірус захищає від шкідливих програм, брандмауер контролює доступ до мережі, а шифрування захищає дані від несанкціонованого доступу, навіть якщо система буде скомпрометована.

2.4. Правила безпечної роботи з інформацією

Безпека інформації – це ключовий аспект сучасного життя, особливо з урахуванням постійного збільшення кількості даних, що зберігаються та передаються онлайн. Дотримання правил безпеки допомагає захистити вашу особисту інформацію, фінанси та репутацію. Розглянемо два важливі аспекти: захист паролів та резервне копіювання даних.

1. Захист паролів:

Паролі є першою лінією захисту від несанкціонованого доступу до ваших облікових записів та даних. Ось **декілька порад** для створення та управління паролями: *паролі мають бути складними*; *довжина* (пароль повинен бути мінімум 12 символів, а краще – довше); *різноманітність*: використовуйте комбінацію великих та малих літер, цифр та спеціальних символів (наприклад, !, @, #, $, %, ^, & тощо); *уникайте особистої інформації*: не використовуйте імена, дати народження, адреси, імена домашніх тварин чи інші легко вгадувані дані; *унікальні паролі*: не використовуйте один і той самий пароль для різних облікових записів (якщо один пароль буде скомпрометовано, зловмисник матиме доступ до всіх ваших облікових записів, які використовують цей пароль); *регулярна зміна паролів*: змінюйте паролі регулярно, особливо для важливих облікових записів, наприклад, електронна пошта, банківські рахунки (рекомендовано змінювати паролі принаймні кожні 3-6 місяців).

Використання менеджера паролів: Менеджер паролів (наприклад, LastPass, 1Password, Bitwarden) генерує та зберігає унікальні, складні паролі для всіх ваших облікових записів. Він також може автоматично заповнювати паролі на вебсайтах та в додатках, що робить їх використання зручним та безпечним.

Двофакторна аутентифікація (2FA): увімкніть двофакторну аутентифікацію для всіх облікових записів, які її підтримують. 2FA додає додатковий рівень захисту, вимагаючи не тільки пароль, але й код, згенерований на вашому телефоні або іншому пристрої.

Не зберігайте паролі в незашифрованих файлах або текстових документах: це значно підвищує ризик їх компрометації.

2. Резервне копіювання даних (backup) – це процес створення копії ваших даних для відновлення в разі втрати, пошкодження або крадіжки пристрою.

Ось деякі *способи резервного копіювання*:

Хмарне резервне копіювання: використовуйте хмарні сервіси (наприклад, Google Drive, iCloud, Dropbox, OneDrive) для автоматичного резервного копіювання ваших файлів, документів та фотографій.

Внутрішнє резервне копіювання: процес створення копій ваших даних, які зберігаються на локальних пристроях, тобто на вашому комп’ютері або підключених до нього зовнішніх накопичувачах.

Внутрішній жорсткий диск: регулярно переміщуйте важливі файли на зовнішній жорсткий диск.

USB-накопичувачі: використовуйте USB-накопичувачі для резервного копіювання даних.

Системи резервного копіювання (Backup Software): використовуйте програми для резервного копіювання, які можуть автоматично створювати резервні копії ваших файлів та системних налаштувань.

Регулярність: регулярно виконуйте резервне копіювання даних – щонайменше раз на місяць, а для важливих даних – щотижня.

Перевірка резервних копій: періодично перевіряйте, чи можуть бути відновлені ваші резервні копії, а це гарантує, що вони працюють належним чином у разі потреби.

Захист паролів та резервне копіювання даних є критично важливими для забезпечення безпеки вашої інформації. Дотримання цих правил допоможе вам уникнути фінансових втрат, втрати особистої інформації та інших неприємностей. Не ігноруйте ці аспекти безпеки – це інвестиція у вашу безпеку та спокій.

2.5. Захист особистої інформації в мережі

У сучасному цифровому світі захист особистої інформації в мережі є надзвичайно важливим аспектом нашого онлайн-життя. З кожним днем ми ділимося все більшою кількістю даних, і це робить нас більш вразливими до різних загроз.

Ось кілька *ключових стратегій та практик*, які допоможуть вам захистити свою інформацію:

1. Паролі та автентифікація:

Складні паролі: використовуйте складні паролі, що містять великі та малі літери, цифри та символи та уникайте використання особистої інформації (дату народження, імені домашнього улюбленця тощо).

Унікальні паролі: не використовуйте один і той самий пароль для різних онлайн-сервісів, бо, якщо один із них буде скомпрометований, інші залишаться в безпеці.

Менеджери паролів: використовуйте менеджер паролів (наприклад, LastPass, 1Password, Bitwarden) для генерації та безпечного зберігання складних паролів.

Двофакторна аутентифікація (2FA): увімкніть 2FA для всіх сервісів, що її підтримують. Це додає додатковий рівень захисту, вимагаючи підтвердження вашої ідентичності за допомогою іншого пристрою (наприклад, SMS-коду або додатку аутентифікації).

2. Безпека браузера:

Використовуйте безпечний браузер: Chrome, Firefox, Safari та Edge регулярно оновлюються та мають вбудовані функції безпеки.

Встановіть плагіни безпеки: розгляньте використання розширень для браузера, таких як AdBlock Plus, Privacy Badger, або HTTPS Everywhere, які блокують рекламу, відстеження та забезпечують безпечне з'єднання.

Регулярно оновлюйте браузер: оновлення містять важливі виправлення безпеки.

3. Захист від шкідливого програмного забезпечення:

Антивірус та антивірусне програмне забезпечення: встановіть надійне антивірусне програмне забезпечення та регулярно його оновлюйте.

Обережно відкривайте вкладення та посилання: не відкривайте підозрілі вкладення та посилання від незнайомих відправників.

Не завантажуйте програми з ненадійних джерел: завантажуйте програми тільки з офіційних магазинів (App Store, Google Play, Microsoft Store).

4. Захист пристроїв:

Захистіть свій телефон/планшет: встановіть на нього надійний пароль або використовуйте біометричну автентифікацію (відбиток пальця, сканування обличчя).

Регулярно оновлюйте операційну систему: оновлення містять виправлення безпеки та покращання продуктивності.

Використовуйте VPN (віртуальну приватну мережу): VPN шифрує ваш інтернет-трафік та приховує вашу IP-адресу, що особливо важливо при використанні публічних Wi-Fi мереж.

5. Особисті дані та соціальні мережі:

Налаштуйте конфіденційність у соціальних мережах: увімкніть налаштування конфіденційності, щоб обмежити доступ до вашої інформації.

Будьте обережні з тим, що ділитесь: не діліться надмірною особистою інформацією в соціальних мережах.

Перевіряйте права доступу додатків: переконайтеся, що додатки мають лише ті права доступу, які їм необхідні.

Використовуйте приватні повідомлення: не надсилайте конфіденційну інформацію через відкриті канали зв'язку.

6. Загальні поради:

Усвідомлюйте ризики: будьте пильними та усвідомлюйте ризики, пов'язані з використанням інтернету.

Оновлюйте інформацію: слідкуйте за новинами про кібербезпеку та оновлюйте свої знання.

Звертайтеся до фахівців: у разі виникнення підозрілих ситуацій звертайтеся до фахівців із кібербезпеки.

Ресурси для отримання додаткової інформації:

Національний Кібербезпековий Хаб: https://kb.gov.ua/kiberbezpeka/osobista-informatsiya/
Сайт CERT-UA (Український центр реагування на інциденти): https://cert.gov.ua/
Національний центр кібербезпеки та захисту інформації: https://nckeyb.gov.ua/

Захист особистої інформації в мережі – це постійний процес, який вимагає уваги та обізнаності. Дотримуючись цих порад, ви можете значно знизити ризик потрапити на шахраїв та захистити свою інформацію в цифровому світі.

ПРАКТИЧНІ ЗАВДАННЯ

Завдання № 1.

(Складність: легка): Складіть список з 5-7 ключових термінів з інформаційної безпеки (наприклад, конфіденційність, цілісність, доступність, загроза, вразливість, ризик). Для кожного терміна надайте просте визначення у 1-2 реченнях. Перевірте правильність визначень.

Завдання № 2.

(Складність: легка): Назвіть 5 прикладів інформаційних активів, які можуть бути важливими для компанії (наприклад, фінансові звіти, бази даних клієнтів, інтелектуальна власність). Опишіть, чому захист цих активів є важливим.

Завдання № 3.

(Складність: легка): Опишіть три можливі наслідки порушення конфіденційності персональних даних (наприклад, фінансові втрати, репутаційні збитки, юридичні проблеми).

Завдання № 4.

(Складність: легка): Наведіть 2 приклади потенційних вразливостей у системі (наприклад, слабкий пароль, незахищений Wi-Fi, застаріле програмне забезпечення).

Завдання № 5.

(Складність: легка): Опишіть ситуацію, коли існує високий ризик для інформаційної системи. Назвіть можливі загрози та вразливості, які сприяють цьому ризику.

Завдання № 6.

(Складність: середня): Вивчіть методи захисту від вірусів. Складіть короткий план дій щодо захисту інформаційної системи від вірусів. Включіть 3-4 ключові заходи (наприклад, встановлення антивірусного програмного забезпечення, регулярне оновлення програмного забезпечення, навчання персоналу).

Завдання № 7.

(Складність: середня): Прочитайте приклад політики безпеки (можна знайти в інтернеті). Визначте три пункти, які, на вашу думку, є найважливішими для забезпечення інформаційної безпеки. Поясніть, чому.

Завдання № 8.

(Складність: середня): Оцініть ризик витоку інформації в компанії. Визначте три можливі загрози та три можливі вразливості. Оцініть ймовірність та вплив кожної загрози.

Завдання № 9.

(Складність: середня): Вивчіть принципи роботи брандмауера. Створіть правила брандмауера для захисту комп’ютера від несанкціонованого доступу. Назвіть 3-5 правил (наприклад, блокування певних портів, обмеження доступу до певних ресурсів).

Завдання № 10.

(Складність: середня): Розробіть короткий навчальний матеріал (наприклад, інструкцію, презентацію) для персоналу, який повинен навчитися правильно використовувати паролі.

Завдання № 11.

(Складність: складна): Опишіть ситуацію, коли відбулося порушення інформаційної безпеки (наприклад, хакерська атака, витік даних). Проаналізуйте причини інциденту, наслідки та заходи, які необхідно вжити для усунення наслідків.

Завдання № 12.

(Складність: складна): Розробіть план реагування на інцидент інформаційної безпеки з чіткими кроками на кожному етапі (наприклад, виявлення, ідентифікація, локалізація, відновлення, аналіз).

Завдання № 13.

(Складність: складна): Вивчіть вимоги стандарту інформаційної безпеки. Оцініть, чи відповідає система компанії вимогам стандарту інформаційної безпеки (наприклад, ISO 27001).

Завдання № 14.

(Складність: складна): Розробіть політику управління доступом для інформаційної системи з чіткими правилами. Визначте принципи при наданні доступу до інформації та ресурсів.

Завдання № 15.

(Складність: складна): Вивчіть принципи шифрування. Опишіть: як шифрування може бути використано для захисту інформації. Наведіть приклади різних видів шифрування та їх застосування.

Завдання № 16.

(Складність: складна): Визначте показники безпеки. Спроєктуйте систему моніторингу безпеки для інформаційної системи. Визначте, які показники необхідно моніторити та як їх аналізувати.

Завдання № 17.

(Складність: складна): Опишіть ризики інформаційної безпеки, пов’язані з використанням хмарних сервісів. Наведіть приклади можливих атак та заходів захисту.

Завдання № 18.

(Складність: складна): Складіть стратегію резервного копіювання даних для інформаційної системи з частотою та місцем зберігання. Визначте, які дані необхідно резервно копіювати, як часто та де зберігати резервні копії.

Завдання № 19.

(Складність: складна): Оцініть ефективність заходів інформаційної безпеки, які використовують в організації. Визначте слабкі місця та запропонуйте шляхи їх усунення.

Завдання № 20.

(Складність: складна): Розробіть план навчання з питань інформаційної безпеки для персоналу організації з методами та матеріалами. Визначте теми, які необхідно висвітлити, та методи навчання.

Завдання № 21.

Налаштувати антивірусну програму та вручну перевірити систему на наявність вірусу. Кроки:

1. Встановити та налаштувати антивірусне програмне забезпечення.
2. Запустити повне сканування системи.
3. Якщо вірус виявлено, виконати рекомендовані дії з видалення (видалення, карантин, відновлення).
4. Перевірити систему після видалення вірусу.

Завдання № 22.

Аналіз підозрілого електронного листа. Визначити, чи є електронний лист фішингом. Кроки:

1. Отримати приклад підозрілого електронного листа.
2. Перевірити адресу відправника на наявність невідповідностей.
3. Звернути увагу на граматичні помилки та нелогічні пропозиції.
4. Перевірити посилання на наявність підозрілих доменів.
5. Запитати у «відправника» про інформацію, яку він просить (наприклад, дані кредитної картки).

Завдання № 23.

Тестування на вразливість вебсайту (Брутфорс). Спробувати отримати доступ до облікового запису користувача шляхом підбору пароля. Кроки:

1. Здійснити тестовий доступ до вебсайту.
2. Використовувати інструмент брутфорсу для підбору пароля.
3. Зафіксувати результати та проаналізувати їх.

Завдання № 24.

Налаштувати брандмауер для блокування несанкціонованого доступу. Кроки:

1. Увійти в інтерфейс налаштування брандмауера.
2. Створити правила для блокування певних типів трафіку.
3. Перевірити правила на наявність помилок.
4. Перевірити, чи блокує брандмауер несанкціонований доступ.

Завдання № 25.

Налаштувати антивірус для сканування USB-накопичувачів при підключенні. Кроки:

1. Увійти в налаштування антивірусу.
2. Увімкнути функцію сканування USB-накопичувачів.
3. Перевірити, чи сканується USB-накопичувач при підключенні.

Завдання № 26.

Використати інструмент для перевірки цілісності важливих системних файлів. Кроки:

1. Встановити інструмент перевірки цілісності (наприклад, HashCheck).
2. Запустити перевірку цілісності важливих файлів (наприклад, системних файлів операційної системи).
3. Порівняти отримані хеші з попередніми значеннями.

Завдання № 27.

Створити резервну копію важливих даних на зовнішній носій. Кроки:

1. Визначити важливі дані для резервного копіювання.
2. Створити резервну копію даних на зовнішній носій (наприклад, USB-накопичувач, зовнішній жорсткий диск).
3. Перевірити цілісність резервної копії.

Завдання № 28.

Проаналізувати журнали подій операційної системи на предмет підозрілої активності. Кроки:

1. Відкрити журнали подій операційної системи.
2. Проаналізувати записи на предмет підозрілих подій (наприклад, невдалі спроби входу, встановлення нових програм).

Завдання № 29.

Визначити, чи є мережевий трафік ознаками DDoS-атаки (моніторинг трафіку). Кроки:

1. Використовувати інструмент для моніторингу мережевого трафіку (наприклад, Wireshark).
2. Проаналізувати трафік на предмет великої кількості запитів з різних IP-адрес.

Завдання № 30.

Створити надійний пароль, який складно зламати. Кроки:

1. Використовувати комбінацію великих і малих літер, цифр і символів.
2. Уникати використання особистої інформації (наприклад, дата народження, ім’я).
3. Використовувати різні паролі для різних облікових записів.

Завдання № 31.

Встановити двофакторну аутентифікацію (2FA) для облікових записів. Кроки:

1. Увійти в налаштування облікового запису, який потрібно захистити.
2. Увімкнути двофакторну аутентифікацію.
3. Вибрати метод двофакторної аутентифікації (наприклад, SMS-код, додаток-аутентифікатор).

Завдання № 32.

Використати інструмент OWASP ZAP для сканування вебсайту на наявність вразливостей. Кроки:

1. Встановити OWASP ZAP.
2. Налаштувати сканування вебсайту.
3. Проаналізувати результати сканування.

Завдання № 33.

Розробити та впровадити політику паролів для організації. Кроки:

1. Визначити вимоги до паролів (довжина, складність).
2. Описати процедури зміни паролів.
3. Забезпечити дотримання політики паролів.

Завдання № 34.

Провести тренінг для працівників щодо розпізнавання фішингових електронних листів. Кроки:

1. Підготувати навчальний матеріал.
2. Провести тренінг.
3. Перевірити знання працівників.

Завдання № 35.

Створити план дій у разі виникнення інциденту інформаційної безпеки. Кроки:
1. Визначити типи інцидентів.
2. Розробити процедури реагування на кожен тип інциденту.
3. Забезпечити доступність необхідних ресурсів.

Завдання № 36.

Налаштувати VPN для шифрування трафіку під час використання публічних Wi-Fi мереж. Кроки:
1. Встановити VPN-клієнт.
2. Підключитися до VPN-сервера.
3. Перевірити, чи шифрується трафік.

Завдання № 37.

Забезпечити регулярне оновлення операційної системи, програм та антивірусного ПЗ. Кроки:
1. Увімкнути автоматичне оновлення.
2. Перевіряти наявність оновлень вручну.
3. Встановлювати оновлення.

Завдання № 38.

Відстежувати активність користувачів у системі для виявлення підозрілої поведінки. Кроки:
1. Використовувати інструменти моніторингу активності користувачів.
2. Визначати підозрілу поведінку (наприклад, спроби доступу до неавторизованих файлів, використання нетипових програм).

Завдання № 39.

Використання пристроїв для керування пакунками (MDM): управління та захист мобільних пристроїв, що використовуються для роботи. Кроки:
1. Встановити MDM на пристрої.
2. Налаштувати політики безпеки (наприклад, шифрування даних, блокування пристрою).

3. Віддалено керувати пристроями.

Завдання № 40.

Залучити фахівців для проведення тестування на проникнення, щоб виявити вразливості в системі. Кроки:

1. Замовити послуги тестування на проникнення.
2. Надати фахівцям доступ до системи.
3. Проаналізувати результати тестування.

