DSPU CYBER SEC

РОБОЧИЙ ЗОШИТ З КІБЕРБЕЗПЕКИ

with support from Google.org

ДМИТРО КАРПИН

ДРОГОБИЧ
2025

ЗМІСТ

МОДУЛЬ 1: ОСНОВИ КІБЕРБЕЗПЕКИ

ТЕМА 1: КЛЮЧОВІ ПОНЯТТЯ КІБЕРБЕЗПЕКИ

Кібербезпека – це сукупність методів, технологій та процесів, що спрямовані на захист інформаційних систем, мереж та пристроїв від цифрових загроз, таких як кібератаки, шкідливе програмне забезпечення та несанкціонований доступ.

Основні принципи кібербезпеки (CIA-тріада):

• Конфіденційність (Confidentiality) – захист даних від несанкціонованого доступу.

• Цілісність (Integrity) – забезпечення незмінності та достовірності даних.

• Доступність (Availability) – гарантія того, що дані та системи будуть доступні авторизованим користувачам у потрібний момент.

Крім CIA-тріади, сучасні системи кібербезпеки також використовують принципи **аутентифікації, авторизації та невідмовності.**

ЗАВДАННЯ. Заповни таблицю

Поняття	Пояснення
Аутентифікація	
Авторизація	
Невідмовність	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Компанія зберігає особисті дані клієнтів у незахищеній базі даних, доступ до якої не обмежений паролем. Один із співробітників випадково надіслав копію цієї бази на зовнішню пошту.

Запитання для роздумів:
Які принципи безпеки даних були порушені?
Які наслідки може мати витік даних?
Як компанія могла запобігти цій ситуації?

Нотатки _____

ТЕМА 2: ОСНОВНІ ТИПИ КІБЕРЗАГРОЗ

Основні види кіберзагроз:

Віруси – шкідливі програми, що самостійно розмножуються, заражаючи файли і системи.
Фішинг – спроби обманом змусити користувача надати конфіденційні дані (паролі, дані банківських карток) через підроблені листи чи сайти.
DDoS-атаки – атаки, спрямовані на перевантаження серверів чи сайтів великим обсягом трафіку з метою вивести їх із ладу.
Соціальна інженерія – використання психологічних методів для отримання доступу до інформації або систем.


Віруси


Фішинг


DDoS-атаки


Соціальна інженерія

Ключові риси загроз:

- Потреба в обережності та уважності при роботі в інтернеті.
- Постійна еволюція загроз (нові типи вірусів, витонченіші атаки).

ЗАВДАННЯ. Заповни таблицю

Ситуація	Тип загрози
Користувач отримав підроблений лист від «банку»	
Сервер недоступний через велику кількість запитів	
На флешці виявлено шкідливий файл	
Дзвінок «працівника техпідтримки», який просить дані акаунта	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Петро отримав електронний лист нібито від служби підтримки соцмережі. У листі його просять терміново перейти за посиланням та оновити свої дані, інакше обліковий запис буде заблоковано. Посилання веде на сайт, схожий на справжній.

Запитання для роздумів:
Який тип атаки використано?
Які ознаки вказують на підробку листа?
Що потрібно було б зробити Петру в цій ситуації?

Нотатки _____

ТЕМА 3: ЕТИЧНІ ТА ПРАВОВІ АСПЕКТИ КІБЕРБЕЗПЕКИ

Етичні принципи в кібербезпеці:

Чесність — не використовувати знання для заподіяння шкоди.
Конфіденційність — повага до приватності інших користувачів.
Відповідальність — усвідомлення наслідків своїх дій у кіберпросторі.
Дотримання законів — дії мають відповідати чинному законодавству.

Правові аспекти кібербезпеки:

- Дані захищаються законами, такими як GDPR.
- За комп'ютерні злочини передбачена відповідальність.
- Збір даних можливий лише за згодою користувача.
- В Україні діють Кримінальний кодекс і Закон про захист інформації.

ЗАВДАННЯ. Заповни таблицю.
Прочитайте приклади і визначте, чи порушені етичні або правові норми:

Приклад	Етичне порушення?	Правове порушення?
Студент завантажив чужий курс без дозволу	Так / Ні	Так / Ні
Користувач встановив антивірус	Так / Ні	Так / Ні
Працівник компанії передав пароль колезі	Так / Ні	Так / Ні
Хакер здійснив DDoS-атаку на сайт	Так / Ні	Так / Ні

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Катерина працює в компанії, яка обробляє персональні дані клієнтів. Вона знайшла спосіб зберігати деякі дані на особистій флешці, щоб працювати вдома без офіційного дозволу керівництва.

Запитання для роздумів:

Які етичні ризики існують у цій ситуації?
Чи є це порушенням закону?
Які можливі наслідки для Катерини та компанії?

Нотатки _____

ТЕМА 4: ОСНОВИ ДОСТУПНОСТІ У КІБЕРБЕЗПЕЦІ

Доступність — це здатність усіх користувачів, незалежно від фізичних або технічних можливостей, безпечно користуватися цифровими сервісами. Вона є однією з трьох ключових складових кібербезпеки (разом із конфіденційністю та цілісністю) та важливою умовою цифрової інклюзії.

Кому вона потрібна?

- Людям з порушеннями зору, слуху або моторики.
- Літнім людям.
- Користувачам з низькою цифровою грамотністю.
- Тимчасово вразливим групам (після травм тощо).

Які стандарти діють?

- WCAG (Web Content Accessibility Guidelines)
- ISO/IEC 40500:2012
- Європейський акт про доступність
- Закон України «Про основні засади забезпечення доступності»

ЗАВДАННЯ. Заповни таблицю.
Заповніть таблицю: хто є вразливою групою — і яку перешкоду в доступі вони можуть мати?

Група користувачів	Можлива проблема доступності
Користувач з порушенням зору	
Літня людина	
Людина з травмою руки	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Онлайн-банкінг пропонує автентифікацію тільки через візуальний капча-код. Користувач з порушенням зору не може пройти авторизацію.

Запитання для роздумів:
Яку помилку допустив сервіс?
Як це впливає на доступність?
Які альтернативи можна запропонувати?

Нотатки _____

ТЕМА 5: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

Як штучний інтелект допомагає у кібербезпеці:

Виявлення загроз у режимі реального часу: AI аналізує величезні обсяги даних для виявлення аномалій, які можуть свідчити про атаку.
Автоматизація реагування на інциденти: AI може самостійно блокувати підозрілу активність або попереджати операторів систем безпеки.
Аналіз поведінки користувачів: AI виявляє нетипові дії, що можуть свідчити про злом акаунта або інсайдерську атаку.
Прогнозування майбутніх атак: На основі аналізу минулих інцидентів AI допомагає передбачити потенційні загрози.

Обмеження та ризики використання AI у кібербезпеці:

- Можливі помилкові спрацьовування (false positives).
- Атаки на самі AI-системи.
- Етичні питання використання даних.

ЗАВДАННЯ. Заповни таблицю.
Вкажіть, чи правда або неправда:

Твердження	Правда/Неправда
AI може допомогти передбачити майбутні атак	
AI завжди дає 100% точні результати	
AI здатний виявляти невідомі типи атак	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Компанія X впровадила систему на базі AI для моніторингу мережевого трафіку. Система виявила незвичайний доступ до бази даних у нічний час і повідомила адміністратора, який вчасно заблокував зловмисника.

Запитання для роздумів:
Як AI допоміг запобігти загрозі?
Чому людський контроль все ще важливий навіть за наявності AI?
Як компанія може покращити ефективність своєї AI-системи?

Нотатки _____

ТЕМА 6: ОСНОВИ БЕЗПЕКИ ДАНИХ У ЦИФРОВОМУ СЕРЕДОВИЩІ

Безпека даних — це процеси та технології, спрямовані на захист даних від несанкціонованого доступу, викрадення, зміни чи знищення.
У сучасному цифровому середовищі дані є одним із найцінніших ресурсів, тому їхній захист є критично важливим.

Типові загрози безпеці даних:

- Злом акаунтів та несанкціонований доступ.
- Витоки даних через фішингові атаки.
- Віруси та шкідливе програмне забезпечення.
- Втрата даних через збої систем або фізичне знищення пристроїв.

ЗАВДАННЯ. Заповни таблицю.

Поведінка користувача	Безпечно / Небезпечно
Зберігає паролі у відкритому документі на робочому столі	
Використовує двофакторну автентифікацію для облікових записів	
Ділиться банківськими реквізитами через месенджер	
Регулярно оновлює операційну систем	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Компанія зберігає особисті дані клієнтів у незахищеній базі даних, доступ до якої не обмежений паролем. Один із співробітників випадково надіслав копію цієї бази на зовнішню пошту.

Запитання для роздумів:
Які принципи безпеки даних були порушені?
Які наслідки може мати витік даних?
Як компанія могла запобігти цій ситуації?

Нотатки _____

ТЕМА 7: РЕЗЕРВНЕ КОПІЮВАННЯ ТА ВІДНОВЛЕННЯ ДАНИХ

Резервне копіювання (бекап) — це процес створення копії даних, яка використовується для їх відновлення у випадку втрати, пошкодження або кібератаки.

Основні стратегії резервного копіювання:
Правило 3-2-1: 3 копії даних, 2 різних носії, 1 копія зберігається окремо (наприклад, у хмарі).
Регулярність: копії слід оновлювати відповідно до частоти змін даних.
Перевірка: важливо тестувати працездатність копій.

Відновлення даних:
- Процес повернення даних із резервної копії у разі втрати або пошкодження оригіналу.
- Критично важливий для бізнесу, освіти, медицини та інших сфер.