Завдання № 41.

Надано звіт антивірусу, що містить інформацію про виявлений шкідливий код. Потрібно визначити тип шкідливого коду (наприклад, вірус, троян, шпигунське ПЗ) та його потенційну небезпеку у такій послідовності: проаналізувати звіт, звертаючи увагу на назву, класифікацію, потенційні дії та рекомендовані дії).

Завдання № 42.

Налаштувати повне сканування системи за допомогою антивірусу. Пояснити, як вибрати режим сканування (швидке, повне, оновлення бази даних), у такій послідовності: відкрити антивірус, перейти до налаштувань сканування, обрати режим та пункт «Повне сканування», натиснути кнопку «Сканувати»).

Завдання № 43.

Оновити базу даних антивірусу до останньої версії. Пояснити важливість регулярних оновлень, у такій послідовності: відкрити антивірус, перейти до налаштувань, знайти розділ «Оновлення баз даних», натиснути кнопку «Оновити»).

Завдання № 44.

Увімкнути та налаштувати Windows Firewall. Пояснити, як дозволити або заблокувати певний трафік. Кроки:

1. Відкрити “Панель управління” -> “Система та безпека” -> “Windows Defender Firewall”.
2. Увімкнути Firewall.
3. Додати правило для дозволу/блокування певного типу трафіку).

Завдання № 45.

Проаналізувати логи брандмауера для виявлення підозрілих спроб доступу до системи. Кроки:

1. Відкрити лог-файли брандмауера.
2. Знайти записи про спроби входу.
3. Визначити: чи відповідають вони нормальній активності.

Завдання № 46.

Налаштувати брандмауер для блокування трафіку з невідомих джерел, у такій послідовності: у налаштуваннях брандмауера, визначити правило для блокування трафіку з IP-адрес, які не знаходяться в дозволеному списку).

Завдання № 47.

Зашифрувати файл за допомогою програмного забезпечення для шифрування (наприклад, VeraCrypt). Пояснити: як створити пароль та шифрувати файл. Кроки:

1. Відкрити VeraCrypt.
2. Створити контейнер.
3. Додати файл.
4. Встановити пароль та шифрувати.

Завдання № 48.

Розшифрувати зашифрований файл за допомогою пароля, у такій послідовності: відкрити VeraCrypt, відкрити контейнер, ввести пароль та отримати доступ до розшифрованого файлу.

Завдання № 49.

Налаштувати шифрування електронної пошти (наприклад, S/MIME) для захисту вмісту листів. Дії залежать від використовуваного провайдера, зазвичай вимагає встановлення додаткових плагінів та налаштування).

Завдання № 50.

Розробити базову політику захисту інформації, яка включає використання антивірусу, брандмауера та шифрування для захисту важливих даних. Кроки:

1. Визначити ключові зони ризику.
2. Обрати відповідні методи захисту.
3. Розробити інструкції для користувачів.

Завдання № 51.

Створити тестовий сценарій для перевірки ефективності брандмауера (наприклад, спробувати отримати доступ до системи з неавторизованого джерела та перевірити: чи блокує брандмауер цей доступ).

Завдання № 52.

Створити резервну копію зашифрованих даних, використовуючи різні методи (наприклад, фізичне сховище, хмарне сховище), у такій послідовності: зашифрувати резервну копію, зберігати її в безпечному місці.

Завдання № 53.

Описати схематично архітектуру безпеки комп’ютера, включаючи антивірус, брандмауер, шифрування та інші компоненти (опис функцій кожного компонента та їх взаємодії).

Завдання № 54.

Порівняти декілька антивірусних програм та вибрати ту, що найбільш підходить для конкретних потреб. Оцінити функціональність, ціну, репутацію та зручність використання.

Завдання № 55.

Налаштувати політики безпеки для користувачів (наприклад, правила використання паролів, обмеження доступу до файлів).

Завдання № 56.

Створити на тестовому комп’ютері симуляцію атаки вірусом та перевірити: чи спрацьовують механізми захисту.

Завдання № 57.

Створити фішинговий лист та перевірити, чи може він обдурити користувача та спровокувати його перейти за посиланням.

Завдання № 58.

Налаштувати антивірус та шифрування на мобільному пристрої.

Завдання № 59.

Ввімкнути захист Wi-Fi (WPA2/WPA3) та налаштувати брандмауер для захисту домашньої мережі.

Завдання № 60.

Припустити, що на комп'ютері виявлено підозрілу активність. Розслідувати інцидент, використовуючи інструменти захисту інформації. Кроки:
1. Проаналізувати логи, звіт антивірусу.
2. Визначити причину інциденту.
3. Вжити заходів для усунення.

Завдання № 61.

Створіть пароль, який відповідає всім вимогам до складності (мінімум 12 символів, комбінація літер, цифр та спеціальних символів). Запишіть пароль у безпечному місці (не в текстовому файлі). Використовуйте генератор паролів (наприклад, на сайті LastPass) або самостійно складіть пароль, дотримуючись рекомендацій.

Завдання № 62.

Використовуйте онлайн-сервіс для перевірки сили створеного пароля (наприклад,
https://www.howsecureismypassword.com/), отримайте оцінку складності та рекомендації щодо покращання Оцініть: чи потребує він покращання.

Завдання № 63.

Зайдіть у налаштування облікового запису, увімкніть двофакторної аутентифікації (2FA) для облікового запису Gmail, Facebook або іншого важливого сервісу, який її підтримує. Налаштуйте метод 2FA (наприклад, SMS-код або застосунок-аутентифікатор).

Завдання № 64.

Завантажте та встановіть менеджер паролів (наприклад, LastPass, 1Password). Налаштуйте його, створіть обліковий запис, додайте до нього обліковий запис Gmail та дозвольте менеджеру автоматично заповнювати пароль.

Завдання № 65.

Змініть пароль для облікового запису, який використовується рідко (наприклад, старий обліковий запис соціальної мережі).

Завдання № 66.

Зробіть резервне копіювання всіх фотографій із вашого телефону на хмарне сховище (наприклад, Google Photos, iCloud). Опишіть послідовність дій.

Завдання № 67.

Зробіть резервне копіювання важливих документів (наприклад, резюме, контракти) на хмарне сховище: Google Drive, Dropbox або інший хмарний сервіс.

Завдання № 68.

Скопіюйте всі важливі файли з вашого комп'ютера на зовнішній жорсткий диск. Опишіть послідовність дій.

Завдання № 69.

Налаштуйте автоматичне резервне копіювання на зовнішній диск за допомогою програми для резервного копіювання (наприклад, EaseUS Todo Backup). Опишіть послідовність дій.

Завдання № 70.

Відновіть один із файлів з резервної копії, щоб перевірити, чи працює процес резервного копіювання належним чином. Опишіть послідовність дій.

Завдання № 71.

Використовуйте інструмент резервного копіювання Windows (дискове резервне копіювання) або macOS Time Machine для створення резервної копії всієї системи, у такій послідовності: запустіть інструмент, виберіть диски для резервного копіювання, налаштуйте графік резервного копіювання.

Завдання № 72.

Відновіть систему з резервної копії на тестовому комп'ютері або віртуальній машині. Дотримуйтесь інструкцій та переконайтеся, що система працює належним чином.

Завдання № 73.

Скопіюйте кілька важливих файлів на USB-накопичувач. Опишіть послідовність дій.

Завдання № 74.

Визначте, які файли не потребують постійного доступу. Зробіть резервне копіювання старих фотографій, документів та інших файлів, які рідко використовуються, на зовнішній диск або в хмару.

Завдання № 75.

Скопіюйте конфігураційні файли операційної системи (наприклад, registry в Windows). Використовуйте програму для резервного копіювання, яка може створити повну копію системи.

Завдання № 76.

Створіть складний пароль для облікового запису, який зберігаєте на зовнішньому диску, та використовуйте менеджер паролів для його захисту. Опишіть послідовність дій.

Завдання № 77.

Зробіть резервне копіювання важливих файлів у хмарний сервіс та увімкніть 2FA для цього сервісу. Опишіть послідовність дій.

Завдання № 78.

Зробіть повне резервне копіювання системи, створіть складний пароль для вашого облікового запису та увімкніть 2FA для всіх важливих сервісів.

Завдання № 79.

Складіть список важливих даних, оцініть їх цінність та розробіть стратегію їх резервного копіювання. Опишіть послідовність дій.

Завдання № 80.

Підготуйте короткий виклад інформації про захист паролів та резервне копіювання. Поясніть другу або члену родини, чому важливо використовувати складні паролі та регулярно робити резервні копії даних.

Завдання № 81.

Створити пароль, що відповідає критеріям складності (великі та малі літери, цифри, символи). Кроки:

1. Виберіть випадкову послідовність символів.
2. Включіть принаймні одну велику літеру, одну малу літеру, одну цифру та один спеціальний символ (!@#$%^&).
3. Перевірте довжину пароля (не менше 12 символів).
4. Перевірте, чи легко його відтворити (не використовуйте особисту інформацію).
5. Запишіть пароль у безпечному місці (наприклад, у менеджері паролів).

Завдання № 82.

Включити двофакторну аутентифікацію (2FA) для облікового запису на популярній платформі (наприклад, Google, Facebook, email). Кроки:

1. Увійдіть в обліковий запис на платформі.
2. Перейдіть до розділу налаштувань безпеки.
3. Знайдіть опцію «Двофакторна аутентифікація» або «2FA».
4. Виберіть метод 2FA (наприклад, SMS, додаток аутентифікації, ключ безпеки).
5. Дотримуйтесь інструкцій для налаштування.

Завдання № 83.

Перевірити та встановити останню версію браузера (наприклад, Chrome, Firefox). Кроки:

1. Відкрийте браузер.
2. Перейдіть у меню (зазвичай, у верхньому правому кутку).
3. Виберіть «Довідка» або «Про браузер».
4. Перевірте, чи доступні оновлення.
5. Завантажте та встановіть останню версію.

Завдання № 84.

Встановити та налаштувати розширення для браузера, що блокує рекламу та відстеження (наприклад, AdBlock Plus, Privacy Badger). Кроки:

1. Перейдіть до магазину розширень для вашого браузера (Chrome Web Store, Firefox Add-ons).
2. Знайдіть потрібне розширення.
3. Натисніть кнопку «Додати до браузера».
4. Налаштуйте параметри розширення (за потреби).

Завдання № 85.

Переглянути та змінити налаштування конфіденційності в соціальній мережі (наприклад, Facebook, Instagram). Кроки:

1. Увійдіть в соціальну мережу.
2. Перейдіть до розділу «Налаштування» або «Профіль».
3. Виберіть «Конфіденційність».
4. Змініть налаштування, щоб обмежити доступ до вашої інформації (наприклад, приховати інформацію про місцезнаходження, друзів).

Завдання № 86.

Перевірити та проаналізувати, які права доступу має встановлений на пристрої додаток. Кроки:

1. На Android: Перейдіть до "Налаштування" -> "Додатки" -> Виберіть додаток -> "Дозвіл".
2. На iOS: Перейдіть до "Налаштування" -> Виберіть додаток -> "Конфіденційність".
3. Перевірте, чи не мають додатки надмірних прав доступу (наприклад, додаток для перекладу не повинен мати доступ до вашої камери).

Завдання № 87.

Підключитися до VPN-сервісу та перевірити: чи шифрується ваш інтернет-трафік. Кроки:

1. Виберіть VPN-сервіс.
2. Завантажте та встановіть додаток VPN.
3. Підключіться до VPN-сервера.
4. Перевірте свій IP-адресу (наприклад, за допомогою сайту whatismyip.com) перед та після підключення до VPN.

Завдання № 88.

Перевірити стан антивірусного програмного забезпечення та встановити найновішу версію. Кроки:

1. Відкрийте антивірусне програмне забезпечення.
2. Перевірте: чи немає загрози.
3. Перевірте: чи доступні оновлення.
4. Завантажте та встановіть останню версію.

Завдання № 89.

Перевірити: чи використовує вебсайт HTTPS (безпечне з’єднання). Кроки:
1. Перейдіть на вебсайт.
2. Перевірте адресний рядок браузера.
3. Переконайтеся, що URL починається з "https://".

Завдання № 90.

Уникати обміну конфіденційною інформацією при використанні публічного Wi-Fi. Кроки:
1. Увімкніть VPN.
2. Уникайте відправлення конфіденційної інформації.

Завдання № 91.

Забезпечити збереження важливих даних (фотографії, документи) на зовнішньому носії або у хмарному сховищі. Опишіть послідовність дій.

Завдання № 92.

Перевірити: чи не були скомпрометовані ваші облікові дані в результаті витоків інформації. Використовуйте сервіси такі, як: Have I Been Pwned (haveibeenpwned.com).

Завдання № 93.

Увімкнути отримання повідомлень про безпеку від операційної системи та програмного забезпечення. Опишіть послідовність дій.

Завдання № 94.

Відвідайте вебсайти сервісів та знайдіть розділ «Конфіденційність» або «Політика конфіденційності». Прочитати та зрозуміти політики конфіденційності популярних онлайн-сервісів.

Завдання № 95.

Використайте антивірусне програмне забезпечення для сканування пристрою на наявність шкідливого програмного забезпечення. Опишіть послідовність дій.

Завдання № 96.

Використовувати інструменти для блокування вебсайтів, що містять шкідливий контент (наприклад, рекламу, фішингові сайти). Опишіть послідовність дій.

Завдання № 97.

Перевірте налаштування безпеки у вашому обліковому записі. Увімкнути оповіщення про підозрілу активність (наприклад, спроби входу з невідомих пристроїв).

Завдання № 98.

Зареєструйтеся в менеджері паролів, створіть обліковий запис та імпортуйте паролі з інших сервісів.

Завдання № 99.

Регулярно перевіряйте налаштування безпеки на всіх пристроях та онлайн-сервісах. Опишіть послідовність дій.

Завдання № 100.

Читайте статті та блоги про кібербезпеку, відвідуйте онлайн-курси та семінари про нові загрози та методи захисту особистої інформації. На основі отриманої інформації підготуйте інструкцію для захисту приватної інформації.

Завдання № 101.

Складіть короткий план дій щодо захисту від вірусів. Опишіть 3-4 кроки, які необхідно виконати.

Завдання № 102.

Опишіть три можливі наслідки порушення конфіденційності персональних даних.

Завдання № 103.

Запропонуйте три правила брандмауера для захисту комп’ютера.

Завдання № 104.

Прочитайте приклад політики безпеки (надається викладачем) та визначте 2 ключові пункти, які, на вашу думку, є найважливішими.

Завдання № 105.

Опишіть: як шифрування може допомогти захистити інформацію.

Завдання № 106.

Опишіть ситуацію, коли відбулося порушення інформаційної безпеки. Проаналізуйте причини, наслідки та заходи, які необхідно вжити.

Завдання № 107.

Складіть план реагування на інцидент інформаційної безпеки. Включіть кроки на різних етапах.

Завдання № 108.

Оцініть: чи відповідає система обраної вами компанії вимогам стандарту інформаційної безпеки (ISO 27001).

Завдання № 109.

Розробіть політику управління доступом для інформаційної системи. Визначте принципи при наданні доступу.

Завдання № 110.

Розробіть стратегію резервного копіювання даних для інформаційної системи. Визначте, які дані необхідно резервно копіювати, як часто та де зберігати резервні копії.

Завдання № 111.

Наведіть два приклади електронних листів, які можуть бути фішинговими.

Завдання № 112.

Створіть сценарій фішингової електронної пошти. Опишіть послідовність дій.

Завдання № 113.

Опишіть: як можна виявити DDoS-атаку.

Завдання № 114.

Розробіть просту політику паролів для будь-якої обраної вами організації. Опишіть послідовність дій.

Завдання № 115.

Опишіть: як працює антивірусне програмне забезпечення для виявлення шкідливого коду та наведіть приклади популярних антивірусних програм.

Завдання № 116.

Розробіть базову політику захисту інформації для домашнього комп'ютера, включаючи використання антивірусу, брандмауера та шифрування.

Завдання № 117.

Порівняйте різні антивірусні програми, враховуючи їхні функції, вартість та репутацію.

Завдання № 118.

Проаналізуйте звіт антивірусу та визначте потенційні загрози.

Завдання № 119.

Розробіть сценарій тестування брандмауера для перевірки його ефективності.

Завдання № 120.

Поясніть: як працює процес шифрування та розшифрування даних.

Завдання № 121.

Створіть складний пароль для свого електронного поштового облікового запису, використовуючи мінімум 12 символів, включаючи великі та малі літери, цифри та спеціальні символи. Запишіть його у безпечному місці.

Завдання № 122.

Увімкніть двофакторну аутентифікацію (2FA) для одного з ваших облікових записів (наприклад, Google, Facebook, email).

Завдання № 123.

Перевірте налаштування конфіденційності у вашій улюбленій соціальній мережі та змініть їх відповідно до ваших побажань.

Завдання № 124.

Знайдіть вебсайт, який використовує HTTPS та переконайтеся, що URL починається з "https://".

Завдання № 125.

Використавши менеджер паролів, створіть та налаштуйте пароль для одного з ваших онлайн-сервісів.

Завдання № 126.

Пошукайте інформацію про поточні витоки даних та перевірте, чи не була ваша особиста інформація скомпрометована (наприклад, використовуйте сайт Have I Been Pwned).

ТЕСТОВІ ЗАВДАННЯ

1. Що таке інформаційна безпека?

а) захист комп'ютерів від вірусів;

б) комплекс заходів для захисту інформації від несанкціонованого доступу та використання;

в) використання антивірусного програмного забезпечення;

г) навчання персоналу основам комп'ютерної грамотності.

2. Які три ключові принципи інформаційної безпеки?

а) шифрування, резервне копіювання, брандмауер;

б) конфіденційність, цілісність, доступність;

в) аутентифікація, авторизація, аутентичність;

г) моніторинг безпеки, реагування на інциденти, відновлення після інцидентів.

3. Що означає термін «вразливість» в контексті інформаційної безпеки?

а) сильний пароль;

б) слабке місце в системі, яке може бути використане зловмисником;

в) захист від вірусів;

г) резервне копіювання даних.

4. Назвіть два приклади інформаційних активів:

а) програма для редагування зображень та фінансова звітність компанії;

б) відеоіграшки та фотографії;

в) книги та журнали;

г) спеціалізоване обладнання та програмне забезпечення.

5. Що таке ризик в інформаційній безпеці?

а) потенційна можливість втрати інформації;

б) негативний вплив на інформаційну систему або інформаційний актив;
в) використання зловмисником вразливості;
г) наявність слабких місць у системі.

6. Що таке вірус і як він поширюється?
а) програма, яка автоматично копіює себе на інші комп'ютери;
б) програма, яка прикріплюється до легітимних файлів та активується при їх використанні;
в) програма, яка блокує доступ до інтернету;
г) програма, яка автоматично видаляє файли з комп'ютера.

7. Яка різниця між вірусом та шкідливим ПЗ (Malware)?
а) вірус завжди більш небезпечний за шкідливе ПЗ;
б) шкідливе ПЗ – це загальний термін, що включає віруси, трояни, черв'яки та інше;
в) віруси не можуть поширюватися самі по собі;
г) шкідливе ПЗ використовується тільки для розваг.

8. Що таке фішинг та як він працює?
а) це атака, яка використовує віруси;
б) це метод шахрайства, коли зловмисники видають себе за легітимні організації для отримання конфіденційної інформації;
в) це атака, яка використовує DDoS-атаки;
г) це метод шифрування даних.

9. Що таке DDoS-атака та як вона впливає на роботу вебсайту?
а) це атака, яка використовує віруси для пошкодження вебсайту;
б) це атака, яка перевантажує вебсайт великою кількістю запитів, виводячи його з ладу;
в) це атака, яка змінює контент вебсайту;
г) це атака, яка видаляє вебсайт з інтернету.

10. Чому важливо регулярно оновлювати програмне забезпечення?
а) це робить комп'ютер швидшим;
б) це усуває вразливості, які можуть бути використані зловмисниками;
в) це робить комп'ютер більш красивим;
г) це збільшує кількість програм, які можна встановити.

11. Що таке брандмауер та для чого він використовується?

а) це програмне забезпечення для видалення вірусів;

б) це система, яка блокує несанкціонований доступ до комп'ютера;

в) це інструмент для перевірки цілісності файлів;

г) це програма для перегляду вебсайтів.

12. Чому важливо використовувати складні паролі? (Оберіть усі відповідні варіанти)

а) вони легше запам'ятовуються;

б) вони роблять ваш обліковий запис більш вразливим до атак;

в) вони ускладнюють зламування вашого облікового запису;

г) вони дозволяють використовувати один і той самий пароль для всіх сервісів.

13. Який найкращий спосіб захистити ваш обліковий запис у соціальній мережі?

а) використовувати простий пароль, який легко запам'ятати;

б) увімкнути двофакторну аутентифікацію;

в) ділитися паролем з друзями та родиною;

г) не змінювати пароль, якщо він вже працює.

14. Які дії слід вжити, якщо ви підозрюєте, що ваш комп'ютер заражений шкідливим програмним забезпеченням? (Оберіть усі відповідні варіанти)

а) продовжувати користуватися комп'ютером, оскільки це не серйозна проблема;

б) встановити антивірусне програмне забезпечення;

в) завантажити безкоштовні програми з ненадійних джерел;

г) запустити повне сканування системи антивірусом.

15. Що таке шифрування?

а) процес видалення файлів із комп'ютера;

б) перетворення інформації на нечитабельний формат для захисту від несанкціонованого доступу;

в) збільшення швидкості роботи комп'ютера;

г) копіювання файлів на інший пристрій.

16. Який тип шкідливого ПЗ використовує шифрування даних для вимагання викупу?

а) троян;

б) черв'як;

в) вірус-вимагач (Ransomware);
г) троян-розвідник.

17. Що таке аутентифікація?
а) захист від вірусів;
б) підтвердження особи користувача;
в) резервне копіювання даних;
г) оновлення програмного забезпечення.

18. Який з наступних варіантів є прикладом соціальної інженерії?
а) встановлення антивірусного програмного забезпечення;
б) використання складного паролю;
в) фішинг, коли зловмисник видає себе за працівника банку;
г) регулярне створення резервних копій даних.

19. Що таке логін та пароль?
а) це назва програмного забезпечення для обробки тексту;
б) це дані, які використовуються для ідентифікації користувача та доступу до системи або облікового запису;
в) це тип обладнання комп'ютера;
г) це процес встановлення оновлень операційної системи.

20. Що таке двофакторна аутентифікація?
а) використання одного пароля для всіх облікових записів;
б) додатковий рівень безпеки, який вимагає надання двох різних факторів під час входу в систему (наприклад, пароль та код з SMS);
в) автоматичне оновлення паролю щодня;
г) використання складного паролю для підвищення безпеки.

21. Який тип захисту використовується брандмауером?
а) шифрування даних на диску;
б) моніторинг мережевого трафіку та блокування несанкціонованого доступу;
в) антивірусне сканування файлів;
г) резервне копіювання даних.

22. Які заходи можна вжити для захисту від фішингу? (Оберіть усі відповідні варіанти)
а) Не відкривайте підозрілі електронні листи та посилання;

б) Надавайте особисті дані у відповідь на запит через електронний лист;
в) Перевіряйте URL-адреси веб-сайтів перед введенням особистої інформації;
г) Будьте обережні з несподіваними пропозиціями та заохоченнями.

23. Що таке черв'як?
а) шкідливе програмне забезпечення, яке прикріплюється до легітимних файлів;
б) шкідливе програмне забезпечення, яке самостійно поширюється на інші комп'ютери в мережі;
в) програма для захисту від вірусів;
г) інструмент для створення резервних копій даних.

24. Що таке троян?
а) вірус, який пошкоджує файли на комп'ютері;
б) шкідливе програмне забезпечення, яке маскується під легітимну програму для отримання доступу до системи;
в) програма для шифрування даних;
г) інструмент для відновлення даних після збою.

25. Яка роль резервного копіювання у забезпеченні інформаційної безпеки?
а) запобігання зараженню комп'ютера вірусами;
б) відновлення даних у разі їх втрати або пошкодження;
в) захист від DDoS-атак;
г) збільшення швидкості роботи комп'ютера.

26. Що таке цілісність інформації?
а) конфіденційність даних;
б) забезпечення точності та повноти інформації, а також захист від несанкціонованих змін;
в) доступність даних для авторизованих користувачів;
г) шифрування даних.

27. Яке значення має моніторинг безпеки?
а) відсутнє, оскільки достатньо встановити антивірусне програмне забезпечення;
б) постійний контроль за системами та мережами для виявлення та реагування на потенційні загрози;
в) регулярна зміна паролів;
г) автоматичне оновлення програмного забезпечення.

28. Як часто слід виконувати резервне копіювання даних?

а) лише раз на рік;

б) кожен день;

в) залежить від важливості даних та частоти їх зміни, але бажано регулярно (наприклад, щодня або щотижня);

г) лише у випадку збою системи.

29. Який тип інформації потребує особливого захисту відповідно до законодавства?

а) публічно доступна інформація;

б) особисті дані (ПІБ, адреса, номер телефону тощо);

в) неважливі файли та документи;

г) зображення тварин.

30. Що таке безпечний пароль? (Оберіть усі відповідні варіанти)

а) містить не менше 12 символів;

б) складається з великих та малих літер, чисел та спеціальних символів;

в) легко вгадується на основі особистої інформації;

г) не використовується для різних облікових записів.

31. Що таке інцидент безпеки?

а) планова перевірка системи безпеки;

б) будь-яка подія, яка може поставити під загрозу конфіденційність, цілісність або доступність інформаційної системи;

в) регулярне оновлення програмного забезпечення;

г) проведення навчання з питань інформаційної безпеки.

32. Яка роль політики безпеки?

а) встановлює правила та процедури для захисту інформаційних активів організації;

б) не має жодного значення для інформаційної безпеки;

в) обмежує доступ до інтернету для працівників;

г) визначає рівень швидкості роботи комп’ютера.

33. Що таке DDoS-атака?

а) атака на електронну пошту;

б) перевантаження вебсайту великою кількістю запитів із різних джерел, що робить його недоступним для легітимних користувачів;

в) видалення файлів з комп’ютера;
г) встановлення вірусу на комп’ютер.

34. Яке програмне забезпечення використовується для виявлення та видалення шкідливого ПЗ?
а) операційна система;
б) антивірусне програмне забезпечення;
в) графічний редактор;
г) програма для перегляду вебсайтів.

35. Що таке конфіденційність?
а) забезпечення доступності інформації для всіх користувачів;
б) захист інформації від несанкціонованого доступу та розголошення;
в) підтвердження особистості користувача;
г) усунення вразливостей у системі.

36. Як часто потрібно перевіряти наявність оновлень безпеки для програм?
а) лише коли з’являється повідомлення про оновлення;
б) регулярно, бажано щодня або щотижня;
в) лише у випадку виникнення інциденту безпеки;
г) не потрібно перевіряти наявність оновлень.

37. Який з наступних варіантів є прикладом слабкого пароля?
а) «P@$$wOrd123»;
б) «MyPetName»;
в) «12345678»;
г) «SecurePassword!»

38. Що таке перевірка цілісності файлів?
а) процес шифрування даних;
б) переконання, що файли не були змінені або пошкоджені з моменту останньої перевірки;
в) регулярне резервне копіювання файлів;
г) оновлення операційної системи.

39. Який тип інформації слід шифрувати?
а) вся інформація, яка містить персональні дані;
б) лише інформація, що зберігається на зовнішніх носіях;

в) тільки паролі до облікових записів;
г) не потрібно шифрувати жодну інформацію.

40. Що таке безпечний браузер?
а) браузер з найшвидшою швидкістю перегляду вебсторінок;
б) браузер, який має вбудовані функції безпеки для захисту від шкідливих сайтів та погроз;
в) браузер із широкими можливостями кастомізації;
г) браузер з найбільшою кількістю розширень.

ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Опишіть три способи поширення вірусів.
2. Які заходи можна вжити для захисту від фішингових атак?
3. Опишіть три способи створення резервної копії важливих даних.
4. Як двофакторна аутентифікація допомагає захистити обліковий запис?
5. Які заходи можна вжити для захисту мобільних пристроїв?
6. Що таке антивірусне програмне забезпечення та які основні функції воно виконує?
7. Чому важливо регулярно оновлювати базу даних антивірусу?
8. Що таке хуманінг в антивірусах і чому це важливо?
9. Що таке брандмауер та яка його основна роль у захисті інформації?
10. Які типи брандмауерів існують? Опишіть відмінності між ними.
11. Як налаштувати Windows Firewall для блокування невідомого трафіку?
12. Що таке логи брандмауера та для чого їх використовують?
13. Як брандмауер відрізняється від антивірусу?
14. Що таке шифрування та як воно працює?
15. Поясніть різницю між симетричним та асиметричним шифруванням.
16. Наведіть приклади використання шифрування (наприклад, шифрування файлів, електронної пошти).
17. Що таке ключ розшифрування та чому він важливий?
18. Як зашифрувати файл за допомогою VeraCrypt? Опишіть основні кроки.
19. Як налаштувати політики безпеки для користувачів (наприклад, правила використання паролів)?
20. Опишіть архітектуру безпеки комп’ютера, включаючи антивірус, брандмауер, шифрування та інші компоненти.
21. Які заходи необхідно вжити для захисту мобільного пристрою?

22. Що робити, якщо на комп’ютері виявлено підозрілу активність? (Опишіть етапи розслідування).
23. Які критерії повинні відповідати складним паролем? Наведіть не менше трьох.
24. Що таке двофакторна аутентифікація (2FA) та навіщо вона потрібна?
25. Які ризики існують, якщо використовувати один і той самий пароль для кількох облікових записів?
26. Як можна перевірити, чи працює процес резервного копіювання?
27. Як часто рекомендується виконувати резервне копіювання даних?
28. Що таке повне резервне копіювання системи?
29. Які основні правила безпечної роботи з паролями ви знаєте? Наведіть не менше трьох.
30. Чому важливо регулярно виконувати резервне копіювання даних?
31. Опишіть, як ви будете захищати свою інформацію в разі збою вашого комп’ютера.
32. Які дії ви вживатимете, якщо отримаєте повідомлення про витік даних із вашого облікового запису?
33. Чому використання менеджера паролів є рекомендованою практикою?
34. Як можна захистити обліковий запис від злому, якщо ви використовуєте один і той самий пароль для всіх сервісів?
35. Що означає HTTPS?
36. Які переваги використання VPN?
37. Як можна захистити свій телефон від несанкціонованого доступу?
38. Який спосіб найкраще захистити вашу особисту інформацію при використанні публічного Wi-Fi?
39. Чому важливо регулярно оновлювати операційну систему на вашому пристрої?
40. Що таке «розм’якшення» (credential stuffing) та як його можна уникнути?
41. Які права доступу слід надати додатку, щоб мінімізувати ризики для вашої приватності?
42. Чому важливо налаштовувати налаштування конфіденційності в соціальних мережах?
43. Які ризики існують, якщо ви ділитеся надмірною особистою інформацією в соціальних мережах?
44. Що таке фішинг та як його розпізнати?
45. Які заходи можна вжити, щоб захистити свою особисту інформацію в онлайн-повідомленнях?

46. Як можна перевірити, чи не була ваша особиста інформація скомпрометована в результаті витоку даних?
47. Які правила слід дотримуватися при заповненні онлайн-форм з особистою інформацією?

ТЕМА 3. ОБРОБЛЕННЯ ЗОБРАЖЕНЬ ЗАСОБАМИ КОМП'ЮТЕРНОЇ ГРАФІКИ

Мета: навчитися використовувати основні функції та інструменти програмного забезпечення для оброблення зображень, освоїти техніки редагування та маніпулювання зображеннями, вивчити принципи створення графічних елементів та композицій, отримати практичний досвід роботи з цифровими зображеннями, вміти передавати просторову та формальну структуру об'єктів за допомогою графічних інструментів.

ТЕОРЕТИЧНІ РЕКОМЕНДАЦІЇ ДО ТЕМИ 3

3.1. Основи комп'ютерної графіки

Підрозділ закладає фундамент для розуміння цифрових зображень та їх представлення в комп'ютерній графіці. Він охоплює ключові поняття, такі як пікселі, розрішення та колірні моделі, що є необхідними для подальшого вивчення оброблення зображень.

Піксель (Pixels) – це найменший окремий елемент цифрового зображення, який має певне значення кольору та яскравість. Уявіть собі зображення як сітку маленьких квадратиків – кожен із цих квадратиків і є пікселем.

Кожен піксель зберігає інформацію про свій колір. Ця інформація може бути представлена різними способами, залежно від використовуваної колірної моделі. Зазвичай, для кожного пікселя визначаються значення для червоного (Red), зеленого (Green) та синього (Blue) каналів (RGB).

Кожен піксель має унікальні координати на зображенні. Зазвичай використовуються декартові координати (x, y), де (0, 0) – це верхній лівий кут зображення. Наприклад: у чорно-білому зображенні кожному пікселю присвоюється значення «чорний» або «білий». У кольоровому зображенні кожен піксель має три значення – для червоного, зеленого та синього каналів, що визначають його колір.

Роздільна здатність (Resolution) – роздільна здатність цифрового зображення визначає кількість пікселів по горизонталі та вертикалі. Воно

виражається у вигляді пари чисел, наприклад, 1920x1080 (1920 пікселів по ширині та 1080 пікселів по висоті).

Більша роздільна здатність означає більше пікселів і, отже, більш деталізоване зображення.

PIXEL DENSITY (PPI/DPI): Важливо враховувати щільність пікселів на дюйм (pixels per inch – PPI) або dots per inch (dots per inch – DPI). Це показує: як багато пікселів розміщено в одному дюймі. Високий PPI/DPI забезпечує чітке та деталізоване зображення при друці або відображенні на дисплеї. Наприклад, зображення 640x480 має менше пікселів, ніж зображення 1920x1080, тому зображення 1920x1080 буде більш чітким і деталізованим (при однаковому розмірі на екрані).

Колірна модель (Color Model) – визначає: як колір представляється в цифровому вигляді та описує простір кольорів, який містить всі можливі комбінації кольорів.

Найбільш поширені ***колірні моделі***:

RGB (Red, Green, Blue): Аддитивна модель кольору, яку використовують для відображення зображень на екранах. Колір створюють шляхом додавання різних кількостей червоного, зеленого та синього світла. Кожен колір представлений трьома значеннями (від 0 до 255) для кожного кольорового каналу. Наприклад, (255, 0, 0) – це чистий червоний колір.

Використання: екрани комп'ютерів, смартфонів, телевізорів.

CMYK (Cyan, Magenta, Yellow, Key/Black): Віднімальна модель кольору, яка використовується для друку. Колір створюється шляхом віднімання різних кількостей синього, пурпурного, жовтого та чорного пігменту з білого світла. Кожен колір представлений трьома значеннями (від 0% до 100%) для кожного каналу: блакитного, пурпурного, жовтого та чорного.

Використання: друк книг, журналів, рекламних матеріалів.

HSV (Hue, Saturation, Value): модель кольору, яка описує колір за допомогою відтінку (Hue), насиченості (Saturation) та яскравості (Value).

Значення:

Відтінок (Hue): кут на колірному колесі, який визначає «колір» (червоний, зелений, синій і т.д.) та вимірюється в градусах (0-360).

Насиченість (Saturation): інтенсивність або чистота кольору, де спостерігаємо позначки: від 0% до 100%. 0% – це сірий колір, 100% – найбільш насичений колір.