ЗАВДАННЯ. Заповни таблицю.

Елемент	Твій варіант
Які дані потрібно копіювати?	
Скільки копій буде створено?	
Які два типи носіїв ти обереш?	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Компанія мала тільки одну копію своїх критичних даних на одному комп'ютері. Після збою жорсткого диска вся інформація була втрачена. Жодної альтернативної копії не існувало.

Запитання для роздумів:
Яких помилок припустилася компанія?
Які стратегії резервного копіювання слід було застосувати?
Що потрібно змінити у підході до захисту даних у майбутньому?

Нотатки _____

МОДУЛЬ 2: ЗАХИСТ ДАНИХ І ПРИСТРОЇВ

ТЕМА 8: МЕТОДИ ШИФРУВАННЯ ДАНИХ

Шифрування — це процес перетворення даних у форму, яка є незрозумілою для сторонніх осіб. Тільки уповноважені користувачі можуть відновити вихідну інформацію за допомогою спеціального ключа.

Основні типи шифрування:
Симетричне шифрування: один і той же ключ використовується для шифрування та розшифрування даних (наприклад, AES).
Асиметричне шифрування: використовується пара ключів — публічний і приватний (наприклад, RSA).

Важливі поняття:

- Публічний ключ — використовується для шифрування повідомлення.
- Приватний ключ — використовується для розшифрування повідомлення.
- Цифровий підпис — гарантує справжність повідомлення і цілісність даних.

ЗАВДАННЯ. Заповни таблицю.

Ситуація	Тип шифрування
Перед відправленням електронного листа система генерує пару ключів: один відкритий, інший приватний.	
USB-накопичувач шифрується єдиним ключем, який знає тільки власник.	
Додаток для обміну повідомленнями використовує один спільний ключ для зашифрування і розшифрування.	
Сайт використовує сертифікат SSL для шифрування з'єднання з браузером.	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Компанія надсилала важливу фінансову інформацію клієнтам електронною поштою без використання шифрування. Одного разу хакери перехопили лист і отримали доступ до конфіденційних даних.

Запитання для роздумів:
Якої помилки припустилася компанія?
Які технології можна було б застосувати для безпечної передачі інформації?
Чому важливо використовувати шифрування при передаванні важливих даних?

Нотатки _____

ТЕМА 9: ЕЛЕКТРОННИЙ ПІДПИС: ПРИНЦИПИ РОБОТИ

Електронний підпис — це електронні дані, які додаються до іншого електронного документа з метою підтвердження його автентичності та цілісності.

Типи електронних підписів:

Простий електронний підпис (ПЕП): мінімальний рівень безпеки, наприклад, сканований підпис.

Кваліфікований електронний підпис (КЕП): створюється за допомогою спеціального захищеного пристрою і має таку ж юридичну силу, як власноручний підпис.

Удосконалений електронний підпис: забезпечує зв'язок між підписом і підписувачем, а також захист від змін даних.

Як працює електронний підпис:

- Використовується асиметричне шифрування (пара ключів: приватний + публічний).
- Дані шифруються приватним ключем підписувача.
- Отримувач перевіряє підпис за допомогою публічного ключа.

ЗАВДАННЯ. Заповни таблицю.

Поняття	Визначення
Приватний ключ	
Публічний ключ	
Кваліфікований електронний підпис	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Організація підписувала договори з клієнтами за допомогою простого електронного підпису (сканованого зображення підпису). Коли виник спір щодо автентичності підписаного документа, суд не визнав цей підпис доказом.

Запитання для роздумів:

Чому виникла проблема?

Який тип електронного підпису варто було використовувати?

Які переваги дає використання кваліфікованого електронного підпису?

Нотатки _____

ТЕМА 10: УПРАВЛІННЯ ДОСТУПОМ ТА ПАРОЛІ

Управління доступом — це система процесів і технологій, яка забезпечує, що тільки авторизовані користувачі мають доступ до певних даних або систем.

Основні компоненти управління доступом:
Ідентифікація — встановлення особи користувача (логін, ID).
Аутентифікація — підтвердження особи (пароль, код, біометрія).
Авторизація — надання прав доступу відповідно до ролі користувача.
Аудит — фіксація дій користувачів для виявлення можливих порушень.

Пароль — це секретна комбінація символів, що використовується для підтвердження ідентичності користувача.

Критерії надійного пароля:
- Мінімум 12 символів.
- Комбінація великих і малих літер, цифр і спеціальних символів.
- Уникнення очевидних комбінацій (дата народження, «123456», «password»).

Поради щодо безпеки паролів:
- Не використовувати один і той самий пароль для кількох сервісів.
- Регулярно змінювати паролі.
- Використовувати менеджери паролів для зберігання складних комбінацій.
- (Вставка графіки: Іконка ключа або замка із символом пароля — «*****».)

ЗАВДАННЯ. Заповни таблицю. Оцініть кожен пароль як «Надійний» або «Ненадійний»:

Пароль	Оцінка
Qwerty123	
3x4!sB7#pL	
Password1	
9Fg$21m!vQ	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Компанія зберігала облікові записи співробітників у текстовому файлі без шифрування. Один із працівників випадково надіслав цей файл сторонній особі, що призвело до масового витоку даних.

Запитання для роздумів:
Яких принципів управління доступом було порушено?
Які заходи могли б запобігти цій ситуації?
Як правильно організувати захист облікових даних?

ТЕМА 11: БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ (MFA)

Багатофакторна автентифікація — це метод підтвердження особи користувача шляхом перевірки двох або більше незалежних факторів.

Три основні фактори автентифікації:
Що ви знаєте (пароль, PIN-код).
Що ви маєте (смартфон, токен, смарт-карта).
Хто ви є (біометричні дані: відбиток пальця, розпізнавання обличчя).

Популярні приклади MFA:

- Підтвердження входу через SMS-код.
- Використання додатку-аутентифікатора (Google Authenticator, Microsoft Authenticator).
- Біометричне підтвердження (відбиток пальця для входу в додаток).

ЗАВДАННЯ. Заповни таблицю.

Фактор	Тип фактора (знання / володіння / біометрія)
Пароль	
Смартфон із кодом підтвердження	
Відбиток пальця	
PIN-код	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Іван використовував складний пароль для входу в корпоративну систему, але одного дня його обліковий запис був зламаний. З'ясувалося, що в системі не була активована багатофакторна автентифікація.

Запитання для роздумів:
Як могло допомогти використання MFA у цій ситуації?
Який другий фактор був би найзручнішим для Івана?
Чи достатньо лише одного фактора для захисту облікового запису?

Нотатки _____

ТЕМА 12: ЗАХИСТ ХМАРНИХ РЕСУРСІВ

Хмарні ресурси — це сервери, сховища даних, програмні сервіси, які доступні через інтернет і управляються сторонніми постачальниками (наприклад, Google Drive, Dropbox, AWS).

Основні ризики при використанні хмарних сервісів:
Несанкціонований доступ до даних.
Витоки або втрата інформації.
Зловмисне використання хмарних облікових записів.
Недостатній контроль над безпекою постачальника.

Ключові заходи захисту хмарних ресурсів:
- Використання сильних паролів і багатофакторної автентифікації (MFA).
- Шифрування даних перед передачею і під час зберігання.
- Обмеження доступу за принципом мінімальних прав.
- Регулярний аудит активностей облікового запису.
- Вибір надійного хмарного постачальника, який має сертифікації безпеки.

ЗАВДАННЯ. Заповни таблицю. Оцініть кожну ситуацію. Чи є вона безпечною, чи створює ризик для даних у хмарному середовищі? Поясніть коротко.

Ситуація	Безпечно / Ризиковано	Чому? (коротко)
Користувач увімкнув двофакторну автентифікацію в Google Drive.		
Дані автоматично синхронізуються з хмарою без шифрування.		
Спільний доступ до документа відкритий для всіх за посиланням.		
Користувач регулярно перевіряє історію входів у хмарний сервіс.		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Малий бізнес зберігав усі документи компанії у безкоштовному хмарному сервісі без налаштування багатофакторної автентифікації та без шифрування файлів. Після компрометації облікового запису всі дані були втрачені.

Запитання для роздумів:
Яких помилок припустилася компанія?
Які прості кроки могли б зменшити ризик?
Чому важливо вибирати хмарного постачальника із сертифікацією безпеки?

Нотатки _____

ТЕМА 13: АНТИВІРУСНІ ПРОГРАМИ ТА ЇХ РОЛЬ У БЕЗПЕЦІ

Антивірус — це спеціальне програмне забезпечення, призначене для виявлення, блокування та видалення шкідливого програмного забезпечення (вірусів, троянів, шпигунських програм, руткітів тощо).

Основні функції антивірусів:
Сканування системи: регулярна перевірка файлів і процесів на наявність шкідливого коду.
Моніторинг у реальному часі: постійне спостереження за діями у системі.
Оновлення баз шкідливих програм: автоматичне завантаження нової інформації про загрози.
Карантин: ізоляція підозрілих файлів для подальшого аналізу.

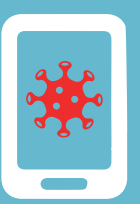
Чому важливо використовувати антивірус:
- Він допомагає запобігти зараженню пристроїв та втраті даних.
- Значно знижує ризик зараження навіть під час випадкового відвідування небезпечних сайтів.