Яскравість (Value): ясність кольору, де спостерігаємо позначки: від 0% до 100%. 0% – чорний колір, 100% – найяскравіший колір.

Використання: редагування кольорів, створення візуальних ефектів.

Вибір правильної колірної моделі є критично важливим для отримання бажаного результату. Наприклад, якщо ви редагуєте зображення для друку, вам слід використовувати CMYK, а не RGB. Інакше кольори можуть виглядати по-різному при друці.

Розуміння пікселів, розрішення та колірних моделей є основою для будь-якої роботи з цифровими зображеннями. Знання цих понять дозволить вам ефективно обробляти та модифікувати зображення за допомогою комп'ютерної графіки.

3.2. Використання програми GIMP

Підрозділ присвячений практичному вивченню **програми GIMP (GNU Image Manipulation Program)** – безкоштовного та потужного редактора зображень. Ми розглянемо інтерфейс програми та основні інструменти, які необхідні для базового оброблення зображень.

Інтерфейс GIMP може здатися трохи складним на перший погляд, але він досить гнучкий і дозволяє користувачеві налаштувати його під свої потреби.

Основні елементи інтерфейсу:

Головне меню (File, Edit, Image, Layer, Select, Filter, View, Help): містить основні команди та функції програми.

Панель інструментів (Toolbox): розташована зліва або зверху екрана, містить інструменти для редагування зображень (вибір, малювання, обрізка тощо). Її можна налаштувати під свої потреби.

Панелі властивостей: розташовані справа, відображають параметри обраного інструменту або шару (прошарку).

Панелі шарів (Layers): розташована праворуч, дозволяє керувати шарами зображення. Шари – це прозорі листи паперу, які можна переміщувати, змінювати та маскувати незалежно один від одного (ключова концепція для складних редагувань).

Вікно зображення (Canvas): основне вікно, де відображається зображення.

Панель кольорів (Color Picker): дозволяє вибирати колір із різних джерел (з вибраного пікселя на зображенні, за допомогою палітри або введення коду кольору (RGB, Hex)).

Основні інструменти GIMP:

Інструмент вибору (Select Tool): дозволяє вибирати певні області зображення для редагування.

Інструмент заповнення (Bucket Fill Tool): заповнює обрану область одним кольором.

Інструмент пензля (Paintbrush Tool): дозволяє малювати на зображенні, використовуючи різні розміри, форми та властивості пензля.

Інструмент гумки (Eraser Tool): видаляє пікселі з зображення.

Інструмент градієнту (Gradient Tool): створює градієнти між двома або більше кольорами.

Інструмент тексту (Text Tool): дозволяє додавати текст на зображення.

Інструмент лінійок (Rectangle Tool): малює прямі лінії та прямокутники.

Інструмент кривих (Curve Tool): редагує криві Безьє, які використовуються для створення плавних переходів і контурів.

Інструмент обертання (Rotate Tool): обертає зображення на певний кут.

Інструмент масштабування (Scale Tool): змінює розмір зображення.

Існують різні *типи вибору*:

Прямокутний вибір (Rectangle Select): вибирає прямокутні області.

Еліпсний вибір (Ellipse Select): вибирає еліптичні області.

Вибір за кольором (Select by Color): вибирає пікселі одного кольору.

Вибір за контуром (Fuzzy Select/Magic Wand): вибирає області з подібними колірними значеннями, які мають певний рівень схожості.

Робота з шарами: робота з шарами є ключовою для складних редагувань у GIMP:

Створення нового шару: `Layer > New Layer`.

Видалення шару: клацніть правою кнопкою миші на шарі у панелі шарів і виберіть "Delete Layer".

Переміщення шару: перетягніть шар у панелі шарів.

Зміна порядку шарів: перетягніть шари в потрібному порядку, наприклад: шари зверху перекривають шари знизу.

Прозорість шару (Opacity): регулює прозорість шару за допомогою слайдера на панелі шарів.

Режими змішування (Blend Modes): змінюють спосіб взаємодії шару з шарами, що знаходяться під ним (наприклад, Multiply, Screen, Overlay). Їх можна вибрати в розкривному меню режиму змішування на панелі шарів.

Маски шарів (Layer Masks): дозволяють приховати або зробити видимими частини шару без його видалення.

Базові операції:

Зміна розміру зображення: `Image > Scale Image`.

Обрізка зображення: `Image > Crop Image`.

Регулювання яскравості та контрасту: `Colors > Brightness-Contrast`.

Корекція кольору (Hue-Saturation): `Colors > Hue-Saturation`.

Практичні поради:

1. Використовуйте шари для складних редагувань. Це дозволяє вам змінювати частини зображення без впливу на інші частини.
2. Експериментуйте з режимами змішування та масками шарів, щоб досягти цікавих ефектів.
3. Не бійтеся використовувати різні інструменти GIMP. З часом ви навчитеся їх ефективно використовувати.
4. Переглядайте онлайн-уроки та туторіали для поглибленого вивчення програми.

Ресурси:

Офіційний сайт GIMP: https://www.gimp.org/
Туторіали на YouTube (пошук "GIMP tutorial"): https://www.youtube.com/results?search_query=gimp+tutorial

Для більш глибокого вивчення програми рекомендується практикуватися та використовувати онлайн-ресурси.

3.3. Редагування зображень

Підрозділ детальніше розглядає основні операції редагування зображень у GIMP, включаючи обрізку, масштабування, зміну кольору та застосування фільтрів. Розглянемо практичне застосування цих функцій для покращання та модифікації зображень.

Обрізка (Cropping) – видалення небажаних частин зображення, фокусування на важливих елементах або зміна співвідношення сторін.

Інструмент: `Tools > Crop Image` (або натисніть Ctrl+I).

Процес:

1. Виберіть інструмент обрізки.
2. Намалюйте прямокутник навколо області, яку потрібно зберегти.
3. Натисніть Enter або клацніть лівою кнопкою миші в центрі прямокутника для застосування обрізки.

***Параметри*:**

Ratio: визначає співвідношення сторін обрізаної області (наприклад, 1:1 для квадратного зображення).

Crop area: дозволяє вказати конкретні координати початку та кінця обрізки.

Масштабування (Resizing) – зміна розміру зображення. Може бути необхідною для адаптації зображення до різних форматів або роздільної здатності.

Інструмент: `Image > Scale Image` (або натисніть Ctrl+T).

Процес:

1. Виберіть інструмент масштабування.
2. Намалюйте прямокутник навколо області, яку потрібно масштабувати.
3. Перетягніть кутовий маркер, щоб змінити розмір зображення.
4. Уведіть бажане значення ширини та висоти у відповідних полях.
5. Натисніть Enter.

Важливі параметри:

Scale: відсоток зміни розміру (наприклад, 100% – без змін).

Width/Height: введення конкретних значень ширини та висоти.

Aspect Ratio: збереження початкового співвідношення сторін під час масштабування. Важливо для уникнення спотворення зображення.

Зміна Кольору (Color Adjustment) – регулювання яскравості, контрасту, насиченості та інших параметрів кольорів зображення для покращання візуального вигляду.

Інструменти: `Colors > Brightness-Contrast`, `Colors > Hue-Saturation`, `Colors > Color Balance`.

Brightness-Contrast: регулює загальну яскравість та контрастність зображення.

Hue-Saturation: дозволяє змінювати відтінок, насиченість та яскравість кольорів. Особливо корисний для корекції кольору.

Color Balance: регулює баланс червоного, зеленого та синього каналів для досягнення бажаного кольорового тону.

Панель "Colorize": дозволяє перетворити чорно-біле зображення на кольорову версію за допомогою вибору одного або кількох кольорів.

Фільтри (Filters) – застосування різноманітних ефектів до зображення для створення візуальних ефектів, покращання якості або зміни стилю.

Інструменти: `Filters` в головному меню. Включає широкий спектр фільтрів: розмиття, різкість, шум, стилізація тощо.

Приклади популярних фільтрів:

Gaussian Blur: розмиває зображення для зменшення деталей або створення ефекту глибини.

Sharpen: збільшує різкість зображення.

Noise: додає шум до зображення для створення текстури або ефекту старого фільму.

Posterize: Зменшує кількість кольорів у зображенні, створюючи ефект постеру.

Find Edges: виділяє краї об’єктів на зображенні.

Практичні поради для роботи з фільтрами:

1. Експериментуйте з різними фільтрами та їх параметрами, щоб знайти оптимальний результат.

2. Використовуйте не надмірну кількість фільтрів, оскільки це може погіршити якість зображення.

3. Застосовуйте фільтри на окремих шарах для більшої гнучкості редагування.

Обрізка, масштабування, зміна кольору та застосування фільтрів є важливими інструментами для обробки зображень в GIMP. Використання цих функцій дозволяє покращити якість зображення, внести творчі зміни та адаптувати його до різних потреб. Рекомендується експериментувати з різними параметрами та комбінаціями інструментів для досягнення бажаного результату.

3.4. Створення простих зображень

Підрозділ присвячений створенню простих графічних елементів у GIMP за допомогою інструментів заливки, тексту та форм. Він допоможе вам навчитися створювати базові візуальні компоненти для ваших проєктів.

Заливка (Fill) – заповнення обраної області одним кольором або градієнтом.

Інструменти:

Bucket Fill Tool (заливка): заповнює область одним кольором, натискаючи лівою кнопкою миші.

Gradient Tool (градієнт): заповнює область градієнтом між двома або більше кольорами.

Процес:

1. Виберіть інструмент заливки.

2. Встановіть колір заповнення в панелі властивостей (зазвичай, це кнопка з кольором).

3. Клацніть лівою кнопкою миші всередині області, яку потрібно заповнити.

4. Для градієнтів: виберіть два або більше кольорів та перетягніть курсор по зображенню для створення градієнту.

Параметри:

Tolerance (допуск): визначає, наскільки близько до вибраного кольору можуть бути інші пікселі, щоб вони також були заповнені.

Текст (Text) – додавання текстових елементів до зображення.

Інструмент: `Text Tool (Текст)`.

Процес:

1. Виберіть інструмент тексту.

2. Клацніть на зображенні, щоб визначити точку початку введення тексту.

3. Введіть текст у текстовому вікні, що з’явиться.

4. Використовуйте панель властивостей для зміни шрифту, розміру, кольору та інших параметрів тексту.

Параметри:

Font (шрифт): вибір шрифту з доступного списку.

Size (розмір): встановлення розміру шрифту.

Color (колір): вибір кольору тексту.

Alignment (вирівнювання): визначення вирівнювання тексту (ліворуч, в центрі, праворуч).

Text Effects (ефекти тексту): дозволяють додавати тіні, обводку та інші ефекти до тексту.

Форми (Shapes) – створення простих геометричних фігур для використання в зображеннях.

Інструменти:

Rectangle Tool (прямокутник): для створення прямокутників та квадратів.

Ellipse Tool (еліпс): для створення еліпсів та кіл.

Polygon Tool (полігон): для створення багатокутників із заданою кількістю сторін.

Line Tool (лінія): для малювання прямих ліній.

Free Select Tool (вільний вибір) / Lasso Tool: дозволяє малювати довільні форми.

Процес:

1. Виберіть інструмент форми.

2. Клацніть і перетягніть мишею на зображенні, щоб створити форму потрібного розміру. Утримуйте Shift під час перетягування для створення фігур з постійними пропорціями (наприклад, квадратів та кіл).

3. Використовуйте панель властивостей для зміни кольору, обводки та інших параметрів форми.

Параметри:

Fill Color (колір заливки): колір, яким заповнюється форма.

Stroke Color (колір обводки): колір лінії, що обводить форму.

Stroke Width (товщина обводки): товщина лінії обводки.

Практичні поради:

1. Використовуйте шари для відокремлення різних елементів створення зображення (текст на одному шарі, форми на іншому).

2. Експериментуйте з різними шрифтами, кольорами та розмірами для тексту.

3. Використовуйте градієнти для створення більш цікавих і динамічних ефектів заливки.

4. Поєднуйте різні форми та текст для створення складніших композицій.

3.5. Редагування та покращання фотографії

У цьому підрозділі ви використаєте знання, отримані в попередніх підрозділах для редагування та покращання реальної фотографії за допомогою GIMP.

Інструкція для роботи з фотографіями

Кроки виконання:

1. Відкрийте обрану фотографію в GIMP (`File > Open`).

2. Ретельно огляньте фотографію, визначте сильні та слабкі сторони. Які елементи потребують корекції? Що можна покращити?

3. Виконайте базові корекції:

Корекція яскравості та контрасту: Застосуйте `Colors > Brightness-Contrast`, щоб скоригувати загальну яскравість і контрастність зображення. Спробуйте трохи збільшити контраст, якщо зображення здається блідим, або зменшити, якщо воно занадто темне.

Корекція кольору: Використовуйте `Colors > Color Balance` для корекції балансу білого та досягнення більш природних кольорів. Можливо, знадобиться трохи скоригувати рівні червоного, зеленого та синього каналів.

Корекція насиченості: За допомогою `Colors > Hue-Saturation` відрегулюйте насиченість кольорів, щоб зробити їх більш яскравими або приглушеними. Будьте обережні – надмірна насиченість може виглядати нереально.

4. Обрізка та масштабування:

Якщо на зображенні є небажані частини, обріжте його за допомогою `Image > Crop Image`.

Якщо потрібно змінити розмір фотографії, використовуйте `Image > Scale Image`. Зверніть увагу на збереження пропорцій.

5. Якщо зображення має шум (зернистість), застосуйте фільтр `Filters > Noise > Reduce Noise`, щоб зменшити його.

6. Різкість та розмиття:

Застосуйте фільтр `Filters > Sharpen > Unsharp Mask` для підвищення різкості зображення (обережно, надмірна різкість може створити артефакти).

Якщо потрібно згладити деякі області або створити ефект розмиття фону, використовуйте `Filters > Blur`.

7. Додаткові ефекти (за бажанням): Ви можете експериментувати з іншими фільтрами та ефектами для створення цікавих візуальних ефектів. Наприклад, додавання тіней або обводки до певних елементів зображення.

8. Збереження: Збережіть відредаговане зображення у форматі JPEG (`File > Export As...`). Виберіть високу якість для кращого результату.

Додаткові поради:

1. Не бійтеся експериментувати з різними параметрами та інструментами.

2. Зробіть резервну копію оригінального зображення перед початком редагування.

3. Застосовуйте корекції поступово, а не одразу всі.

ПРАКТИЧНІ ЗАВДАННЯ

Завдання № 1.

Завантажити різні формати зображень (JPG, PNG, GIF, TIFF) і зберегти їх у потрібних форматах. Описати послідовність дій.

Завдання № 2.

Змінити розмір зображення (пікселі, дюйми), розрізнення (DPI). Поясніть вплив цих параметрів на якість зображення. Описати послідовність дій.

Завдання № 3.

Перетворити зображення за різними кольоровими моделями (RGB, CMYK, Grayscale). Описати послідовність дій.

Завдання № 4.

Створити зображення в рівноті сірого з кольорового. Описати послідовність дій.

Завдання № 5.

Збільшити або зменшити яскравість і контрастність зображення. Описати послідовність дій.

Завдання № 6.

Виправити баланс білого на зображенні, щоб воно виглядало природніше. Описати послідовність дій.

Завдання № 7.

Змінити насиченість кольорів у зображенні. Описати послідовність дій.

Завдання № 8.

Розділити зображення на окремі кольорові канали (червоний, зелений, синій). Описати послідовність дій.

Завдання № 9.

Створити та редагувати маски для вибору певних ділянок зображення. Описати послідовність дій.

Завдання № 10.

Ознайомитися з основними інструментами вибору (прямокутник, овал, lasso, magic wand). Описати процес роботи з ними.

Завдання № 11.

Копіювати та вставляти частини зображення. Описати послідовність дій.

Завдання № 12.

Видалити фон із зображення за допомогою інструментів вибору та масок. Описати послідовність дій.

Завдання № 13.

Злити кілька прошарків на зображенні в один. Описати послідовність дій.

Завдання № 14.

Розділити один прошарок на зображенні на декілька. Описати послідовність дій.

Завдання № 15.

Регулювати прозорість прошарків зображення.

Завдання № 16.

Експериментувати з режимами змішування шарів (Multiply, Screen, Overlay). Описати послідовність дій.

Завдання № 17.

Використовувати шари-канали для створення складних ефектів на зображеннях. Описати послідовність дій.

Завдання № 18.

Відстежувати історію змін і відкочувати їх назад за потреби. Описати послідовність дій.

Завдання № 19.

Додавати нові прошарки для редагування зображення без зміни оригінального. Описати послідовність дій.

Завдання № 20.

Змінювати порядок прошарків у масиві зображень. Описати послідовність дій.

Завдання № 21.

Видалити дрібні дефекти з використанням інструменту «Точкового відновлення». Описати послідовність дій.

Завдання № 22.

Використовувати інструменти ретуші для покращання текстури шкіри на фотографії. Описати послідовність дій.

Завдання № 23.

Зменшити шум і згладити зображення за допомогою фільтрів. Описати послідовність дій.

Завдання № 24.

Видалити плями, подряпини та інші недоліки на поверхні об’єкта зображення. Описати послідовність дій.

Завдання № 25.

Виправити перспективи зображення (наприклад, фотографії архітектури). Описати послідовність дій.

Завдання № 26.

Змінити колір певного об’єкта на зображенні. Описати послідовність дій.

Завдання № 27.

Перефарбувати волосся на фотографії. Описати послідовність дій.

Завдання № 28.

Використовувати інструменти для відновлення пошкоджених або старіючих фотографій. Описати послідовність дій.

Завдання № 29.

Використовуйте фільтри для зменшення розмиття зображень. Описати послідовність дій.

Завдання № 30.

Збільшити різкість зображення за допомогою інструментів «Sharpen» або «Unsharp Mask». Описати послідовність дій.

Завдання № 31.

Видалити невеликі предмети з фотографії (наприклад, людей або сміття). Описати послідовність дій.

Завдання № 32.

Використовуйте функцію заповнення на основі вмісту для видалення великих об’єктів. Описати послідовність дій.

Завдання № 33.

Застосувати фільтри або ефекти для створення портретного стилю зображення. Описати послідовність дій.

Завдання № 34.

Використовуйте інструменти для відновлення втрачених кольорів у старіших знімках. Описати послідовність дій.

Завдання № 35.

Усуньте розводку на склі або інших поверхнях, що відбивають світло. Описати послідовність дій.

Завдання № 36.

Використовуйте інструменти для зменшення цифрового шуму у фотографіях, зроблених при низькій освітленості. Описати послідовність дій.

Завдання № 37.

Покращити динамічний діапазон зображення, коригуючи тіні та світлі. Описати послідовність дій.

Завдання № 38.

Використовуйте інструменти для виправлення геометричних спотворень, спричинених використанням об’єктивів із великим зумом. Опишіть послідовність дій.

Завдання № 39.

Використати автоматичні інструменти корекції зображення. Описати послідовність дій.

Завдання № 40.

Створити ефект «розмиття руху», щоб підкреслити динаміку в кадрі. Описати послідовність дій.

Завдання № 41.

Створити ефект розмиття зображення (Gaussian Blur, Motion Blur). Описати послідовність дій.

Завдання № 42.

Створіть простий логотип, використовуючи текст, форму (наприклад, коло) та градієнт для заповнення.

Завдання № 43.

Застосувати ефекти різкості для підкреслення деталей малюнка. Описати послідовність дій.

Завдання № 44.

Застосувати теплові фільтри для створення певного настрою у зображенні. Описати послідовність дій.

Завдання № 45.

Застосуйте фільтр «Попіл» для надання зображенню вінтажного вигляду. Опишіть послідовність дій.

Завдання № 46.

Перетворити кольорову фотографію в чорно-білу з різними ефектами. Описати послідовність дій.

Завдання № 47.

Створити ефект, де зображення плавно переходить у розмитість. Описати послідовність дій.

Завдання № 48.

Застосувати текстурні фільтри для надання зображенню нової візуальної якості (наприклад, дерево, метал).

Завдання № 49.

Використовувати інструмент «Пензель» із різними налаштуваннями для створення ефектів малюнка. Описати послідовність дій.

Завдання № 50.

Вставити одне зображення в інше та змінити його розмір, положення і прозорість. Описати послідовність дій.

Завдання № 51.

Додавати світлові промені для створення драматичного ефекту. Описати послідовність дій.

Завдання № 52.

Створити ефект розбитого скла на зображенні. Описати послідовність дій.

Завдання № 53.

Додавати ефект води до зображення (хвилі, бризки). Описати послідовність дій.

Завдання № 54.

Створити ефект туману або диму на зображенні. Описати послідовність дій.

Завдання № 55.

Застосувати ефект для створення незвичайного неба з різними кольорами. Описати послідовність дій.

Завдання № 56.

Використати інструменти деформації для зміни форми об’єктів на зображенні (наприклад, "Twirl", "Wave"). Описати послідовність дій.

Завдання № 57.

Створити ефект повітряного світіння навколо об’єктів. Описати послідовність дій.

Завдання № 58.

Застосувати різні фільтри і регулювання кольорів для створення вінтажного стилю зображення. Описати послідовність дій.

Завдання № 59.

Використати художні шари для додавання текстури та візуального інтересу до зображення. Описати послідовність дій.

Завдання № 60.

Підсилити або зменшити різниці між кольорами на зображенні. Описати послідовність дій.

Завдання № 61.

Зібрати кілька зображень в один колаж. Описати послідовність дій.

Завдання № 62.

Додати текст до зображення з різними шрифтами, розмірами і кольорами. Описати послідовність дій.

Завдання № 63.

Створити простий логотип за допомогою графічних інструментів. Описати послідовність дій.

Завдання № 64.

Розмістити об’єкти на зображенні з урахуванням композиції. Описати послідовність дій.

Завдання № 65.

Використати шаблони для створення банерів, листівок та інших графічних матеріалів. Описати послідовність дій.

Завдання № 66.

Створити зображення для різних платформ соціальних мереж (Facebook, Instagram, Twitter). Описати послідовність дій.

Завдання № 67.

Розробити дизайн обкладинки для книги або альбому. Описати послідовність дій.

Завдання № 68.

Намалювати просту ілюстрацію за допомогою графічних інструментів. Описати послідовність дій.

Завдання № 69.

Створити зображення, використовуючи векторну графіку (наприклад, фігури, лінії). Описати послідовність дій.

Завдання № 70.

Застосувати різні типи градієнтів для створення плавного переходу між кольорами. Описати послідовність дій.

Завдання № 71.

Додати тіні та блиск до об’єктів на зображенні для створення 3D-ефекту. Описати послідовність дій.

Завдання № 72.

Обвести об’єкти на зображенні лінією іншого кольору. Описати послідовність дій.

Завдання № 73.

Створити складні форми зображень за допомогою масок та фільтрів. Описати послідовність дій.

Завдання № 74.

Розмити фон зображення, щоб виділити об’єкт на передньому плані. Описати послідовність дій.

Завдання № 75.

Додати світловий ореол навколо об’єкта для підкреслення його важливості. Описати послідовність дій.

Завдання № 76.

Застосувати перспективні трансформації для створення ілюзії глибини. Описати послідовність дій.

Завдання № 77.

Створити динамічний вигляд, імітуючи рух об’єктів на зображенні. Описати послідовність дій.

Завдання № 78.

Надати векторним фігурам візуальної глибини за допомогою текстур. Описати послідовність дій.

Завдання № 79.

Створити ілюзії світла, яке проєктуються на поверхню об’єкта. Описати послідовність дій.

Завдання № 80.

Розмістити кілька зображень так, щоб вони гармонійно поєднувалися між собою. Описати послідовність дій.

Завдання № 81.

Використовуйте інструменти для створення маски, заснованої на певному кольорі в зображенні. Опишіть послідовність дій.

Завдання № 82.

Відкрити та редагувати RAW файл фотографії. Описати послідовність дій.

Завдання № 83.

Витягти палітру кольорів із зображення. Описати послідовність дій.

Завдання № 84.

Створити анімовану GIF-ілюстрацію. Описати послідовність дій.

Завдання № 85.

Редагувати 3D моделі (якщо можливо): змінити колір, текстуру або форму 3D моделі. Описати послідовність дій.

Завдання № 86.

Застосувати спеціальні алгоритми для підвищення різкості застарілих зображень. Описати послідовність дій.

Завдання № 87.

Використовуйте інструменти для відновлення деталей у розмитому зображенні. Описати послідовність дій.

Завдання № 88.

Створити візуальний ефект світлової кулі на зображенні. Описати послідовність дій.

Завдання № 89.

Накласти текстуру на тривимірний об’єкт, щоб зробити його більш реалістичним. Описати послідовність дій.

Завдання № 90.

Додати ефект вогню до зображення. Описати послідовність дій.

Завдання № 91.

Додати ефект снігу до зображення. Описати послідовність дій.

Завдання № 92.

Редагувати портрети з різним освітленням. Використовувати інструменти для корекції освітлення на портретах. Описати послідовність дій.

Завдання № 93.

Створити ілюстрації у стилі аніме: використовуйте графічні інструменти для створення зображень у стилі аніме. Описати послідовність дій.

Завдання № 94.

Редагувати зображення для друку, налаштовуючи параметри зображення (роздільна здатність, формат).

Завдання № 95.

Додати світловий відблиск на об’єкти, що відображають світло на зображенні. Описати послідовність дій.

Завдання № 96.

Створіть візуальний ефект зупинки руху в динамічному зображенні. Опишіть послідовність дій.

Завдання № 97.

Призначте розмиття тільки в одному напрямку, щоб створити відчуття руху. Опишіть послідовність дій.

Завдання № 98.

Редагуйте фотографії з низькою освітленістю. Використовуйте інструменти для зменшення шуму та покращання деталей у темних фотографіях. Опишіть послідовність дій.

Завдання № 99.

Застосуйте градієнтне розмиття до текстур, щоб створити більш м’який перехід між кольорами на зображеннях. Опишіть послідовність дій.

Завдання № 100.

Використовуйте інструменти для зміни форми обличчя на фотографії (наприклад, збільшення очей або зменшення носа). Опишіть послідовність дій.

Завдання № 101.

Створити 3D текстури з використанням програмного забезпечення комп’ютерної графіки. Описати послідовність дій.

Завдання № 102.

Додайте реалістичні властивості (відбиття, розсіювання) до об’єктів у сцені зображення. Опишіть послідовність дій.

Завдання № 103.

Підготувати зображення для використання в додатках віртуальної реальності. Опишіть послідовність дій.

Завдання № 104.

Використовуйте алгоритми машинного навчання для автоматичного покращання якості фотографій. Опишіть послідовність дій.

Завдання № 105.

Додати ефект кінокамери до зображення (наприклад, експозицію, баланс білого). Описати послідовність дій.

Завдання № 106.

Зменшення динамічного діапазону та видалення артефактів із високонаповнених (HDR) зображень. Описати послідовність дій.

Завдання № 107.

Створіть ілюзію збільшення кількості кадрів (HFR) у секунду для створення більш плавного руху. Опишіть послідовність дій.

Завдання № 108.

Вивчити та використати скрипти та плагіни для автоматизації завдань оброблення зображень. Описати послідовність дій.

Завдання № 109.

Створити складний візуальний ефект (VFX), наприклад, вибух або потік води. Описати послідовність дій.

Завдання № 110.

Комбінуйте графіку та анімацію для створення динамічних зображень. Опишіть послідовність дій.

Завдання № 111.

Використовуйте кольорові палітри та шаблони, характерні для поп-арту. Опишіть послідовність дій.

Завдання № 112.

Створіть імітацію хромованого металу на об’єктах у зображенні. Опишіть послідовність дій.

Завдання № 113.

Використовуйте спеціальні фільтри та ефекти для створення вінтажного вигляду фотографіям. Опишіть послідовність дій.

Завдання № 114.

Вивчіть алгоритми стилізації. Застосуйте алгоритми штучного інтелекту для зміни стилю фотографій (наприклад, перетворення в малюнки Ван Гога). Опишіть послідовність дій.

Завдання № 115.

Використовуйте рівняння та математичні функції для створення складного розмиття руху зображення. Опишіть послідовність дій.

Завдання № 116.

Додайте об’єкти 3D в реалістичні сцени, щоб покращити візуальну привабливість зображень. Опишіть послідовність дій.

Завдання № 117.

Зробіть текст або інші об’єкти на зображенні прозорими, щоб вони інтегрувалися з фоном. Опишіть послідовність дій.

Завдання № 118.

Використовуйте інструменти штучного інтелекту для автоматичного створення колажів із заданих фотографій. Опишіть послідовність дій.

Завдання № 119.

Використовуйте моделі машинного навчання (за допомогою нейронних мереж) для покращання якості та стилізації зображень. Опишіть послідовність дій.

Завдання № 120.

Створіть більш точне розмиття фону за допомогою масок, що дозволяють зберегти чіткість об’єктів на передньому плані зображення. Опишіть послідовність дій.

Завдання № 121.

Напишіть короткий код (на будь-якій мові програмування) для обертання зображення на певний кут.

ТЕСТИ

1. Що є основним процесом в обробленні зображень?

а) зміна розміру зображення;

б) математичне перетворення пікселів для досягнення бажаного ефекту;

в) додавання текстури до зображення;

г) розділення зображення на окремі елементи.

2. Який тип кодування зазвичай використовується для зберігання чорно-білих зображень?

а) RGB;

б) CMYK;

в) HSV;

г) Бінарне (1-бітове).

3. Що таке піксель?

а) алгоритм обробки зображення;

б) файл зображення в форматі JPEG;

в) найменший елемент зображення, який має колір;

г) програма для редагування зображень.

4. Який із наведених методів використовується для збільшення контрастності зображення?

а) Згладжування (Blurring);

б) Розмиття (Smearing);

в) Еквалізація гістограми;

г) Додавання шуму.

5. Що таке фільтр розмиття?

а) фільтр, який збільшує різкість зображення;

б) фільтр, який змінює кольори зображення;

в) фільтр, який зменшує різкість та деталізацію зображення;

г) фільтр, який виділяє контури об’єктів на зображенні.

6. Який із наступних методів використовується для підвищення різкості зображення?

а) згладжування;

б) розмиття;

в) підсилення країв;

г) еквалізація гістограми.

7. Що таке шуми в зображенні?

а) природний ефект, що покращує візуальне сприйняття;

б) навмисне додавання кольорів до зображення;

в) випадкові зміни у значеннях пікселів;

г) алгоритм стиснення зображень.

8. Який тип шуму найчастіше зустрічається в цифрових зображеннях?

а) гаусівський шум;

б) білий шум;

в) мозаїчний шум;

г) кольоровий шум.

9. Що таке гістограма зображення?

а) графік, що показує розподіл кольорів на зображенні;

б) алгоритм обробки пікселів;

в) графік, який відображає кількість пікселів кожного значення інтенсивності;

г) програма для редагування зображень.

10. Що таке кольорове коліно?

а) ефект розмиття кольорів на краях об’єктів;

б) перетворення одного кольору в інший за допомогою фільтрів;

в) змішування кольорів при переході від одного до іншого, що призводить до появи небажаних відтінків;

г) процес стиснення зображень у форматі jpeg.

11. Який колірний простір використовується для роботи з кольорами на моніторах?

а) CMYK;

б) Бінарний;

в) RGB;

г) HSV.

12. Що таке CMYK?

а) колірний простір, що використовується для друку;

б) алгоритм стиснення зображень;

в) модель кольорів, що використовується в друкарській справі;

г) тип фільтру для оброблення зображень.

13. Що таке HSV?

а) колірний простір, який базується на математичних розрахунках;

б) алгоритм стиснення зображень;

в) модель кольорів, що описує колір за допомогою відтінків, насиченості та яскравості;

г) тип фільтру для оброблення зображень.

14. Що таке морфологічні операції в обробленні зображень?

а) операції, що змінюють колір пікселів;

б) операції з розмиттям та підвищенням різкості;

в) операції, що змінюють форму об’єктів на зображенні;

г) алгоритми стиснення зображень.

15. Які морфологічні операції є основними?

а) збільшення та зменшення масштабу зображення;

б) фільтрація шуму та підвищення різкості;

в) ерозія, дилатація, відкриття, закриття;

г) корекція кольору та контрастності.

16. Що таке ерозія в морфології зображень?

а) операція, що розширює об’єкти на зображенні;

б) операція, що змінює колір пікселів;

в) операція, що зменшує розміри об’єктів на зображенні;

г) алгоритм стиснення зображень.

17. Що таке дилатація в морфології зображень?

а) операція, що зменшує розміри об’єктів на зображенні;

б) операція, що змінює колір пікселів;

в) операція, що розширює об’єкти на зображенні;

г) алгоритм стиснення зображень.

18. Для чого використовується операція відкриття?

а) для збільшення розміру об’єктів на зображенні;

б) для зменшення розміру об’єктів на зображенні;

в) для видалення невеликих об’єктів та шуму з зображення;

г) для виділення контурів об’єктів.

19. Для чого використовується операція закриття?

а) для видалення шумів і невеликих дірок в об’єктах;

б) для збільшення різкості зображення;

в) для заповнення невеликих дірок та розривів у об’єктах;

г) для зміни кольору пікселів.

20. Що таке контур зображення?

а) внутрішня частина об’єкта на зображенні;

б) зовнішній вигляд об’єкта на зображенні;

в) межа між об’єктом та фоном;

г) колір об’єкта на зображенні.

21. Який алгоритм використовується для виявлення контурів зображення?

а) гаусівський фільтр;

б) фільтр розмиття;

в) алгоритм Кенни;

г) фільтр еквалізації гістограми.

22. Що таке сегментація зображення?

а) процес стиснення зображення;

б) процес розмиття зображення;

в) розділення зображення на кілька регіонів або об’єктів;

г) процес підвищення різкості зображення.

23. Який метод сегментації використовує порогове значення інтенсивності пікселів?

а) кластеризація K-means;

б) метод градієнтів;

в) порогова сегментація;

г) метод виявлення країв.

24. Що таке фільтр Гауса в обробленні зображень?

а) фільтр, який підвищує контрастність зображення;

б) фільтр, який змінює кольори зображення;

в) фільтр для розмиття зображення;

г) фільтр для виділення контурів об’єктів.

25. Яка функція фільтра Гауса?

а) збільшення різкості зображення;

б) виявлення шумів в зображенні;

в) зменшення шуму та розмиття зображення;

г) підвищення контрастності зображення.

26. Що таке згладжування зображення?

а) Процес збільшення різкості зображення;

б) Процес виділення контурів об’єктів;

в) Процес зменшення шуму та розмиття зображення;

г) Процес зміни кольорів зображення.

27. Який із методів використовується для стиснення зображень без втрати якості?

а) JPEG;

б) GIF;

в) PNG;

г) BMP.

28. що таке стиснення без втрат?

а) стиснення, що призводить до втрати даних;

б) стиснення, яке використовує тільки один колір;

в) стиснення, при якому дані відновлюються повністю;

г) стиснення, яке змінює розмір зображення.

29. Що таке стиснення з втратами?

а) Стиснення, що не дозволяє відновити оригінальне зображення;

б) Стиснення, що використовує тільки один колір;

в) Стиснення, при якому частина даних видаляється для зменшення розміру файлу;

г) Стиснення, яке збільшує розмір зображення.

30. Який формат файлу зазвичай використовується для зберігання векторної графіки?

а) JPEG;

б) PNG;

в) GIF;

г) SVG.

31. Що таке векторна графіка?

а) графіка, що складається з пікселів;

б) графіка, яка зберігає колір кожного пікселя;

в) графіка, що описується математичними рівняннями;

г) графіка, яка використовується для створення фотографій.