ЗАВДАННЯ. Заповни таблицю. Підпишіть правильні функції антивірусної програми:

Функція	Так / Ні
Виявлення шкідливого програмного забезпечення	
Копіювання особистих файлів користувача	
Оновлення баз загроз	
Ізоляція підозрілих файлів	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Олена використовувала комп'ютер без антивірусної програми. Після завантаження файлу з невідомого сайту її пристрій почав поводитись дивно: сповільнилась робота, з'явилися підозрілі вікна і спливаючі реклами.



Запитання для роздумів:
Яких помилок припустилася Олена?
Як антивірус міг би допомогти запобігти зараженню?
Які додаткові заходи безпеки варто застосовувати при роботі в інтернеті?

Нотатки _____

ТЕМА 14: ОНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Оновлення програмного забезпечення — це процес встановлення нових версій операційної системи, застосунків або драйверів. Такі оновлення випускаються розробниками для усунення помилок, підвищення безпеки, поліпшення функціоналу або адаптації до нових стандартів. Небезпека використання застарілих версій полягає в тому, що хакери часто користуються відомими вразливостями в ПЗ, яке давно не оновлювалося. Чим більше часу минає від останнього оновлення, тим вищий ризик зламу.

Існують три основні типи оновлень:

- Безпекові (security patches): закривають уразливості.
- Функціональні: додають нові можливості або покращують інтерфейс.
- Критичні (critical updates): обов'язкові для стабільної роботи.

Автоматичне оновлення зазвичай є найкращим варіантом для звичайних користувачів. У великих організаціях оновлення часто планують централізовано, щоби уникнути конфліктів із іншими системами.

ЗАВДАННЯ. Заповни таблицю. Прочитай твердження та познач, правильне воно чи ні. Якщо неправильно — коротко поясни чому.

Твердження	Так / Ні	Пояснення
Встановлювати оновлення можна лише вручну		
Безпекові оновлення слід встановлювати якомога швидше		
Оновлення може зробити пристрій повільнішим		
Якщо комп'ютер працює нормально, оновлення не потрібні		

КЕЙС ДЛЯ АНАЛІЗУ

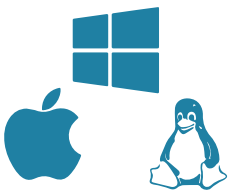
Ситуація: У школі вчителька інформатики ігнорувала повідомлення про оновлення Windows протягом кількох місяців. Після відкриття вкладення з невідомого листа її комп'ютер почав самостійно пересилати файли іншим працівникам школи. Антивірус був застарілий, а система не оновлювалась.

Запитання для роздумів:

Яку роль зіграла відсутність оновлень у цій ситуації?
Як можна було запобігти цьому?
Які дії потрібно зробити після такого інциденту?

Нотатки _____

ТЕМА 15: ЗАХИСТ КОМП'ЮТЕРІВ ПІД УПРАВЛІННЯМ РІЗНИХ ОС



Операційна система (ОС) керує всіма процесами на комп'ютері, і саме вона є першою лінією захисту від зовнішніх загроз. Різні ОС — Windows, macOS, Linux — мають свої особливості безпеки, сильні та слабкі сторони.

Windows найпопулярніша, а тому й найбільш атакована. Вона потребує регулярного оновлення, антивіруса та ввімкненого брандмауера.
macOS вважається більш захищеною за замовчуванням завдяки закритій архітектурі та системам перевірки додатків, але також потребує оновлень і обачності при роботі з файлами.
Linux часто використовується IT-фахівцями. Має високу керованість, але потребує глибшого розуміння системи для налаштування безпеки.

Незалежно від ОС, є спільні принципи захисту:

- встановлення лише перевірених програм;
- регулярні оновлення;
- обмеження прав доступу;
- використання паролів та шифрування.

ЗАВДАННЯ. Заповни таблицю. Уяви, що ти консультант з кібербезпеки. Тобі потрібно дати базові рекомендації для захисту комп'ютерів на різних ОС. Заповни таблицю, вказавши по 2 ключові поради для кожної системи.

Операційна система	Порада 1	Порада 2
Windows		
macOS		
Linux		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: У школі використовуються комп'ютери з Windows та Linux. У деяких користувачів Windows з'явились підозрілі спливаючі вікна та зникли файли. У той час один із комп'ютерів на Linux підключився до шкільної мережі без жодної перевірки. З'ясувалось, що захист мережі був слабким, а ОС не оновлювались вчасно.

Запитання для роздумів:
Які помилки були допущені при роботі з обома ОС?
Які заходи захисту потрібно було вжити заздалегідь?
Чи варто було мати різні правила для різних ОС?

Нотатки _____

ТЕМА 16: ЗАХИСТ МОБІЛЬНИХ ПРИСТРОЇВ

Мобільні пристрої зберігають особисті дані, листування, паролі, банківську інформацію. Вони постійно підключені до мережі, а тому потребують особливої уваги до безпеки. Основні загрози: шкідливі додатки, фішинг через месенджери, незахищені Wi-Fi, відсутність блокування екрана або оновлень.

Щоб захистити пристрій:

- використовуй блокування екрану (PIN, біометрія);
- не встановлюй додатки поза офіційними магазинами;
- регулярно оновлюй систему;
- активуй «Знайти пристрій»;
- користуйся VPN у відкритих мережах.

ЗАВДАННЯ. Заповни таблицю. Познач, чи виконано кожен пункт. Якщо ні — постав собі нагадування.

Дія	Виконано? (✓ / ✗)
Установлено PIN або біометрію	
Увімкнено автоматичне оновлення	
VPN для публічного Wi-Fi	
Додатки лише з офіційного магазину	
Увімкнено функцію «Знайти пристрій»	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Студент встановив застосунок для розпізнавання музики з невідомого сайту. Після цього пристрій почав повільно працювати, у месенджері з'явилися повідомлення, яких він не писав. Він також підключався до безкоштовного Wi-Fi у кав'ярні без VPN.

Запитання для роздумів:

Які ризики проявились?
Що потрібно змінити у поведінці користувача?
Які налаштування варто перевірити?

Нотатки _____

ТЕМА 17: ЗАХИСТ IOT-ПРИСТРОЇВ

IoT-пристрої — це будь-які «розумні» пристрої, підключені до інтернету: камери відеоспостереження, фітнес-браслети, смарт-лампи, телевізори, домашні асистенти тощо. Вони зручні, але часто мають слабкий захист. Основні ризики: стандартні паролі, відсутність оновлень, незашифровані підключення, відкритий доступ до керування. Зламаний IoT-пристрій може бути використаний для стеження, атак або контролю над іншими системами.

Базові поради:

- змінюй стандартні паролі;
- відключай ті пристрої, які не використовуєш;
- оновлюй прошивку;
- використовуй окрему мережу Wi-Fi для IoT;
- слідкуй, які додатки мають доступ до пристроїв.

ЗАВДАННЯ. Заповни таблицю. Познач, які з дій ти вже виконуєш (або можеш виконати вдома).

Дія	Так / Ні
У всіх пристроях змінено стандартний пароль	
Створено окрему Wi-Fi мережу для “розумних” пристроїв	
Увімкнено автоматичні оновлення прошивки	
Смарт-камери не доступні ззовні без авторизації	
Усі додатки для керування завантажено з офіційних магазинів	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: У класі використовувалась смарт-дошка, підключена до інтернету. Учитель залишив стандартний пароль. Через кілька днів на екрані почали з’являтись сторонні повідомлення. Виявилось, що доступ до пристрою отримав сторонній користувач.

Запитання для роздумів:

Що було зроблено неправильно?

Які кроки потрібно зробити для захисту пристрою?

Як уникнути подібної ситуації в майбутньому?

Нотатки _____

ТЕМА 18: ЗАХИСТ ДАНИХ ДІТЕЙ В ІНТЕРНЕТІ

Діти активно користуються інтернетом — соцмережами, онлайн-іграми, навчальними платформами. Проте вони часто не усвідомлюють, які дані про них збираються і хто їх бачить. Особливо вразливими є: ім'я, вік, фото, місцезнаходження, повідомлення, поведінкові звички.

Основні ризики:
розголошення особистої інформації незнайомцям;
публікація фото без згоди батьків;
ігри та застосунки, що відстежують активність;
фішинг і маніпуляції в соцмережах.

Захист починається з довіри та знань:
- навчайте дитину не публікувати особисте;
- використовуйте налаштування приватності;
- встановлюйте батьківський контроль;
- оновлюйте програми;
- слідкуйте, до яких сайтів і сервісів має доступ дитина.

ЗАВДАННЯ. Заповни таблицю. Оціни дії — які з них безпечні, а які потребують уваги. Познач ✓ або ✗. Поясни, якщо ✗.

Дія	✓ / ✗	Пояснення
Дитина публікує фото з табору у відкритому профілі		
Налаштовано "лише для друзів" у соцмережах		
У грі вказано справжнє ім'я та вік		
Встановлено батьківський контроль у браузері		
Онлайн-опитування з питаннями про сім'ю		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: 12-річна Софія створила відкритий профіль у соцмережі, де публікує фото, пише про школу та місця, де буває. До неї почали писати незнайомці. Один із них представився підлітком, запропонував перейти в інший месенджер і почав просити особисті фото.

Запитання для роздумів:
У чому загроза?
Як правильно пояснити дитині, що сталося?
Які налаштування потрібно змінити?

Нотатки _____

ТЕМА 19: ОСНОВИ БЕЗПЕКИ МЕРЕЖ

Безпека мереж — це сукупність заходів, спрямованих на захист комп'ютерних мереж від несанкціонованого доступу, атак, крадіжки даних і збоїв у роботі.