32. Який формат файлу зазвичай використовується для зберігання растрової графіки?

а) SVG;

б) EPS;

в) JPEG;

г) PDF.

33. Що таке пікселізація зображення?

а) збільшення різкості зображення;

б) зменшення розміру зображення;

в) виявлення окремих пікселів на зображенні;

г) видалення шуму з зображення.

34. Яка операція використовується для зміни масштабу зображення?

а) фільтр розмиття;

б) морфологічні операції;

в) збільшення або зменшення розмірів;

г) корекція кольору.

35. Що таке зсув зображення?

а) обертання зображення навколо точки;

б) масштабування зображення;

в) переміщення зображення на певну відстань;

г) зміна кольору пікселів.

36. Що таке обертання зображення?

а) зміна розміру зображення;

б) переміщення зображення;

в) поворот зображення навколо точки;

г) додавання ефектів.

37. Що таке масштабування зображення?

а) переміщення об’єктів на зображенні;

б) зміна кольору пікселів;

в) збільшення або зменшення розміру зображення;

г) видалення шуму з зображення.

38. Що таке прозорість у графіці?

а) колір, який використовується для заповнення об’єктів;

б) ефект розмиття зображення;

в) можливість бачити через певні області зображення;

г) формат файлу зображення.

39. Що таке альфа-канал?

а) канал, що відповідає за колір об’єкта;

б) канал, що використовується для створення ефектів розмиття;

в) канал, що визначає рівень прозорості об’єкта;

г) канал, що використовується для стиснення зображення.

40. Що таке композиція зображень?

а) стиснення зображень;

б) розмиття зображень;

в) збільшення різкості зображень;

г) об’єднання кількох зображень в одне.

ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Що таке цифрове зображення?
2. Які основні характеристики цифрового зображення?
3. Опишіть процес цифрового захоплення зображення.
4. Що таке піксель? Який його вплив на якість зображення?
5. Які формати файлів зображень ви знаєте? Назвіть їх переваги та недоліки. (JPEG, PNG, GIF, TIFF, RAW).
6. Що таке бітова глибина зображення? Як вона впливає на колірну палітру та якість зображення?
7. Які типи кодування кольору ви знаєте? Опишіть RGB, CMYK, HSV (HSL).
8. Що таке колірний простір? Для чого він потрібен?
9. Поясніть різницю між растровими та векторними зображеннями.
10. Які переваги та недоліки растрових зображень?
11. Які переваги та недоліки векторних зображень?
12. Що таке масштабування зображення? Які проблеми можуть виникнути при масштабуванні растрового зображення?
13. Опишіть процес фільтрації зображень.
14. Які типи фільтрів ви знаєте? (розмиття, різкість, еліптичний розмиття тощо)
15. Що таке контур зображення? Як його можна виділити?
16. Опишіть процес сегментації зображень. Для чого вона використовується?
17. Які методи сегментації зображень ви знаєте? (порогова сегментація, кластерний аналіз).
18. Що таке еластична деформація зображення? За яких випадків її застосовують?
19. Опишіть процес стиснення зображень. Які типи стиснення ви знаєте? (З втратами та без втрат)
20. Який алгоритм стиснення зображень JPEG використовує?
21. Що таке артефакти стиснення? Як їх можна уникнути?
22. Поясніть поняття «шум» у цифровому зображенні.
23. Які методи шумозаглушення ви знаєте? (Гаусовий фільтр, медіанний фільтр)
24. Що таке еквівалентна інформація (ЕЕ)? Як вона використовується при стисненні зображень?
25. Опишіть процес обертання та масштабування зображення.
26. Які алгоритми використовуються для виявлення країв на зображенні?
27. Що таке морфологічні операції в обробленні зображень? Наведіть приклади (розширення, звуження, вирізання).
28. Поясніть роль математики у обробленні зображень (лінійна алгебра, диференціальне числення).

29. Що таке піксельний зміст? Як він використовується для розпізнавання об’єктів?
30. Опишіть процес виділення об’єктів на зображенні за допомогою контурів.
31. Які застосування має оброблення зображень у медицині?
32. Які застосування має оброблення зображень у системі відеоспостереження?
33. Що таке комп’ютерний зір? В яких задачах він використовується?
34. Опишіть основні етапи розпізнавання об’єктів на зображенні.
35. Які сучасні тенденції в області обробки зображень? (Глибоке навчання, штучний інтелект)
36. Які інструменти для оброблення зображень ви знаєте? Назвіть їх основні можливості (Photoshop, GIMP, OpenCV, ImageMagick).
37. Напишіть алгоритм на псевдокоді для розмиття зображення гаусовим фільтром.
38. Як можна змінити колірне представлення зображення з RGB на HSV?
39. Поясніть, як за допомогою програмного забезпечення можна виділити об’єкт на зображенні за його кольором.
40. Опишіть процес створення палітри кольорів для зображення.
41. Як можна збільшити роздільну здатність зображення без втрати якості? Які обмеження існують у цьому процесі?
42. Які методи стиснення зображень ви можете використовувати для зменшення розміру файлу, зберігаючи при цьому прийнятну якість зображення?
43. Як можна видалити шум з цифрового зображення за допомогою медіанного фільтра?
44. Як можна автоматично визначити контури на зображенні за допомогою алгоритмів морфології?
45. Як ви можете використовувати програмне забезпечення для корекції освітлення та контрастності зображення?
46. Опишіть процес створення пастельних ефектів на зображенні.
47. Які методи можна використовувати для підвищення різкості зображення?
48. Як ви можете створити маску для частини зображення?
49. Як можна застосувати алгоритми комп’ютерного зору для визначення кількості об’єктів на зображенні?
50. Як можна використовувати машинне навчання для класифікації зображень? (Наприклад, розпізнавання котів та собак)
51. Які проблеми можуть виникнути при автоматичному виділенні об’єктів на зображенні?
52. Опишіть процес створення візуальних ефектів у відеороликах за допомогою комп’ютерної графіки.

53. Як можна створити 3D-модель з 2D-зображення? (Наприклад, за допомогою фотограметрії).
54. Як ви можете використовувати програмне забезпечення для створення анімацій на основі зображень?
55. Опишіть процес створення віртуальної реальності (VR) або доповненої реальності (AR).
56. Як можна створити інтерактивне зображення, яке реагує на дії користувача?
57. Які методи використовуються для створення фотореалістичних зображень?
58. Опишіть процес 3D-рендерингу та його роль у комп'ютерній графіці.
59. Як можна використовувати програмне забезпечення для редагування відео з додаванням візуальних ефектів?

ТЕМА 4. КОМП'ЮТЕРНІ ПУБЛІКАЦІЇ

Мета: освоїти основи роботи з комп'ютерними публікаціями, вивчити типи та формати файлів документів; навчитися створювати, редагувати та форматувати текстові документи; орієнтуватися у різних режимах роботи програмного забезпечення для створення комп'ютерних публікацій, використовувати графічний дизайн та елементи верстки при оформленні документів; навчитися вставляти таблиці, зображення, посилання та інші об'єкти у текстові документи.

ТЕОРЕТИЧНІ РЕКОМЕНДАЦІЇ ДО ТЕМИ 4

4.1. Основи верстки

Комп'ютерні публікації – це широкий спектр матеріалів, створених та поширених за допомогою комп'ютерів. Вони охоплюють різноманітні формати, від текстових документів до мультимедійного контенту, і відіграють ключову роль у сучасній інформаційній епосі.

Верстка – це процес організації та розташування текстового та графічного контенту на сторінці для створення візуально привабливих і зручних для читання матеріалів. Вона є ключовою складовою будь-якого цифрового публікації, від веб-сайтів до документів.

1. Основні принципи верстки:

Ієрархія інформації: Важливіші елементи повинні бути більш помітними (більший розмір шрифту, контрастний колір), а менш важливі – менш виділеними. Це допомагає читачеві швидко орієнтуватися в контенті.

Візуальний баланс: Розподіл елементів на сторінці повинен бути збалансованим, щоб не створювати відчуття перевантаження або порожнечі. Це досягається за допомогою симетрії та асиметрії.

Контраст: Використання різних кольорів, розмірів шрифтів і стилів для виділення важливих елементів і створення візуального інтересу.

Простота: Не перевантажуйте сторінку зайвими елементами. Чіткий та лаконічний дизайн робить контент більш зрозумілим.

Читабельність: Вибір відповідного шрифту, розміру шрифту та інтервалу між рядками для забезпечення комфортного читання.

2. Основні компоненти верстки:

Текст: основний елемент публікації.

Шрифт (Font): Стиль тексту (наприклад, Arial, Times New Roman). Вибір шрифту впливає на загальний вигляд та читабельність.

Розмір шрифту (Font Size): Розмір символів. Визначає візуальну вагу тексту.

Тип шрифту (Font Weight): Товщина ліній символів (наприклад, нормальний, жирний, курсив).

Інтервал між рядками (Line Height/Leading): Відстань між рядками тексту. Впливає на читабельність та візуальну структуру.

Інтервал між символами (Letter Spacing): Відстань між окремими літерами. Може використовуватися для створення певного ефекту.

Зображення: візуальний контент, який доповнює текст.

Розмір зображення: визначає візуальну вагу та вплив на загальний вигляд сторінки.

Формат зображення (JPEG, PNG, GIF): впливає на якість та розмір файлу.

Альтернативний текст (Alt Text): опис зображення для людей із вадами зору та для пошукових систем.

Елементи структури:

Заголовки (Headings): Використовуються для поділу тексту на розділи і підрозділи. Важливі для ієрархії інформації.

Параграфи (Paragraphs): групи речень, що виражають одну тему.

Списки (Lists): Використовуються для переліку елементів. Можуть бути нумерованими або з маркерами.

Таблиці (Tables): для організації даних у рядки та стовпці.

3. Відступи:

Відступи – це простір навколо тексту, який допомагає структурувати інформацію і зробити її більш читабельною. Існують різні типи відступів:

Лівий відступ (Left Indent): відступ з лівого краю сторінки.

Правий відступ (Right Indent): відступ з правого краю сторінки.

Початковий відступ (First Line Indent): відступ тільки для першого рядка в параграфі.

Квадратний відступ (Hanging Indent): відступ для всіх рядків, крім першого, який починається з лівого краю сторінки.

4. Берег:

Береги – це простір навколо вмісту на сторінці, який залишається незаповненим. Вони визначають межі публікації.

Верхнє поле (Top Margin): відстань від верхнього краю сторінки до вмісту.

Нижнє поле (Bottom Margin): відстань від нижнього краю сторінки до вмісту.

Ліве поле (Left Margin): відстань від лівого краю сторінки до вмісту.

Праве поле (Right Margin): відстань від правого краю сторінки до вмісту.

5. Інструменти верстки:

Редактори текстів (Microsoft Word, Google Docs, LibreOffice Writer): мають вбудовані інструменти для керування відступами, полями та форматуванням тексту.

Системи управління контентом (CMS) (WordPress, Joomla, Drupal): забезпечують більш гнучкі можливості верстки за допомогою шаблонів і тем.

HTML/CSS: для створення вебсторінок. CSS дозволяє точно контролювати зовнішній вигляд та розташування елементів на сторінці.

Розуміння цих основних принципів допоможе вам створювати професійно оформлені публікації, які будуть привабливими для читачів і ефективно доносити інформацію. Експериментуйте з різними параметрами верстки, щоб знайти оптимальний варіант для вашого контенту.

4.2 Використання редактора LaTeX для створення наукових публікацій

LaTeX – це потужна мова розмітки та система компонування документів, яка широко використовується в науковій спільноті для створення високоякісних публікацій: наукових статей, книг, дисертацій, презентацій тощо. Він забезпечує чудовий контроль над форматуванням, автоматично керує нумерацією та цитуваннями, а також створює професійно виглядні документи.

Переваги програми:

Відмінна типографіка: LaTeX відомий своєю високою якістю друку. Він забезпечує ідеальне вирівнювання тексту, чітке представлення математичних формул та професійний зовнішній вигляд документів.

Автоматизоване керування цитуваннями: LaTeX інтегрується з різними системами управління бібліографією (BibTeX, BibLaTeX), що значно спрощує процес цитування джерел у тексті та списку літератури.

Математичні формули: LaTeX – найкращий вибір для представлення складних математичних формул. Він забезпечує чітке та професійне відображення математичного контенту.

Структура документа: LaTeX підтримує чітку структуру документів із розділами, підрозділами, таблицями, зображеннями тощо.

Портативність: документи LaTeX можна легко переносити між різними операційними системами та комп'ютерами.

Контроль версій: легко інтегрується з системами контролю версій (Git) для відстеження змін у документі.

Популярні редактори LaTeX:

TeXstudio: Один із найпопулярніших і простих у використанні редакторів LaTeX. Має вбудований автодоповнення, підсвічування синтаксису та інтеграцію з компілятором LaTeX (Windows, macOS, Linux).

TeXmaker: Ще один чудовий редактор LaTeX з широким набором функцій та підтримкою різних компіляторів LaTeX (Windows, macOS, Linux).

Overleaf: Онлайн-редактор LaTeX. Не потребує встановлення програмного забезпечення. Чудовий варіант для спільної роботи над документами (веббраузер).

VS Code з розширенням LaTeX Workshop: Популярний редактор коду, який можна налаштувати для роботи з LaTeX за допомогою розширення LaTeX Workshop (Windows, macOS, Linux).

TeXworks: Простий і легкий у використанні редактор LaTeX, підходить для початківців (Windows, macOS, Linux).

Основний процес створення документа LaTeX:

1. ***Написання тексту та математичних формул***: Ви пишете текст за допомогою спеціальних команд LaTeX. Математичні формули записуються у так званому «режимі математики».

2. ***Визначення структури документа***: Ви використовуєте команди для визначення розділів, підрозділів, списків тощо.

3. ***Цитування джерел***: Ви використовуєте команди `\cite` та інтегруєтесь з BibTeX/BibLaTeX для керування бібліографією.

4. ***Компіляція документа***: Ви запускаєте компілятор LaTeX (наприклад, pdfLaTeX) для перетворення файлу `.tex` у PDF-документ. Компіляція може потребувати декількох проходів для правильного формування списку літератури та інших елементів.

Основи синтаксису LaTeX:

Команди: Починаються з символу `\`. Наприклад, `\section{Вступ}` створює розділ з назвою "Вступ".

Режими: LaTeX має різні режими: режим тексту, режим математики, режим заголовка тощо.

Окремі елементи: Використовуються для форматування тексту (наприклад, `\textbf{жирний шрифт}`, `\textit{курсив}`).

Приклад простого документа LaTeX:

```latex
\documentclass{article} % Тип документа: стаття
\title{Моя наукова публікація} % Заголовок статті
\author{Ваше Ім’я} % Автор статті
\date{\today} % Дата публікації
\begin{document} % Початок вмісту документа
\maketitle % Створення заголовку з інформацією про автора та дату
\section{Вступ} % Розділ «Вступ»
Це короткий опис вступу до статті.
\subsection{Підрозділ Вступу} % Підрозділ «Підрозділ Вступу»
Детальніший опис вступу.
\section{Методологія} % Розділ «Методологія»
Опис використаної методології дослідження.
\bibliographystyle{plain} % Вибір стилю бібліографії
\bibliography{references} % Вказує на файл з бібліографією (references.bib)
\end{document}
```

Щоб запустити цей приклад:

1. Збережіть код у файл `my_article.tex`.
2. Створіть файл `references.bib` із вашими цитуваннями у форматі BibTeX. (Приклад: `\cite{author2023}`)
3. Використовуйте редактор LaTeX (наприклад, TeXstudio) для компіляції файлу `my_article.tex`.

Ресурси для вивчення LaTeX:

Overleaf Learn: https://www.overleaf.com/learn
LaTeX Wikibook: https://en.wikibooks.org/wiki/LaTeX
CTAN (Comprehensive TeX Archive Network): https://ctan.org/ - Центральний репозиторій для всіх матеріалів LaTeX.

Вивчення LaTeX потребує часу та зусиль, але це інвестиція, яка окупиться у вигляді професійно оформлених наукових публікацій та значного полегшення процесу написання документів.

4.3 Підготовка рукопису до набору в журнал: покрокова Інструкція

Підготовка рукопису до надсилання в науковий журнал – це критично важливий етап, який значною мірою впливає на шанси публікації. Дотримання вимог журналу та чітке оформлення рукопису демонструє професіоналізм та повагу до редакторів і читачів.

Ось детальна *інструкція з підготовки рукопису*:

1. Вибір журналу:

Спеціалізація: переконайтеся, що журнал відповідає тематиці вашої роботи.

Імпакт-фактор (Impact Factor): Вказує на частоту цитування публікацій у журналі. Більш високий імпакт-фактор зазвичай асоціюється з більш престижним журналом.

Вимоги до рукописів: Уважно прочитайте «Інструкції для авторів» журналу, перш ніж починати написання. Зверніть увагу на вимоги щодо формату, обсягу, стилю цитування тощо.

2. Структура рукопису:

Назва: коротка, чітка та інформативна назва, яка відображає основний зміст роботи.

Анотація (Abstract): короткий огляд роботи (зазвичай 150-300 слів). Вона повинна містити мету дослідження, методи, результати та висновки.

Ключові слова (Keywords): список ключових слів, які допоможуть іншим дослідникам знайти вашу роботу в пошукових системах.

Вступ (Introduction): Представлення теми дослідження, огляд попередніх робіт та обґрунтування актуальності вашої роботи. Чітко сформулюйте мету та завдання дослідження.

Матеріали та методи (Materials and Methods): детальний опис матеріалів, використаних у дослідженні, та методів, які були застосовані. Забезпечте достатню інформацію для можливості повторення вашого дослідження іншими дослідниками.

Результати (Results): представлення результатів дослідження в чіткій та об’єктивній формі. Використовуйте таблиці, графіки та інші візуалізації для кращого представлення даних.

Обговорення (Discussion): інтерпретація отриманих результатів, порівняння з попередніми дослідженнями та обговорення їх значущості. Обмеження вашого дослідження також мають бути зазначені тут.

Висновок (Conclusion): короткий підсумок основних висновків роботи та перспективи подальших досліджень.

Подяки (Acknowledgments) (Необов'язково): висловлення подяки людям або організаціям, які допомогли у проведенні дослідження.

Список літератури (References): перелік усіх джерел, використаних у рукописі. Форматування списку літератури повинно відповідати вимогам журналу.

Додатки (Appendices) (Необов'язково): додаткова інформація, яка не є необхідною для розуміння основної частини роботи (наприклад, детальні розрахунки, додаткові таблиці).

3. Форматування рукопису:

Шрифт: зазвичай Times New Roman, Arial або інші стандартні шрифти розміром 12 пунктів.

Інтервал між рядками: переважно 1.5 або подвійний інтервал.

Поля: Перевірте вимоги журналу щодо розміру полів (зазвичай 2.5 см з усіх боків).

Нумерація сторінок: додайте нумерацію сторінок, починаючи з першої сторінки анотації.

Стиль цитування: використовуйте стиль цитування, який вимагає журнал (наприклад, APA, MLA, Chicago). Переконайтеся, що всі джерела правильно цитуються в тексті та у списку літератури.

4. Перевірка рукопису:

Граматика та орфографія: Ретельно перевірте рукопис на граматичні помилки, орфографію та пунктуацію. Використовуйте онлайн-перевірки або попросіть когось іншого прочитати ваш рукопис.

Стиль написання: Переконайтеся, що стиль написання чіткий, лаконічний та професійний. Уникайте жаргону та надмірного використання складної термінології.

Логічність та послідовність: Перевірте, чи логічно організована ваша робота та чи є послідовність у представленні аргументів.

Відповідність вимогам журналу: Переконайтеся, що ваш рукопис повністю відповідає вимогам журналу щодо формату, обсягу та стилю цитування.

5. Підготовка додаткових матеріалів (якщо потрібно):

Фігури та Таблиці: Переконайтеся, що фігури та таблиці мають чіткі заголовки та підписи. Вони повинні бути легко зрозумілими без довідки до тексту.

Згода на публікацію (Copyright Form): можливо, вам потрібно буде заповнити форму згоди на публікацію, щоб передати права на вашу роботу журналу.

6. Надсилання рукопису:

Онлайн-система надсилання: більшість журналів використовують онлайн-системи для подання рукописів.

Супровідний лист (Cover Letter): напишіть супровідний лист, в якому представте вашу роботу та поясніть її актуальність для журналу.

Корисні Інструменти:

Grammarly: онлайн-перевірка граматики та стилю.
Microsoft Word/LaTeX Editors: для форматування рукопису.
Citation Management Software (Zotero, Mendeley): для управління цитуваннями.

Дотримуючись цих кроків, ви зможете підготувати якісний та професійно оформлений рукопис, який збільшить ваші шанси на публікацію у науковому журналі.

ПРАКТИЧНІ ЗАВДАННЯ

Завдання № 1.

Відкрийте текстовий редактор (наприклад, Microsoft Word, Google Docs) і напишіть короткий текст (приблизно 200 слів) про ваше улюблене хобі.

Завдання № 2.

Виділіть текст у попередньому завданні та застосуйте різні стилі форматування: жирний, курсив, підкреслення, зміна розміру шрифту.

Завдання № 3.

Змініть шрифт тексту в різних частинах документа для створення візуального поділу на заголовки, основний текст та цитати.

Завдання № 4.

Експериментуйте з різними варіантами вирівнювання тексту (ліворуч, праворуч, по центру, по ширині).

Завдання № 5.

Виконайте ряд завдань:

1. Створіть список маркований із п’яти пунктів про переваги використання комп’ютерних публікацій.

2. Перетворіть попередній список на нумерований.

3. Додайте вкладений список до одного з пунктів нумерованого списку.

Завдання № 6.

Виконайте ряд завдань:

1. Додайте заголовки та підзаголовки різного рівня для структуризації тексту.

2. Використовуйте стилі заголовків (Heading 1, Heading 2, etc.) для створення консистентної ієрархії заголовків у документі.

3. Створіть покажчик документів із заголовками та підзаголовками.

Завдання № 7.

Скопіюйте текст з одного документа та вставте його в інший, використовуючи різні методи вставки (з форматуванням, без форматування).

Завдання № 8.

Використовуйте функцію пошуку та заміни для знаходження та зміни певних слів або фраз у документі.

Завдання № 9.

Перевірте текст на орфографічні та граматичні помилки, використовуючи вбудовані інструменти перевірки.

Завдання № 10.

Виконайте ряд завдань:

1. Створіть таблицю з трьох стовпців і чотирьох рядів для представлення даних про ваші улюблені фільми.

2. Застосуйте різні стилі форматування до таблиці (рамки, заливка, вирівнювання).

3. Об’єднайте кілька клітинок в одній і розділіть одну клітинку на дві.

4. Організуйте інформацію про книги (назву, автора, рік видання, жанр) у вигляді таблиці з можливістю сортування та фільтрування.

Завдання № 11.

Виконайте ряд завдань:

1. Вставте гіперпосилання на вебсайт, який вас цікавить.

2. Створіть список із посиланнями на інші документи або вебсторінки.

Завдання № 12.

Налаштуйте власні стилі для різних елементів тексту (наприклад, цитати, примітки).

Завдання № 13.

Виконайте ряд завдань:

1. Додайте автоматичне нумерування сторінок до документа.

2. Вставте роздільники сторінок для візуального поділу тексту на частини.

Завдання № 14.

Виконайте ряд завдань:

1. Створіть документ на основі готового шаблону (наприклад, бізнес-листівки, резюме).

2. Змініть шаблон документа для створення власного дизайну.

Завдання № 15.

Виконайте ряд завдань:

1. Вставте зображення з файлу в документ.

2. Змініть розмір зображення, зберігаючи пропорції та без пропорцій.

3. Обріжте зображення для видалення зайвих частин.

4. Налаштуйте яскравість і контрастність зображення.

5. Змініть колір зображення (наприклад, у чорно-білий або з фільтром).

6. Додайте до зображення різні ефекти (наприклад, тінь, ореол, розмиття).

7. Вставте текст на зображення для створення графічного повідомлення.

Завдання № 16.

Виконайте ряд завдань:

1. Створіть колаж із декількох зображень.

2. Використовуйте онлайн-редактори зображень (наприклад, Canva, Pixlr) для редагування та покращення якості зображень.

3. Змініть формат зображення з одного на інший (наприклад, з JPG на PNG).

Завдання № 17.

Виконайте ряд завдань:

1. Оптимізуйте розмір зображення для вебвикористання, щоб зменшити час завантаження сторінки.

2. Додайте водяний знак до зображень для захисту авторських прав.

3. Використовуйте інструменти редагування для виправлення дефектів зображення (наприклад, подряпини, плями).

Завдання № 18.

Створіть графіки та діаграми на основі даних (наприклад, кругові діаграми, стовпчасті діаграми).

Завдання № 19.

Виконайте ряд завдань:

1. Вставте 3D-зображення в документ.

2. Робота з векторною графікою: Створіть просту векторну графіку за допомогою інструментів редагування (наприклад, створення фігур та контурів).

3. Знайдіть та використовуйте безкоштовні або платні бібліотеки зображень для вашого проєкту.

4. Створіть прості ілюстрації за допомогою інструментів редагування.

Завдання № 20.

Перетворіть растрові зображення (наприклад, JPG) у векторні (наприклад, SVG).

Завдання № 21.

Створіть прості анімації з зображень за допомогою спеціалізованих інструментів.

Завдання № 22.

Виконайте ряд завдань:

1. Виконайте базове редагування фотографії в Photoshop: коригування кольору, освітлення, обрізка.

2. Застосуйте різні фільтри в Photoshop для зміни стилю зображення.

Завдання № 23.

1. Створіть маски для зображень, щоб частково приховати або показати їх.

Завдання № 24.

Створіть текстури на основі зображень для використання в графічному дизайні.

Завдання № 25.

Експериментуйте з різними режимами глибини кольору при роботі із зображеннями (наприклад, RGB, CMYK).

Завдання № 26.

Виконайте ряд завдань:

1. Змініть розмір полів сторінки.

2. Змініть орієнтацію сторінки з книжної на аркуш або навпаки.

3. Змініть розмір сторінки (наприклад, A4, Letter).

4. Додайте колонтитули зверху та знизу сторінки з інформацією про назву документа, дату тощо.

5. Налаштуйте нумерацію сторінок (початок, формат).

6. Вирівняйте колонтитули по лівому краю, правому краю або по центру.

Завдання № 27.

Виконайте ряд завдань:

1. Створіть розділи в документі з різними налаштуваннями сторінки (наприклад, різні поля, орієнтація).

2. Додайте горизонтальні та вертикальні лінії для візуального поділу тексту.

3. Перетворіть текст на стовпчиковий формат (наприклад, для газети).

4. Використовуйте готові шаблони сторінок для створення професійного вигляду документа.

5. Автоматично додавайте номери сторінок до заголовків розділів.

6. Створіть індекси сторінок для зручної навігації по документу.

7. Виберіть різні типи паперу та їх колір для візуалізації вигляду документа на друкованому носії.

Завдання № 28.

Виконайте ряд завдань:

1. Створіть кілька шаблонів документів з різними налаштуваннями сторінок для різних цілей.

2. Налаштуйте двосторонній друк документа.

3. Експортуйте документ у формат PDF зі збереженням всіх налаштувань форматування сторінок.

Завдання № 29.

Стилізуйте вебсторінку за допомогою базових правил CSS: колір шрифту, фон, розмір.

Завдання № 30.

Налаштуйте макет сторінки для оптимального відображення на мобільних пристроях та планшетах (адаптивний дизайн).

Завдання № 31.

Використовуйте HTML-теги (наприклад, <b>, <i>, <u>) для форматування тексту на вебсторінці.

Завдання № 32.

Створіть багатосторінковий документ з інтегрованими зображеннями, відео та аудіофайлами. Опишіть послідовність дій.

Завдання № 33.

Створіть макет вебсторінки за допомогою інструментів векторної графіки або HTML/CSS. Опишіть послідовність дій.

Завдання № 34.

Використовуйте систему сітки для створення структурованого макету сторінки. Опишіть послідовність дій.

Завдання № 35.

Розташуйте різні блоки контенту (текст, зображення, відео) на сторінці за допомогою CSS. Опишіть послідовність дій.

Завдання № 36.

Виконайте ряд завдань:

1. Використовуйте Flexbox для створення гнучких макетів сторінки.
2. Використовуйте Grid Layout для створення складних макетів сторінки.

Завдання № 37.

Створіть навігаційне меню для вебсайту. Опишіть послідовність дій.

Завдання № 38.

Додайте кнопки та форми на вебсторінку. Опишіть послідовність дій.

Завдання № 39.

Розташуйте текст та зображення в кількох колонках.

Завдання № 40.

Створіть ротаційні слайдери для відображення декількох зображень або повідомлень. Опишіть послідовність дій.

Завдання № 41.

Додайте інтерактивні елементи на вебсторінку (наприклад, анімації, відео). Опишіть послідовність дій.

Завдання № 42.

Налаштуйте макет сторінки для оптимального відображення на різних розмірах екранів. Опишіть послідовність дій.

Завдання № 43.

Використовуйте JavaScript для додавання додаткової функціональності та інтерактивності до вебсторінки. Опишіть послідовність дій.

Завдання № 44.

Створіть карту з позначками місць і інформацією про них. Опишіть послідовність дій.

Завдання № 45.

Вставте відео з YouTube або Vimeo на вебсторінку. Опишіть послідовність дій.

Завдання № 46.

Використовуйте AJAX для динамічного оновлення контенту на сторінці без перезавантаження. Опишіть послідовність дій.

Завдання № 47.

Створіть прості анімації за допомогою CSS. Опишіть послідовність дій.

Завдання № 48.

Створюйте та стилізуйте векторну графіку у форматі SVG. Опишіть послідовність дій.

Завдання № 49.

Оптимізуйте зображення, код та інші елементи сторінки для зменшення часу завантаження. Опишіть послідовність дій.

Завдання № 50.

Використовуйте інструменти розроблення браузера (Chrome DevTools, Firefox Developer Tools) для налагодження коду та виявлення помилок. Опишіть послідовність дій.

Завдання № 51.

Створіть вебсайт із декількома сторінками та зручною навігацією між ними. Опишіть послідовність дій.

Завдання № 52.

Використовуйте спеціалізовані інструменти для створення електронних книг (eBook) у різних форматах (EPUB, MOBI). Опишіть послідовність дій.

Завдання № 53.

Налаштуйте шрифт, розмір та інтервал між рядками для забезпечення комфортного читання тексту на екрані. Опишіть послідовність дій.

Завдання № 54.

Використовуйте семантичні HTML-теги (наприклад, <article>, <aside>, <nav>) для покращання доступності та SEO вебсторінки. Опишіть послідовність дій.

Завдання № 55.

Створіть інтерактивні інфографіки з анімацією та можливістю взаємодії з даними. Опишіть послідовність дій.

Завдання № 56.

Використовуйте онлайн-сервіси (наприклад, Canva, Figma) для швидкої верстки та дизайну вебсторінок. Опишіть послідовність дій.

Завдання № 57.

Створіть прості мобільні додатки на основі web-технологій, з використанням HTML, CSS та JavaScript. Опишіть послідовність дій.

Завдання № 58.

Додайте кнопки для поширення контенту в соціальних мережах та інтегруйте потоки соціальних мереж на свій сайт. Опишіть послідовність дій.

Завдання № 59.

Налаштуйте простий онлайн-магазин за допомогою готової eCommerce платформи (наприклад, Shopify, WooCommerce). Опишіть послідовність дій.

Завдання № 60.

Використовуйте Prezi або інші інструменти для створення динамічних та захоплюючих презентацій. Опишіть послідовність дій.

Завдання № 61.

Експортуйте документ із Microsoft Word або Google Docs у формат PDF. Опишіть послідовність дій.

Завдання № 62.

Перетворіть вебсторінку на PDF-файл. Опишіть послідовність дій.

Завдання № 63.

Використовуйте Adobe Acrobat Pro або інші інструменти для редагування PDF-файлів. Опишіть послідовність дій.

Завдання № 64.

Додайте нові сторінки до PDF-документа або видаліть зайві. Опишіть послідовність дій.

Завдання № 65.

Вставте текст, зображення та інші об’єкти у PDF-файл. Опишіть послідовність дій.

Завдання № 66.

Змініть шрифт, розмір та стиль тексту в PDF-документі. Опишіть послідовність дій.

Завдання № 67.

Додайте гіперпосилання у PDF-файл. Опишіть послідовність дій.

Завдання № 68.

Захистіть PDF-файл паролем для обмеження доступу. Опишіть послідовність дій.

Завдання № 69.

Додайте цифровий підпис до PDF-документа для підтвердження автентичності. Опишіть послідовність дій.

Завдання № 70.

Заповніть форми у PDF-файлах. Опишіть послідовність дій.

Завдання № 71.

Перетворіть PDF-файл у інші формати документів: Word, Excel, PowerPoint. Опишіть послідовність дій.

Завдання № 72.

Стисніть розмір PDF-файлу для зменшення його обсягу. Опишіть послідовність дій.

Завдання № 73.

Розділіть великий PDF-файл на кілька менших. Опишіть послідовність дій.

Завдання № 74.

Об’єднайте декілька PDF-файлів у один документ. Опишіть послідовність дій.

Завдання № 75.

Додайте коментарі та анотації до PDF-документу для обговорення з іншими користувачами. Опишіть послідовність дій.

Завдання № 76.

Вилучіть текст з PDF-файлу. Опишіть послідовність дій.

Завдання № 77.

Вилучіть зображення з PDF-файлу. Опишіть послідовність дій.

Завдання № 78.

Перетворіть кожну сторінку PDF на окреме зображення (JPEG, PNG). Опишіть послідовність дій.

Завдання № 79.

Створюйте та керуйте PDF-документами за допомогою командного рядка. Опишіть послідовність дій.

Завдання № 80.

Напишіть скрипти (наприклад, на Python) для автоматичного створення PDF-файлів. Опишіть послідовність дій.

Завдання № 81.

Створіть багатосторінковий електронний бюлетень (newsletter) із використанням HTML, CSS та зображень. Опишіть послідовність дій.

Завдання № 82.

Розробіть макет вебсайту для невеликої компанії, враховуючи її цільову аудиторію та брендинг. Опишіть послідовність дій.

Завдання № 83.

Зробіть цікаву і динамічну презентацію в PDF-форматі з інтерактивними елементами (анімація, відео). Опишіть послідовність дій.

Завдання № 84.

Застосуйте базові принципи SEO для оптимізації вебсторінки. Опишіть послідовність дій.

Завдання № 85.

Створіть адаптивний макет вебсайту для різних пристроїв за допомогою Responsive Design. Переконайтесь, що ваш сайт має естетичний вигляд на всіх екранах. Опишіть послідовність дій.

Завдання № 86.

Розроблення онлайн-каталогу продуктів із використанням HTML та CSS: створіть функціональний каталог товарів. Опишіть послідовність дій.

Завдання № 87.

Створіть PDF-документи зі змінним контентом (наприклад, персоналізовані листи). Опишіть послідовність дій.

Завдання № 88.

Використайте онлайн-інструменти для перевірки доступності вебсторінки. Опишіть послідовність дій.

Завдання № 89.

Оцініть якість та зручність використання різних форматів публікацій: PDF, HTML, EPUB. Опишіть послідовність дій.

Завдання № 90.