Ключові елементи безпеки мереж:
Межові пристрої: маршрутизатори, брандмауери.
Засоби контролю доступу: обмеження доступу до ресурсів мережі.
Шифрування трафіку: захист передаваних даних.
Сегментація мережі: поділ мережі на ізольовані зони для підвищення безпеки.
Моніторинг та аудит мережевого трафіку: виявлення підозрілої активності.

Типові загрози для мереж:

- Несанкціонований доступ (хакинг).
- Атаки типу DDoS (розподілені атаки на відмову в обслуговуванні).
- Перехоплення даних (Sniffing).
- Впровадження шкідливого програмного забезпечення через мережу.

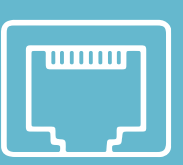
ЗАВДАННЯ. Заповни таблицю. У кожному випадку опиши, яка проблема існує в організації мережі, та запропонуй рішення.

Ситуація	У чому проблема?	Як це виправити?
Усі пристрої в мережі мають однаковий пароль доступу до роутера		
В офісі не використовується жоден брандмауер		
Wi-Fi мережа не має пароля, і не відслідковується, хто підключається		
Співробітники мають повний доступ до всіх частин мережі		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Компанія не використовувала брандмауер для захисту своєї мережі. Одного дня зловмисники змогли отримати доступ до внутрішніх даних, скориставшись незахищеним портом.

Запитання для роздумів:
Яких заходів безпеки бракувало?
Як можна було попередити цю атаку?
Чому регулярний моніторинг мережевого трафіку важливий?



Нотатки _____

ТЕМА 20: РОЛЬ БЕЗПЕЧНОЇ ПОВЕДІНКИ В МЕРЕЖІ

Безпечна поведінка в мережі — це дотримання правил, які мінімізують ризики втрати даних, шахрайства, зараження пристроїв вірусами або втручання в особисту інформацію.

Основні принципи безпечної поведінки:

Не відкривати підозрілі посилання і файли.
Використовувати унікальні складні паролі для різних сервісів.
Регулярно оновлювати операційні системи та програми.
Не розголошувати особисту інформацію у відкритому доступі.
Використовувати антивірус і активувати багатофакторну автентифікацію.
Підтверджувати достовірність отриманих повідомлень і запитів.

Типові помилки користувачів у мережі:

- Користування одним і тим самим паролем на багатьох сайтах.
- Завантаження програм із неперевірених джерел.
- Ігнорування оновлень програмного забезпечення.
- Безконтрольне розміщення особистих даних у соцмережах.

ЗАВДАННЯ. Заповни таблицю. Позначте дії, які є прикладами безпечної поведінки в інтернеті. Обґрунтуйте вибір.

Поведінка	Безпечно (☑)	Чому? (коротко)
Вхід у соцмережу через відкриту Wi-Fi мережу без VPN		
Регулярне оновлення паролів до важливих сервісів		
Використання одного і того ж пароля всюди		
Перевірка адреси сайту перед введенням даних		
Прийняття всіх файлів від незнайомців у месенджері		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Анастасія використовувала той самий пароль для електронної пошти та соціальних мереж. Після того як один із сайтів був зламаний, зловмисники отримали доступ до всіх її облікових записів.

Запитання для роздумів:

Якої помилки припустилася Анастасія?
Як уникнути подібних ситуацій у майбутньому?
Які правила допомагають захистити свої облікові записи?

ТЕМА 21: ОСНОВИ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ WI-FI

Wi-Fi — це технологія бездротового зв'язку, яка дозволяє пристроям підключатися до інтернету або локальної мережі без використання кабелів.

Чому безпека Wi-Fi важлива:
Бездротові мережі можуть бути легше перехоплені зловмисниками. Несанкціонований доступ може призвести до крадіжки даних, використання вашого інтернету або зламу пристроїв.

Основні загрози для Wi-Fi мереж:
Перехоплення трафіку (Sniffing).
Підключення неавторизованих користувачів.
Атаки типу «злий двійник» (створення підробленої мережі з ідентичним ім'ям).

Заходи безпеки для захисту Wi-Fi:
- Використання сильного пароля для мережі.
- Активація WPA3 або WPA2 шифрування (застаріле WEP — небезпечне).
- Вимкнення широкого транслювання імені мережі (SSID), якщо це можливо.
- Обмеження доступу за MAC-адресами пристроїв.
- Регулярне оновлення прошивки маршрутизатора.

ЗАВДАННЯ. Заповни таблицю. Прочитай опис мережі та визнач, які налаштування потребують покращення. Запропонуй безпечні альтернативи.

Поточне налаштування	Проблема	Що змінити або додати
Пароль: 12345678		
Тип шифрування: WEP		
Назва мережі (SSID): public-wifi		
Адміністративна панель доступна без пароля		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Іван встановив Wi-Fi у своєму домі, але залишив стандартний пароль, встановлений виробником. Через деякий час його мережу використали для розсилки спаму.

Запитання для роздумів:
Якої помилки припустився Іван?
Як правильно налаштувати безпечну Wi-Fi мережу?
Чому небезпечно залишати стандартні налаштування?

ТЕМА 22: БРАНДМАУЕРИ ТА ЇХ РОЛЬ У ЗАХИСТІ

Брандмауер (Firewall) — це програмний або апаратний засіб, який контролює вхідний та вихідний мережевий трафік на основі визначених правил безпеки.

Основні функції брандмауера:
Фільтрація трафіку: пропускання або блокування даних залежно від заданих правил.
Захист від зовнішніх атак: блокування спроб несанкціонованого доступу.
Контроль доступу: визначення, які пристрої та сервіси можуть з'єднуватися з мережею.
Моніторинг активності: ведення журналів мережевої активності для подальшого аналізу.

Типи брандмауерів:
- Мережеві брандмауери: захищають локальні мережі.
- Особисті брандмауери: встановлюються на окремі пристрої (ноутбуки, ПК).
- Апаратні брандмауери: окремі пристрої, що контролюють трафік між мережами.
- Хмарні брандмауери: захищають сервіси в інтернеті.

ЗАВДАННЯ. Заповни таблицю. Завдання на налаштування брандмауера. Уяви, що ти відповідаєш за базове налаштування брандмауера в офісній мережі. Заповни таблицю, обґрунтувавши свої дії.

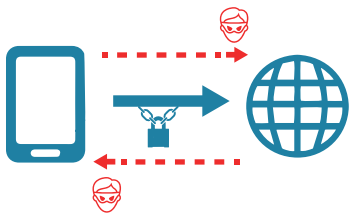
Ситуація	Дозволити чи Заборонити?	Чому?
Вхідні з'єднання з невідомих IP-адрес		
Доступ до внутрішнього принтера з локальної мережі		
З'єднання з портом 21 (FTP) з Інтернету		
Вихідний доступ співробітників до електронної пошти		

КЕЙС ДЛЯ АНАЛІЗУ
Ситуація: Підприємство під'єднало свою корпоративну мережу напряму до інтернету без налаштування брандмауера. Через деякий час мережа зазнала несанкціонованого доступу і витоку важливих даних

Запитання для роздумів:
Яких заходів безпеки бракувало?
Як міг допомогти брандмауер у цій ситуації?
Який тип брандмауера варто було б використати для корпоративної мережі?

ТЕМА 23: VPN: ПРИНЦИП РОБОТИ ТА ВИКОРИСТАННЯ

VPN (Virtual Private Network) — це технологія створення захищеного каналу зв'язку поверх публічних мереж (наприклад, Інтернету), що забезпечує конфіденційність і безпеку передаваних даних.



Основні принципи роботи VPN:

Шифрування даних: усі дані, що передаються через VPN, зашифровані.

Тунелювання: створення захищеного «тунелю» між пристроєм користувача і сервером VPN.

Приховування IP-адреси: реальна IP-адреса користувача маскується, що забезпечує анонімність.

Переваги використання VPN:

- Захист при використанні публічних Wi-Fi мереж.
- Обхід географічних обмежень доступу до ресурсів.
- Підвищення рівня конфіденційності в мережі.
- Захист від перехоплення трафіку.

ЗАВДАННЯ. Заповни таблицю. Оціни кожну ситуацію та вкажи, чи потрібно використовувати VPN. Поясни чому.

Ситуація	Потрібен VPN? (Так/Ні)	Чому?
Користувач працює з конфіденційними документами через публічний Wi-Fi		
Перегляд новин на локальному сайті з домашнього Wi-Fi		
Підключення до внутрішньої корпоративної мережі з-за кордону		
Відкриття електронної пошти через перевірений домашній ПК		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Катерина працювала у кав'ярні, підключившись до відкритої Wi-Fi мережі без використання VPN. Через деякий час її облікові записи в соцмережах були зламані.

Запитання для роздумів:

Які ризики пов'язані з відкритими мережами без VPN?

Як VPN допоміг би уникнути цієї ситуації?

Які ще заходи безпеки варто застосовувати під час роботи в публічних мережах?

ТЕМА 24: МЕРЕЖЕВІ ПРОТОКОЛИ БЕЗПЕКИ

Мережеві протоколи безпеки — це стандарти, які забезпечують **захист даних під час передавання через інтернет** або локальні мережі. Вони потрібні для шифрування, автентифікації, цілісності інформації та захисту від атак.

Найпоширеніші протоколи:

- **HTTPS** — шифрує з'єднання між браузером і сайтом, захищає від перехоплення.
- **SSL / TLS** — основа HTTPS, відповідає за безпечну передачу даних.
- **VPN** (наприклад, OpenVPN, IPSec) — створює зашифрований "тунель" між пристроєм і сервером.
- **WPA2 / WPA3** — використовуються для захисту Wi-Fi мереж.
- **SSH** — безпечне віддалене підключення до серверів.

Ці протоколи дозволяють уникати фішингу, MITM-атак (атаки "людина посередині") та захищати особисту інформацію.

ЗАВДАННЯ. Заповни таблицю. З'єднай протокол із його функцією.

Протокол	Функція
HTTPS	
VPN	
SSH	
WPA3	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Під час підключення до відкритої Wi-Fi у кафе користувач не помітив, що веб-сайт не використовував HTTPS. Він увів пароль, після чого з облікового запису почали надсилатися підозрілі листи.
З'ясувалося, що дані перехоплено через атаку "людина посередині".

Запитання для роздумів:
Чому використання HTTPS могло запобігти цьому?
Як діяти в публічних мережах?
Яку роль могли би зіграти VPN або WPA3?

Нотатки _____

ТЕМА 25: ВИКОРИСТАННЯ БЛОКЧЕЙНУ ДЛЯ БЕЗПЕКИ

Блокчейн — це розподілений реєстр, у якому інформація зберігається у вигляді послідовних блоків, що зв'язані між собою і захищені криптографією. Найвідоміше застосування — криптовалюти, але технологію також використовують для забезпечення довіри, незмінності та прозорості в інших сферах.

Блокчейн сприяє безпеці завдяки:
неможливості змінити збережену інформацію без згоди мережі;
відсутності єдиного центру управління — складніше зламати систему;
публічності або контрольованій прозорості — всі бачать зміни;
криптографії — інформація захищена математично.

Сфери застосування для безпеки:
- електронні голосування;
- верифікація особи без передачі паролів;
- збереження журналів змін у системах без можливості фальсифікації;
- захист авторських прав.

ЗАВДАННЯ. Заповни таблицю. Вибери, для чого може використовуватись блокчейн. Познач ✓ або ✗. Поясни, якщо ✗.

Протокол	✓ / ✗	Пояснення
Захист особистих даних у хмарі		
Контроль за оновленням антивіруса		
Реєстрація авторських прав		
Моніторинг дій в адміністративній системі		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: У системі внутрішнього документообігу державної установи зникли записи про зміну файлів. Після впровадження блокчейн-реєстру для фіксації змін кожне редагування почало зберігатися як окремий блок із датою, автором і хешем. Виявлення несанкціонованих змін стало простішим, адже їх не можна було стерти або підробити.

Запитання для роздумів:
Яку функцію тут виконує блокчейн?
Як ця система підвищує рівень безпеки?
У яких ще випадках подібне рішення може бути корисним?

Нотатки _____

ТЕМА 26: ОСНОВИ МОНІТОРИНГУ ТА ВИЯВЛЕННЯ ЗАГРОЗ У МЕРЕЖІ

Моніторинг мережі — це процес постійного спостереження за активністю мережі для виявлення проблем, збоїв або підозрілої діяльності.
Виявлення загроз — це ідентифікація спроб вторгнення, аномалій або шкідливої активності у мережевому трафіку.

Основні цілі моніторингу:
Виявлення підозрілої активності у реальному часі.
Запобігання вторгненням та атакам.
Оцінка ефективності заходів безпеки.
Реагування на інциденти безпеки.

Основні інструменти моніторингу і виявлення загроз:
IDS (Intrusion Detection System) — система виявлення вторгнень.
IPS (Intrusion Prevention System) — система запобігання вторгнень.
SIEM (Security Information and Event Management) — рішення для збору і аналізу подій безпеки.
Пакетні аналізатори (наприклад, Wireshark) — інструменти для детального аналізу трафіку.

Типові ознаки загроз у мережі:
- Незвичні обсяги трафіку.
- Підозрілі спроби входу до системи.
- Нетипові з'єднання із зовнішніми IP-адресами.
- Часті помилки автентифікації.

ЗАВДАННЯ. Заповни таблицю. Поєднайте інструмент і його призначення:

Інструмент	Призначення
IDS	
SIEM	
Пакетний аналізатор	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: У корпоративній мережі почали помічати значне збільшення трафіку в неробочий час. При перевірці виявилось, що зловмисник отримав доступ до одного з серверів і почав передавати дані за кордон.

Запитання для роздумів:
Які інструменти могли б допомогти вчасно виявити загрозу?
Які ознаки повинні були насторожити адміністратора мережі?
Які дії потрібно виконати для запобігання подібним інцидентам у майбутньому?

ТЕМА 27: АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ

Мережевий трафік — це всі дані, які передаються в комп'ютерній мережі. Аналіз цього трафіку дозволяє виявити підозрілу активність, наприклад: спроби вторгнення, розсилку вірусів, крадіжку даних або роботу ботнетів.

Як це працює:

- Спочатку фіксуються всі з'єднання, адреси, обсяги переданих даних.
- Далі аналізуються незвичні шаблони поведінки: багато запитів за короткий час, з'єднання з невідомими серверами, нестандартні порти.
- На основі цього можна визначити загрози — як активні (атака), так і приховані (шкідливе ПЗ).

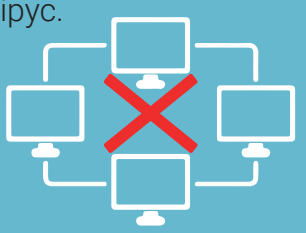
Інструменти: Wireshark, NetFlow, IDS/IPS (системи виявлення загроз). Аналіз можуть виконувати як спеціалісти, так і автоматизовані системи (SIEM).

ЗАВДАННЯ. Заповни таблицю. Познач, яка поведінка в мережі виглядає підозрілою. Якщо підозріла — поясни чому.

Поведінка	✓ / ✗	Пояснення
Користувач підключається до 5 сайтів за хвилину		
Один комп'ютер надсилає трафік на 1000 IP-адрес		
Усі з'єднання йдуть через порт 443 (HTTPS)		
З локального принтера надходить багато DNS-запитів		
Обсяг завантаження — 50 ГБ за ніч		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Під час моніторингу мережі у школі було виявлено, що один із комп'ютерів щохвилини підключається до різних IP-адрес у різних країнах. Обсяг вхідного трафіку значно перевищує вихідний. На комп'ютері не було оновлено антивірус.



Запитання для роздумів:

Яка загроза могла виникнути?

Які дії потрібно зробити адміністратору?

Як подібні інциденти виявляються автоматично?

Нотатки _____

ТЕМА 28: ВИКОРИСТАННЯ СИСТЕМ IDS/IPS

Системи IDS (Intrusion Detection System) та IPS (Intrusion Prevention System) — це інструменти для **виявлення та запобігання вторгненням у мережу.**

- **IDS** — система виявлення атак. Вона аналізує трафік, фіксує підозрілу активність, повідомляє адміністратора, але не втручається.
- **IPS** — система запобігання атак. Вона не лише виявляє, а й блокує підозрілі дії в реальному часі.

Обидві системи:

- аналізують мережеві пакети;
- використовують базу відомих загроз (сигнатури);
- можуть використовувати поведінковий аналіз;
- інтегруються з іншими інструментами безпеки.

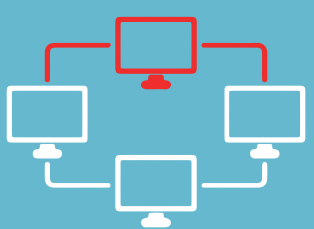
Різниця в реакції:
IDS → виявляє → повідомляє
IPS → виявляє → блокує

ЗАВДАННЯ. Заповни таблицю. Вкажи, що краще використати у ситуації — IDS, IPS або обидва.

Ситуація	IDS / IPS / Обидва
Моніторинг комп'ютерного класу без втручання	
Захист серверу від несанкціонованого доступу	
Навчання з кібербезпеки, де аналізуються атаки	
Автоматичне блокування DDoS	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: На навчальному сервері спостерігається незвично велика кількість з'єднань з IP-адреси, яка не належить жодному користувачу. IDS виявила спробу сканування портів, але нічого не блокувала. Через годину спроба повторилась, цього разу з атаками на авторизацію.



Запитання для роздумів:
Як IDS допомогла?
Чому її було недостатньо?
Як би діяла IPS у цій ситуації?

Нотатки _____

ТЕМА 29: СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА ЇЇ НЕБЕЗПЕКИ

Соціальна інженерія — це методика маніпулювання людьми для отримання конфіденційної інформації або доступу до систем без застосування технічних засобів злому.

Чому соціальна інженерія небезпечна:

Використовує психологічні слабкості людей.

Може обійти навіть найкращі технічні засоби захисту.

Часто залишається непоміченою до моменту заподіяння шкоди.

Типові ознаки спроб соціальної інженерії:

- Несподівані повідомлення з проханням надати особисті дані.
- Вимоги діяти терміново або під тиском.
- Пропозиції виграшів, призів або фінансових винагород.

ЗАВДАННЯ. Заповни таблицю. Завдання на розпізнавання ситуацій. Визначте, чи є ознака соціальної інженерії в наступних прикладах:

Приклад	Так / Ні
Отримання листа із проханням терміново змінити пароль за посиланням	
Отримання SMS із кодом для активації виграшу в лотереї	
Вхід на офіційний сайт банку через пряме посилання з власноручного введення адреси	
Отримання дзвінка від «служби підтримки», яка вимагає надати пароль	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Петро отримав дзвінок від людини, яка представилася працівником служби безпеки банку. Йому повідомили про підозрілу активність на рахунку та попросили назвати код підтвердження, надісланий SMS-повідомленням.