Виконайте ряд завдань:

1. Створіть простий документ у текстовому редакторі з використанням різних стилів форматування тексту (заголовок, підзаголовок, основний текст).
2. Вставте зображення у документ та змініть його розмір і положення.
3. Створіть таблицю в документі та заповніть її даними.
4. Додайте гіперпосилання на вебсайт у документ.
5. Створіть нумерований та маркований список у документі.
6. Перевірте орфографію та граматику в документі.

Завдання № 91.

Виконайте ряд завдань:

1. Створіть зміст до документа, використовуючи автоматичну функцію створення змісту.
2. Додайте колонтитули з датою та назвою документа на кожну сторінку.
3. Змініть макет сторінки (наприклад, додайте поля).
4. Збережіть документ у форматі PDF.
5. Конвертуйте текстовий файл в документ Microsoft Word.

Завдання № 92.

Виконайте ряд завдань:

1. Створіть просту публікацію з використанням графіки та тексту.

2. Додайте аудіофайл до публікації.

3. Зробіть скріншот екрана та вставте його у документ.

Завдання № 93.

Створіть просту інтерактивну публікацію з використанням гіперпосилань та кнопок. Опишіть послідовність дій.

Завдання № 94.

Змініть колір фону та тексту у документі. Опишіть послідовність дій.

Завдання № 95.

Додайте рамку навколо таблиці. Опишіть послідовність дій.

Завдання № 96.

Використайте функцію «Пошук і Заміна» для редагування тексту в документі. Опишіть послідовність дій.

Завдання № 97.

Створіть макет сторінки з двома колонками. Опишіть послідовність дій.

Завдання № 98.

Налаштуйте параметри друку документа (кількість копій, орієнтація). Опишіть послідовність дій.

Завдання № 99.

Створіть простий вебсайт за допомогою текстового редактора та базових HTML тегів.

Завдання № 100.

Використайте інструменти для створення інтерактивних діаграм. Опишіть послідовність дій.

Завдання № 101.

Створіть просту електронну книгу з використанням текстового редактора та програмного забезпечення для перетворення файлів.

Завдання № 102.

Налаштуйте параметри збереження PDF-файлу (розмір зображень, якість). Опишіть послідовність дій.

Завдання № 103.

Розмістіть текст так, щоб він гармонійно поєднувався із графікою.

Завдання № 104.

Оптимізуйте розмір PDF-файлу без втрати якості зображень. Опишіть послідовність дій.

Завдання № 105.

Використайте інструменти для автоматичного перетворення документів на різні формати. Опишіть послідовність дій.

Завдання № 106.

Створіть публікацію, яка буде адаптована для перегляду на мобільних пристроях. Опишіть послідовність дій.

Завдання № 107.

Оцініть якість комп'ютерної публікації, з точки зору читабельності та візуального оформлення. Опишіть послідовність дій.

ТЕСТИ

1. Що таке комп'ютерна публікація?

а) програмне забезпечення для створення електронних документів;

б) процес створення, редагування та розповсюдження інформації у цифровому форматі;

в) апаратне забезпечення для зберігання даних;

г) алгоритм оброблення текстової інформації.

2. Який із перелічених форматів є найбільш поширеним для комп'ютерних публікацій?

а) PDF;

б) DOC;

в) TXT;

г) всі перелічені варіанти.

3. Що таке DTP (Desktop Publishing)?

а) дизайн вебсайтів;

б) програми для роботи з базами даних;

в) процес створення графічних документів, таких як журнали та брошури;

г) розроблення мобільних додатків.

4. Який програмний пакет є найбільш популярним для DTP?

а) Microsoft Word;

б) Adobe InDesign;

в) Microsoft Excel;

г) Adobe Photoshop.

5. Що таке колонтитул у комп'ютерній публікації?

а) основний текст документа;

б) зображення, що вставляються в документ;

в) повторювані елементи інформації на початку або в кінці сторінки;

г) форматування тексту (шрифт, розмір).

6. Який із перелічених шрифтів є найбільш загальноприйнятим для друкованих публікацій?

а) Comic Sans MS;

б) Papyrus;

в) Times New Roman;

г) Arial.

7. Що таке колонтитул першої сторінки?

а) колонтитули, що зустрічаються на кожній сторінці документу;

б) колонтитул, який відображається тільки на першій сторінці;

в) колонтитул з назвою документа;

г) колонтитул з датою створення файлу.

8. Що таке макетування?

а) процес редагування тексту;

б) розміщення елементів (текст, зображення) на сторінці;

в) форматування шрифтів;

г) коректура помилок.

9. Який із перелічених форматів найкраще підходить для розповсюдження документа в інтернеті?

а) PDF;

б) DOC;

в) HTML;

г) TXT.

10. Що таке метадані у комп’ютерній публікації?

а) основний текст документа;

б) зображення, що вставляються в документ;

в) інформація про документ (автор, дата створення, ключові слова);

г) форматування тексту.

11. Яка роздільна здатність зображення найкраще підходить для вебсайту?

а) 300 dpi;

б) 72 dpi;

в) 600 dpi;

г) 1200 dpi.

12. Що таке векторна графіка?

а) графіка, що складається з пікселів;

б) фотографії;

в) графіка, що визначається математичними рівняннями;

г) створення 3D моделей.

13. Який формат файлу зазвичай використовується для векторної графіки?

а) JPG;

б) PNG;

в) SVG;

г) GIF.

14. Що таке растрова графіка?

а) графіка, що складається з математичних рівнянь;

б) графіка, що складається з пікселів;

в) 3D моделі;

г) текст.

15. Який формат файлу зазвичай використовується для растрової графіки?
а) SVG;
б) JPG;
в) TXT;
г) DOC.

16. Що таке колонтитул сторінки?
а) текст, що знаходиться в основному блоці тексту;
б) інформація, яка повторюється на кожній сторінці;
в) графічне оформлення сторінки;
г) списки та таблиці.

17. Що таке спливаюче вікно (pop-up)?
а) звичайний текст в документі;
б) вікно, що з’являється на екрані поверх іншого додатка;
в) графічне оформлення сторінки;
г) спеціальний тип шрифту.

18. Який формат файлу краще використовувати для зберігання зображень у вебсайті?
а) BMP;
б) TIFF;
в) JPEG;
г) RAW.

19. Що таке HTML?
а) програма для редагування тексту;
б) мова розмітки для створення вебсторінок;
в) графічний редактор;
г) база даних.

20. Який інструмент використовується для створення гіперпосилань?
а) текстовий редактор;
б) HTML-редактор;
в) графічний редактор;
г) програма для роботи з базами даних.

21. Що таке CSS?

а) мова програмування;

б) мова стилів для оформлення вебсторінок;

в) база даних;

г) текстовий редактор.

22. Яка мета JavaScript?

а) створення графіки;

б) додавання інтерактивності на вебсторінки;

в) оформлення тексту;

г) управління базами даних.

23. Що таке XML?

а) формат зображень;

б) маркована мова для зберігання та передавання даних;

в) графічний редактор;

г) текстовий редактор.

24. Яка основна відмінність між PDF та HTML?

а) PDF призначений лише для читання, а HTML – для друку;

б) PDF зберігає фіксоване форматування, а HTML адаптується до різних пристроїв;

в) HTML може містити графіку, а PDF – ні;

г) HTML краще підходить для створення вебсайтів, а PDF – для документів.

25. Що таке OCR (Optical Character Recognition)?

а) процес перетворення аудіо в текст;

б) процес розпізнавання тексту на зображенні;

в) створення 3D моделей;

г) оформлення сторінок.

26. Який з перелічених форматів файлів є найбільш сумісним для обміну документами між різними операційними системами?

а) DOCX;

б) PDF;

в) RTF;

г) TXT.

27. Що таке емуляція шрифтів?

а) перетворення тексту в зображення;

б) заміна відсутнього шрифту на схожий;

в) форматування тексту;

г) створення колонтитулів.

28. Який із перелічених інструментів використовується для створення таблиць у комп'ютерній публікації?

а) графічний редактор;

б) текстовий редактор;

в) програмне забезпечення DTP;

г) програма для роботи з базами даних.

29. Що таке верстка?

а) створення графічних елементів;

б) редагування тексту;

в) розміщення тексту та зображень на сторінці;

г) форматування шрифтів.

30. Який із перелічених форматів файлів найкраще підходить для збереження вебсайту?

а) DOCX;

б) PDF;

в) ZIP;

г) TXT.

31. Що таке «мацання»?

а) написання тексту на клавіатурі, не дивлячись на клавіші;

б) написання тексту на клавіатурі безпосередньо, не дивлячись на клавіші;

в) використання спеціальної клавіатури;

г) написання тексту за допомогою голосового управління.

32. Що таке набір?

а) графічний елемент;

б) набір символів, що характеризуються певним стилем;

в) розмір шрифту;

г) колір тексту.

33. Який із перелічених форматів файлу найбільш компактний?

а) PNG;

б) JPG;

в) GIF;

г) TIFF.

34. Що таке інверсія кольору?

а) зміна тексту на іншу мову;

б) додавання ефекту тіні до тексту;

в) зміна кольорів на протилежні;

г) форматування шрифтів.

35. Який із перелічених інструментів використовується для створення ілюстрацій?

а) текстовий редактор;

б) програма для роботи з базами даних;

в) графічний редактор;

г) програма для обробки аудіо.

36. Що таке кропованість?

а) зміна розміру тексту;

б) додавання ефекту тіні до тексту;

в) вирізання частини зображення;

г) форматування шрифтів.

37. Який із перелічених форматів найкраще підходить для створення презентацій?

а) DOCX;

б) PDF;

в) TXT;

г) PPTX.

38. Що таке індексація?

а) додавання зображень до документа;

б) форматування тексту;

в) створення списку ключових слів у документі;

г) коректура помилок.

39. Що таке слайд шоу?

а) процес створення презентації;

б) послідовне відображення слайдів презентації;

в) редагування тексту на слайді;

г) додавання анімації до слайдів.

40. Який із перелічених форматів файлу використовується для створення інтерактивних документів?

а) PDF;

б) DOCX;

в) TXT;

г) EPUB.

ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Що таке комп’ютерна публікація?
2. Які основні етапи створення комп’ютерної публікації?
3. Перерахуйте основні формати файлів, що використовуються в комп’ютерних публікаціях.
4. Що таке розмітка документів і яке її значення?
5. У чому різниця між векторною та растровою графікою? Наведіть приклади.
6. Які основні компоненти програмного забезпечення для створення комп’ютерних публікацій?
7. Опишіть функціональні можливості текстового редактора.
8. Що таке шрифти і які їх класифікації ви знаєте?
9. Яке значення має типографіка у процесі створення публікації?
10. Що таке колонтитули та як вони використовуються?
11. Як створюються списки (нумеровані та марковані) в текстовому редакторі?
12. Які засоби форматування тексту ви знаєте?
13. Опишіть процес вставки зображень у документ.
14. Що таке об’єкти та як їх можна використовувати в публікаціях?
15. Як працюють таблиці в текстових редакторах?
16. Що таке гіперпосилання і яке його призначення?
17. Які можливості створення індексів та глосаріїв, передбачені сучасними програмами для публікацій?
18. Опишіть процес перевірки орфографії та граматики в текстовому редакторі.
19. Що таке макети документів і які основні принципи їх створення?

20. Які типи макетів ви знаєте (наприклад, односторінковий, багатосторінковий)?
21. Як створюються колонтитули з різним вмістом для різних сторінок?
22. Що таке стилі та які переваги їх використання?
23. Опишіть процес створення змісту до публікації.
24. Які можливості інтеграції мультимедійного контенту (аудіо, відео) передбачені сучасними програмами для публікацій?
25. Що таке PDF-файл і які його основні переваги?
26. Як конвертувати документи з одного формату в інший?
27. Які програмні пакети використовуються для створення професійних комп'ютерних публікацій (назвіть хоча б три)?
28. Що таке верстка і яка її роль у створенні публікації?
29. Як забезпечити доступність публікації для людей з обмеженими можливостями?
30. Які вимоги до оформлення наукових статей?
31. Опишіть процес створення електронної книги.
32. Що таке цифрова верстка і які її особливості?
33. Як використовувати програмне забезпечення для створення інтерактивних публікацій?
34. Яке значення має оптимізація розміру файлу публікації?
35. Опишіть процес друку комп'ютерної публікації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

Основні нормативні акти:

1. Про авторське право і суміжні права : Закон України від 23.12.1993 р. № 3792-XII : станом на 1 січ. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/3792-12#Text.
2. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
3. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
4. Про Національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР : станом на 1 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text.

Підручники:

1. Weverka P. Office 365 All-in-One For Dummies. 2nd ed. For Dummies, 2022. 960 p.
2. Буйницька О. Інформаційні технології та технічні засоби навчання : навч. посіб. Київ : Центр навч. літ., 2019. 240 с.
3. Караванова Т. П. Олімпіадна інформатика [Текст] : навч. посіб. ; Чернівец. нац. ун-т ім. Юрія Федьковича. Чернівці : Рута, 2024. 231 с.
4. Клиса І. І. Інформатика [Текст] : навч. посіб. ; Відокремл. структур. підрозд. «Івано-Франк. фах. коледж фіз. виховання Нац. ун-ту фіз. виховання і спорту України». Львів : Бона, 2023. 235 с.
5. Павлиш В., Гліненко Л., Шаховська Н. Основи інформаційних технологій і систем : підручник. Львів : Львів. політехніка, 2018. 620 с.
6. Свистельник І. Інформаційна культура студента : підручник. Київ : Кондор, 2018. 182 с.

Навчальні посібники, інші дидактичні та методичні матеріали:

1. Eastman A. Wordpress for Beginners 2020: A Visual Step-by-Step Guide to Mastering Wordpress and Create your Blog and Website from Zero. Independently published, 2020. 162 p.
2. Биков І. Ю. Microsoft Office в задачах економіки та управління: навч. посіб. для студ. вищ. навч. закл. Київ: Професіонал, 2016. 263 с.
3. Бош Р. Opt Art. Від математичного оптимізації до візуального дизайну [Текст] / Роберт Бош ; [пер. з англ. Е. Рабинович]. Харків : Фабула, 2023. 199 с.

4. Ментинський С. М. Збірник задач з основ алгоритмізації та програмування [Текст] : навч. посіб. з курсів «Обчислювальна техніка та програмування», «Інформатика», «Основи інформатики і програмування» для студентів техн. спец. для першого (бакалавр.) рівня освіти. Львів : Колір ПРО, 2023. 319 с.
5. Нужний Є., Клименко І., Акімов О. Інструментальні засоби електронного офісу : навч. посіб. Київ : «Центр учб. літ.», 2017. 296 с.

Інтернет-ресурси

1. Draw Freely | Inkscape. URL: https://inkscape.org/?switchlang=en.
2. Word та Excel: інструменти і лайфхаки. Prometheus. URL: https://prometheus.org.ua/course/course-v1:DNU+PRIN-101+2017_T1.
3. Дніпропетровська обласна універсальна наукова бібліотека. URL: https://www.libr.dp.ua/.
4. Національна бібліотека України імені В. І. Вернадського. URL: http://www.nbuv.gov.ua/.
5. Офіційний портал Верховної Ради України. URL: https://www.rada.gov.ua/.
6. Служба підтримки Microsoft. Microsoft Support. URL: https://support.microsoft.com/uk-UA.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ:

Оцінка в балах	Оцінка за національною шкалою (екзамен /залік)	Оцінка за шкалою ЄКТС	
		Оцінка	Пояснення
90–100	**Відмінно**	**A**	**«Відмінно»** – теоретичний зміст курсу засвоєний **у повному обсязі; сформовані** необхідні практичні навички роботи із засвоєним матеріалом; **всі** навчальні завдання, передбачені програмою навчання, **виконані** в повному обсязі.
83–89	**Добре**	**B**	**«Дуже добре»** – теоретичний зміст курсу засвоєний **у повному обсязі; в основному сформовані** необхідні практичні навички роботи із засвоєним матеріалом; **всі** навчальні завдання, передбачені програмою навчання, **виконані**, якість виконання **більшості** з них оцінена кількістю балів, близькою до **максимальної**.
75–82		**C**	**«Добре»** – теоретичний зміст курсу засвоєний **цілком; в основному сформовані** практичні навички роботи із засвоєним матеріалом; **всі** навчальні завдання, передбачені програмою навчання, **виконані**, якість виконання **жодного** з них **не оцінена мінімальною** кількістю балів, деякі види завдань виконані **з помилками**.
68–74	**Задовільно**	**D**	**«Задовільно»** – теоретичний зміст курсу засвоєний **не повністю**, але **прогалини не носять істотного** характеру; **в основному сформовані** необхідні практичні навички роботи із засвоєним матеріалом; **більшість** передбачених програмою навчання навчальних завдань **виконано, деякі** з виконаних завдань містять **помилки**.
60–67		**E**	**«Достатньо»** – теоретичний зміст курсу засвоєний **частково; не сформовані деякі** практичні навички роботи; **частина** передбачених програмою навчання навчальних завдань **не виконані** або якість виконання деяких з них оцінено числом балів, близьким до **мінімального**.
35–59	**Незадовільно**	**FX**	**«Умовно незадовільно»** – теоретичний зміст курсу засвоєний **частково; не сформовані** необхідні практичні навички роботи; **більшість** навчальних завдань **не виконано** або якість їх виконання оцінено кількістю балів, близькою до **мінімальної**; при **додатковій самостійній** роботі над матеріалом курсу **можливе підвищення якості** виконання навчальних завдань (**з можливістю повторного складання**).
1–34		**F**	**«Безумовно незадовільно»** – теоретичний зміст курсу **не засвоєний; не сформовані** необхідні практичні навички роботи; **всі виконані** навчальні завдання містять грубі **помилки або не виконані взагалі; додаткова самостійна** робота над матеріалом курсу **не призведе** до значного **підвищення якості** виконання навчальних завдань.

Алєксєєв Артур Васильович,
викладач кафедри міжкультурної
комунікації та соціально-гуманітарних
дисциплін Вищого навчального
приватного закладу «Дніпровський
гуманітарний університет»