Запитання для роздумів:

Який тип атаки застосовано?

Як повинен був діяти Петро у цій ситуації?

Які правила слід пам'ятати під час спілкування з невідомими особами?

Нотатки _____

ТЕМА 30: МЕТОДИ ЗАХИСТУ ВІД СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Соціальна інженерія — це метод обману, спрямований не на комп'ютер, а на людину. Але як захистити себе?

Основна відповідь — **усвідомленість, обережність і практика реагування.**

Найефективніші методи захисту:

- **Цифрова гігієна:** не відкривай підозрілі посилання, не пиши пароль у чат, не ділись кодом підтвердження.
- **Мислення з недовірою:** перевіряй, хто пише — навіть знайомі акаунти можуть бути зламані.
- **Двофакторна автентифікація:** навіть якщо пароль вкрадено, доступ не отримають.
- **Навички перевірки фактів:** розпізнавання фейкових новин, маніпуляцій, фішингових шаблонів.
- **Внутрішня політика в організаціях:** інструкції, хто має право просити доступ або дані.

Захист — це не лише про заборони, а про **звички мислити критично** та **ставити питання.**

ЗАВДАННЯ. Заповни таблицю. Познач, які дії ти вже виконуєш або вважаєш важливими.

Дія	Так / Ні
Ніколи не надсилаю коди з SMS іншим людям	
Завжди перевіряю URL перед тим як клікнути	
Якщо щось здається підозрілим — питаю поради	
Маю MFA для важливих сервісів	
Знаю, як виглядає типова фішинг-атака	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Студент отримав листа, нібито від адміністратора університету, з проханням перейти за посиланням і оновити облікові дані. Він помітив дивну адресу відправника й звернувся до техпідтримки. Виявилось, це була спроба фішингу.

Запитання для роздумів:

Які дії були правильні?

Як міг діяти студент необачно?

Які ознаки допомогли розпізнати загрозу?

Нотатки _____

_____

ТЕМА 31: ОСНОВИ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Кіберінцидент — це порушення політики безпеки інформаційних систем, яке може призвести до компрометації даних, збоїв у роботі систем або втрати інформації.

Типові приклади кіберінцидентів:
Несанкціонований доступ до системи.
Витік конфіденційних даних.
Атаки програм-вимагачів.
Масові фішингові кампанії.
DDoS-атаки на вебресурси.

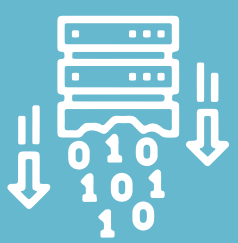
Етапи реагування на кіберінциденти:
1. Виявлення — ідентифікація аномальної діяльності або порушення безпеки.
2. Аналіз — оцінка масштабу і впливу інциденту.
3. Стримування — локалізація інциденту для запобігання подальшому поширенню.
4. Усунення — видалення причин інциденту (наприклад, шкідливого ПЗ).
5. Відновлення — повернення систем до нормальної роботи.
6. Аналіз наслідків і поліпшення — розробка заходів для запобігання подібним інцидентам у майбутньому.

ЗАВДАННЯ. Заповни таблицю. Прочитай опис ситуації і вкажи, чи це кіберінцидент. Якщо так — запропонуй перший крок реагування.

Ситуація	Це інцидент? (Так / Ні)	Що робити першим?
Сайт компанії недоступний без пояснень		
Співробітник випадково надіслав клієнтські дані не туди		
Користувач не може ввійти до акаунту через неправильний пароль		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: В організації виявили спробу несанкціонованого доступу до бази даних клієнтів. Спочатку подію проігнорували, і лише після витоку даних почали вживати заходів.

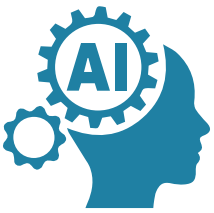


Запитання для роздумів:
Яка помилка була допущена під час реагування на інцидент?
Який етап реагування був проігнорований?
Як варто було діяти для мінімізації шкоди?

Нотатки _____

ТЕМА 32: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МОНІТОРИНГУ ЗАГРОЗ

Штучний інтелект (ШІ) дедалі активніше застосовується для виявлення та моніторингу кіберзагроз. Завдяки здатності аналізувати великі обсяги даних і виявляти аномалії, ШІ допомагає реагувати на атаки швидше, ніж людина.



Основні переваги:
Автоматичне виявлення аномалій: система бачить відхилення від звичайної поведінки.
Навчання на прикладах атак: моделі ШІ вчаться розпізнавати загрози.
Цілодобовий моніторинг: постійна перевірка трафіку, логів, дій користувачів.
Прогнозування ризиків: оцінка, де ймовірно виникне атака.

Використовується в:
- SIEM-системах (моніторинг подій);
- XDR/EDR-рішеннях;
- інтелектуальних фільтрах спаму, фішингу, ботів.

ЗАВДАННЯ. Заповни таблицю. Познач, чи є твердження правильним. Якщо міф — поясни.

Твердження	Міф / Правда	Пояснення
ШІ завжди реагує точно		
ШІ не може працювати без навчання		
ШІ розпізнає всі типи атак		
ШІ може помилково заблокувати легальну дію		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Компанія встановила систему з ШІ для аналізу логів. Через тиждень система попередила про аномальну активність: користувач увійшов у незвичний час із нової країни та завантажив велику кількість файлів. Перевірка показала витік службової документації.

Запитання для роздумів:
Яку роль зіграв ШІ у виявленні інциденту?
Як діяти при подібному сповіщенні?
Які ризики є у використанні ШІ (наприклад, хибні спрацювання)?

Нотатки _____

ТЕМА 33: ОСНОВНІ АСПЕКТИ КІБЕРБЕЗПЕКИ В ОРГАНІЗАЦІЯХ

Організація — це не лише техніка, а й люди, політики, процеси. Кібербезпека в організаціях охоплює всі рівні: від пароля працівника до інфраструктури серверів.

Ключові аспекти:

- Політика безпеки: чіткі правила доступу, оновлення, використання пристроїв, збереження даних.
- Навчання персоналу: обізнаність про фішинг, соціальну інженерію, роботу з конфіденційною інформацією.
- Розмежування прав доступу: кожен працівник має доступ лише до потрібного.
- Захист мереж і пристроїв: антивірус, брандмауер, VPN, резервне копіювання.
- Реагування на інциденти: плани дій у разі витоку, зламу чи збою.
- Дотримання законодавства: зокрема про захист персональних даних.

Безпека організації — це системна робота, а не одноразове рішення.

ЗАВДАННЯ. Заповни таблицю. Познач твердження як ✓ (правильно) або ✗ (неправильно). Поясни, якщо ✗.

Твердження	✓ / ✗	Пояснення
Працівники мають доступ лише до потрібних їм файлів		
Політика безпеки створюється один раз і не змінюється		
Резервні копії зберігаються у тій самій мережі, що й оригінали		
Усі користувачі проходять навчання з кібергігієни		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: У невеликій компанії один із працівників випадково надав хакерам доступ, ввівши пароль у фішинговій формі. Компанія не мала політики безпеки й не проводила навчання. Дані клієнтів були викрадені, а роботу систем — порушено.

Запитання для роздумів:

Що можна було зробити наперед?

Які аспекти захисту були проігноровані?

Як організація має змінити свою політику після інциденту?

Нотатки _____

ТЕМА 34: РОЗРОБКА ПОЛІТИКИ КІБЕРБЕЗПЕКИ

Політика кібербезпеки — це **офіційний документ** в організації, що визначає, **як захищати інформацію, системи та користувачів.** Вона — як дорожня карта: пояснює, хто за що відповідає, які правила діють і що робити у разі загрози.

Основні розділи політики:

- Цілі та сфера дії: кого і що охоплює;
- Ролі та відповідальність: хто що контролює;
- Керування доступом: хто має до чого доступ і як;
- Захист даних: резервне копіювання, шифрування, обробка персональних даних;
- Реагування на інциденти: хто і як діє;
- Навчання та перевірки: як підтримувати обізнаність;
- Оновлення та перегляд: документ не має бути “вічним”.

Політика — не “для галочки”, а щоденний інструмент, що допомагає зменшити ризики і діяти злагоджено.

ЗАВДАННЯ. Заповни таблицю. Познач, які елементи повинні бути в політиці кібербезпеки. Якщо ні — поясни, чому.

Елемент	✓ / ✗	Пояснення
Перелік святкових днів		
Опис рівнів доступу до систем		
Інструкція з дій у разі виявлення підозрілої активності		
Правила використання власних пристроїв (BYOD)		
Контакти керівника відділу кадрів		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Організація мала проблеми з витоками інформації, але не мала жодної письмової політики. Після інциденту створили документ, у якому чітко описали рівні доступу, дії у разі фішингу та регулярні інструктажі. Витоки припинились.

Запитання для роздумів:

Які частини політики могли змінити ситуацію?
Хто має слідкувати за виконанням політики?
Чому недостатньо просто мати документ?

Нотатки _____

ТЕМА 35: УПРАВЛІННЯ РИЗИКАМИ В КІБЕРБЕЗПЕЦІ

Управління ризиками — це **процес виявлення, оцінки та реагування на загрози,** які можуть вплинути на інформаційні системи, дані чи репутацію організації.
Завдання — **не усунути всі ризики, а зменшити їх до прийнятного рівня.**

Ключові етапи:
Ідентифікація ризиків: що може статися? (наприклад, витік даних, злам, збій);
Оцінка впливу та ймовірності: наскільки серйозний ризик і як часто може трапитись;
Пріоритезація: які ризики критичні, а які можна тимчасово прийняти;
План реагування: уникати, зменшувати, передавати або приймати ризик;
Моніторинг і перегляд: ризики змінюються — політика теж.

Інструменти:
- Матриці ризиків;
- Журнали інцидентів;
- Політика резервного копіювання;
- Контроль доступу;
- Навчання персоналу.

ЗАВДАННЯ. Заповни таблицю. Оціни ризики в таблиці та впиши рівень (низький / середній / високий) і рекомендовану дію.

Ризик	Рівень	Дія
Співробітник використовує той самий пароль усюди		
Сервери не мають резервного копіювання		
Фішингові листи надходять щотижня		
Немає плану реагування на атаки		
Дані зберігаються на особистих пристроях		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: У навчальному закладі стався злам облікових записів викладачів через повторне використання паролів. Це призвело до підміни результатів навчання. Виявилось, що ризик був задокументований, але не оцінений як пріоритетний, і не було вжито заходів.

Запитання для роздумів:
Який тип ризику реалізувався?
Що було пропущено на етапі оцінки?
Як діяти після інциденту?

ТЕМА 36: ЮРИДИЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ

Кібербезпека — це не лише про технології, а й про **законодавство**. Воно визначає, **що дозволено, що заборонено і яка відповідальність настає** у разі порушення правил у цифровому просторі.

Ключові поняття:
Персональні дані — будь-яка інформація, що дозволяє ідентифікувати особу. Їх збір, зберігання та обробка мають здійснюватись з дозволу користувача.
Кіберзлочини — злам акаунтів, фішинг, розповсюдження вірусів, атаки на системи — усе це кримінальні порушення.
Відповідальність — може бути адміністративною, цивільною або кримінальною, залежно від шкоди.
Законодавство в Україні:
– Закон «Про захист персональних даних»
– Закон «Про захист інформації в інформаційно-телекомунікаційних системах»
– Статті Кримінального кодексу України (361–363¹)
У ЄС діє **GDPR**, який встановлює жорсткі правила обробки персональної інформації.

ЗАВДАННЯ. Заповни таблицю. Познач, що відповідає нормам законодавства.
Якщо ✗ — поясни, чому.

Дія	✓ / ✗	Пояснення
Студент опублікував дані з чужого акаунта без дозволу		
Компанія запитує згоду на обробку персональних даних		
Використання фото з особою без її дозволу в соцмережах		
Працівник ІТ-кафедри створив резервну копію журналів оцінювання		
Організація не повідомила про витік даних клієнтів		

КЕЙС ДЛЯ АНАЛІЗУ
Ситуація: У школі було встановлено систему відеоспостереження, однак учнів і батьків про це не повідомили. Коли один із записів потрапив у соцмережі, частина батьків звернулась до уповноважених органів через порушення їхніх прав.

Запитання для роздумів:
Яке законодавство було порушено?
Які права було порушено?
Як мала діяти школа до і після встановлення камер?

ТЕМА 37: ОСНОВИ КРИПТОГРАФІЇ

Криптографія — це наука про методи захисту інформації шляхом її шифрування, щоб тільки уповноважені особи могли її прочитати.

Основні цілі криптографії:
Конфіденційність: тільки уповноважені особи мають доступ до інформації.
Цілісність: дані не змінені у процесі передачі чи зберігання.
Автентичність: підтвердження, що дані надійшли від заявленого джерела.
Незаперечність: відправник не може заперечити факт надсилання даних.

Ключові поняття криптографії:
Шифрування: перетворення відкритого тексту у зашифрований вигляд.
Дешифрування: відновлення оригінального тексту із зашифрованого.
Ключі шифрування: секретні дані, які використовуються для шифрування і дешифрування.

Види шифрування:
- Симетричне шифрування: використовується один ключ для шифрування і дешифрування.
- Асиметричне шифрування: використовується пара ключів — публічний і приватний.

ЗАВДАННЯ. Заповни таблицю. Поєднайте поняття з його описом:

Твердження	Опис
Шифрування	
Дешифрування	
Публічний ключ	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Компанія передавала важливі контракти електронною поштою без шифрування. У результаті сторонні особи змогли перехопити і змінити зміст документів.

Запитання для роздумів:
Яких заходів безпеки бракувало?
Як використання криптографії могло б запобігти інциденту?
Який тип шифрування був би найбільш доречним у цій ситуації?

*****

Нотатки _____

ТЕМА 38: ОСНОВИ ЦИФРОВИХ ПІДПИСІВ

Цифровий підпис — це криптографічний механізм, який підтверджує справжність та цілісність електронних даних.

Функції цифрового підпису:
Підтвердження авторства: гарантує, що дані створені конкретною особою.
Цілісність даних: підтверджує, що дані не були змінені після підписання.
Незаперечність: підписант не може відмовитися від факту підписання.

Як працює цифровий підпис:
Створюється з використанням приватного ключа підписанта.
Перевіряється за допомогою відповідного публічного ключа.
Зазвичай включає хеш-функцію для фіксації унікального відбитка даних.

Де застосовується цифровий підпис:
- Електронні контракти.
- Підписання електронної пошти.
- Електронні документи та звіти.

ЗАВДАННЯ. Заповни таблицю. Познач, чи є твердження правильним, і коротко поясни чому.

Твердження	Так / Ні	Пояснення
Цифровий підпис гарантує цілісність документа		
Приватний ключ відомий усім учасникам		
Цифровий підпис можна підробити вручну		
Для перевірки підпису потрібен публічний ключ		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Бухгалтерія компанії підписала фінансовий звіт, але згодом виявилося, що документ було змінено сторонньою особою після відправлення.

Запитання для роздумів:
Як використання цифрового підпису могло б запобігти зміні документа?
Чому важливо перевіряти підписи на отриманих документах?
Який ключ використовується для перевірки підпису?

Нотатки _____

ТЕМА 39: ЕЛЕКТРОННА ІДЕНТИФІКАЦІЯ ТА ЕЛЕКТРОННИЙ ПІДПИС В УКРАЇНІ

Електронна ідентифікація — це процес встановлення особи користувача в електронному середовищі за допомогою цифрових засобів.

Що таке електронний підпис в Україні?
В Україні електронний підпис має юридичну силу відповідно до закону «Про електронні довірчі послуги» і прирівнюється до власноручного підпису при певних умовах.

Типи електронних підписів в Україні:
Простий електронний підпис (ПЕП): базовий рівень без спеціальних захистів.
Кваліфікований електронний підпис (КЕП): вищий рівень безпеки, заснований на сертифікованих засобах електронної ідентифікації.
Удосконалений електронний підпис (УЕП): проміжний рівень між ПЕП і КЕП.

Ключові положення українського законодавства:
- КЕП має ту ж юридичну силу, що і власноручний підпис.
- Кваліфіковані довірчі послуги надаються акредитованими центрами сертифікації ключів.
- Електронний підпис може використовуватися для підписання договорів, подання заяв до державних органів тощо.

ЗАВДАННЯ. Заповни таблицю. Порівняй простий, удосконалений і кваліфікований електронний підпис.

Ознака	Простий	Удосконалений	Кваліфікований
Чи має юридичну силу?			
Як створюється?			
Який рівень безпеки?			

КЕЙС ДЛЯ АНАЛІЗУ
Ситуація: Марина вирішила подати податкову декларацію через електронний кабінет, використовуючи простий електронний підпис, але її документи не були прийняті.

Запитання для роздумів:
Чому простого електронного підпису могло бути недостатньо?
Який тип підпису потрібно було використати?
Як Марина могла отримати кваліфікований електронний підпис?

Нотатки _____

ТЕМА 40: ЗАХИСТ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

Електронні комунікації — це обмін повідомленнями через електронні канали, такі як електронна пошта, месенджери, відеоконференції тощо.

Чому потрібно захищати електронні комунікації?
Електронні повідомлення можуть містити конфіденційну інформацію.
Вони можуть бути перехоплені або змінені без відповідного захисту.
Шкідливі атаки (фішинг, підроблені листи) часто використовують електронні канали для розповсюдження.

Основні загрози для електронних комунікацій:
Перехоплення повідомлень.
Фішингові атаки та підробка листів.
Несанкціонований доступ до акаунтів.
Витоки конфіденційної інформації.

ЗАВДАННЯ. Заповни таблицю. Сформулюй правила безпеки для захисту електронних комунікацій.
Заповни таблицю.

Ситуація	Моє правило безпеки
Користування публічною Wi-Fi мережею для листування	
Отримання листа з вкладенням від незнайомця	
Пересилання конфіденційного документа	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Олег отримав лист нібито від свого банку з проханням підтвердити облікові дані, перейшовши за посиланням. Після введення даних він втратив доступ до свого рахунку.

Запитання для роздумів:
Яка атака була здійснена проти Олега?
Як він міг розпізнати фальшивий лист?
Яких правил безпеки потрібно дотримуватися при роботі з електронною поштою?

Нотатки _____

ТЕМА 41: ЗАХИСТ ОСОБИСТОЇ ІНФОРМАЦІЇ В ІНТЕРНЕТІ

Особиста інформація — це будь-які дані, які можуть ідентифікувати особу: ім'я, адреса, телефон, електронна пошта, фото, місцезнаходження, банківські реквізити.
Викрадення особистих даних може призвести до фінансових втрат, крадіжки особистості, шахрайства або порушення приватності.

Основні загрози для особистої інформації в інтернеті:
Фішинг та соціальна інженерія.
Витік даних через незахищені сайти або сервіси.
Використання особистих даних у маркетингових і шахрайських цілях.
Віруси та шкідливе програмне забезпечення.

Заходи для захисту особистої інформації:
- Використання складних і різних паролів для кожного акаунта.
- Мінімізація особистої інформації, що розміщується у відкритому доступі.
- Перевірка налаштувань конфіденційності у соціальних мережах.
- Уважне ставлення до дозволів, які надаються додаткам.
- Регулярне оновлення програмного забезпечення та антивірусного захисту.

ЗАВДАННЯ. Заповни таблицю. Проаналізуй ситуації. Визнач, чи є в них загроза для особистих даних. Якщо є — поясни, у чому вона.

Ситуація	Є загроза? (Так / Ні)	У чому загроза
Користувач публікує фото ID-картки в соцмережі		
Обліковий запис захищено двофакторною автентифікацією		
Особа використовує пароль qwerty123 для всіх сервісів		
GPS-навігація ввімкнена постійно, геолокація доступна		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Андрій публікував багато особистої інформації у відкритому профілі соціальної мережі. Згодом зловмисники використали ці дані для спроб шахрайства від його імені.

Запитання для роздумів:
Які помилки допустив Андрій?
Які налаштування конфіденційності допомогли б уникнути проблеми?
Чому варто обмежувати коло осіб, які мають доступ до особистих даних в інтернеті?

Нотатки _____

ТЕМА 42: ОСНОВИ ЗАКОНОДАВСТВА У СФЕРІ ЗАХИСТУ ДАНИХ

Захист персональних даних — це комплекс заходів, спрямованих на забезпечення конфіденційності, цілісності та безпеки інформації, що стосується фізичних осіб.

Ключові законодавчі акти в Україні:

- Закон України "Про захист персональних даних":

Визначає поняття персональних даних і принципи їх обробки.
Встановлює права суб'єктів даних та обов'язки володільців баз даних.
Регулює передачу даних третім особам.

- Загальний регламент про захист даних (GDPR):

Стосується українських компаній, що працюють з громадянами ЄС.
Передбачає високі стандарти обробки персональної інформації.

Права суб'єктів персональних даних:

- Право на доступ до своїх даних.
- Право на виправлення або видалення даних.
- Право на обмеження обробки або заперечення проти обробки.
- Право на перенесення даних.

ЗАВДАННЯ. Заповни таблицю. "Так / Ні / Поясни"Познач правильність твердження і поясни свою відповідь.

Твердження	Так / Ні	Пояснення
Кожен має право знати, які його дані обробляються		
Закон дозволяє збір персональних даних без згоди		
Організація повинна захищати персональні дані клієнтів		
Шифрування — єдина вимога законодавства		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Інтернет-магазин зберігав особисті дані клієнтів без їхнього згоди та передавав їх рекламним партнерам. Після скарги клієнтів магазин зазнав штрафних санкцій.

Запитання для роздумів:

Яке порушення законодавства допустив магазин?
Які права були порушені?
Як компанії слід організувати обробку персональних даних?

Нотатки _____

ТЕМА 43: ОСНОВИ ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Критична інформаційна інфраструктура — це сукупність інформаційних систем, мереж і ресурсів, порушення або руйнування яких може мати серйозні наслідки для національної безпеки, економіки, охорони здоров'я, громадської безпеки чи добробуту громадян.

Чому важливо захищати КІІ:
Атаки на такі об'єкти можуть паралізувати суспільні процеси.
Порушення роботи КІІ може призвести до значних економічних збитків або навіть загибелі людей.
Захист КІІ є частиною національної безпеки кожної країни.

Основні принципи захисту КІІ:
- Ідентифікація критичних об'єктів і ресурсів.
- Проведення аналізу ризиків і загроз.
- Впровадження заходів захисту (технічних, адміністративних, організаційних).
- Постійний моніторинг і реагування на інциденти безпеки.
- Співпраця між державними структурами, приватним сектором і міжнародними партнерами.

ЗАВДАННЯ. Заповни таблицю. Оціни ситуації і запропонуй відповідну дію з боку фахівця з безпеки.

Ситуація	Що робити?
Виявлено несанкціонований вхід до акаунту	
Отримано повідомлення про витік даних	
Один із комп'ютерів почав розсилати спам	

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Унаслідок кібер-атаки на енергетичну систему міста було знеструмлено кілька районів, що спричинило зупинку лікарень, транспорту та банківських послуг.

Запитання для роздумів:
Чому енергетичні системи вважаються об'єктами КІІ?
Які заходи безпеки могли б зменшити ризик таких інцидентів?
Як важливе оперативне реагування на інциденти в КІІ?

Нотатки _____

ТЕМА 44: ПЛАНУВАННЯ ВІДНОВЛЕННЯ ПІСЛЯ ІНЦИДЕНТІВ

Планування відновлення після інцидентів - це процес підготовки до дій, спрямованих на швидке відновлення нормальної роботи організації після кіберінциденту чи іншої кризи.

Мета планування:
Мінімізувати вплив інцидентів на бізнес-процеси.
Скоротити час простою систем.
Забезпечити захист даних і репутації організації.

Ключові елементи плану відновлення:

- Оцінка ризиків і пріоритизація активів: визначення, які системи критично важливі для роботи.
- Резервне копіювання: регулярне створення копій даних і систем.
- Визначення відповідальних осіб: створення команд із чітко розподіленими обов'язками.
- Сценарії реагування: прописані дії у випадку різних типів інцидентів (наприклад, злам системи, атака програм-вимагачів).
- Тестування плану: регулярні тренування і симуляції для перевірки готовності.

ЗАВДАННЯ. Заповни таблицю. Уяви, що після інциденту потрібно відновити різні сервіси. Обери правильну черговість дій і поясни вибір.

Сервіс	Порядковий номер	Чому саме так?
Система електронної пошти		
Сайт організації		
Внутрішня база даних студентів		
Резервне копіювання		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Після атаки програм-вимагачів організація втратила дані за останні два тижні. Виявилось, що резервні копії створювалися нерегулярно, а план відновлення не тестувався кілька років.

Запитання для роздумів:
Яких заходів не вистачало для ефективного відновлення?
Як визначення RPO допомогло б у цій ситуації?
Чому важливо періодично тестувати план відновлення?

Нотатки _____

ТЕМА 45: ЗАХИСТ ДІТЕЙ В ОСВІТНЬОМУ СЕРЕДОВИЩІ

У цифровому освітньому просторі діти — особливо вразлива категорія. Їхній захист включає **безпеку особистих даних, психологічний комфорт та цифрову обізнаність.**

Ключові напрями захисту:
Конфіденційність: персональні дані учнів (імена, оцінки, фото) не мають бути у відкритому доступі без дозволу батьків.
Безпечне онлайн-середовище: фільтрація контенту, контроль за доступом до сайтів, запобігання кібербулінгу.
Захист під час відеозанять: заборона записів без згоди, контроль сторонніх осіб у відеочатах.
Цифрова грамотність: навчання дітей основам безпеки: паролі, приватність, поведінка в мережі.
Законодавчі основи: Закон України «Про захист персональних даних», Конвенція ООН про права дитини, стандарти UNICEF.

ЗАВДАННЯ. Заповни таблицю. Познач, які дії відповідають принципам захисту дітей. Якщо ✗ — поясни, чому.

Дія	✓ / ✗	Коментар
Публікація фото дітей на сайті школи без згоди батьків		
Встановлення фільтрів контенту на комп'ютерах у класі		
Запис відеозаняття без попередження		
Проведення уроку про кібербулінг для учнів 5 класу		
Збір контактів дітей через відкриту Google-форму		

КЕЙС ДЛЯ АНАЛІЗУ

Ситуація: Під час онлайн-заняття один з учнів увімкнув запис і виклав фрагмент із коментарями в соцмережі. Інші учасники не давали на це згоди. Деякі учні зазнали насмішок у коментарях.

Запитання для роздумів:
Які права були порушені?
Хто несе відповідальність?
Як цього уникнути в майбутньому?

Нотатки _____

СЛОВНИК ЦИФРОВОЇ БЕЗПЕКИ

ТЕРМІН	ПОЯСНЕННЯ
Антивірус	Програма для пошуку, ізоляції та видалення шкідливих файлів.
Брандмауер (Firewall)	Засіб контролю інтернет-трафіку: фільтрує підозрілу активність.
VPN	Віртуальна приватна мережа — шифрує з'єднання, приховує IP.
Пароль	Код для входу. Має бути складним, довгим, унікальним.
Фішинг	Обман для викрадення паролів (через підроблені сайти чи листи).
2FA (Двофакторна автентифікація)	Пароль + другий код (SMS, додаток, біометрія).
Шифрування	Перетворення даних у захищений, нечитабельний вигляд.
Кіберзлочин	Злочин, що відбувається у цифровому середовищі.
Cookies	Файли, які сайти зберігають у браузері для запам'ятовування.
Захист даних	Комплекс заходів для недопущення витоку особистої інформації.
Конфіденційність	Право особи зберігати дані у таємниці.
Інформаційна гігієна	Навички безпечного використання інформації та цифрових пристроїв.
Кібергігієна	Практики, що знижують ризик інцидентів (оновлення, паролі тощо).
Фішингова сторінка	Сайт, що імітує справжній, щоб вкрасти дані.
Вірус	Шкідлива програма, що самовідтворюється та шкодить системі.
Троян	Шкідливе ПЗ, що маскується під корисну програму.
Spyware (шпигунське ПЗ)	Збирає дані користувача без його відома.
Ransomware	Блокує дані і вимагає викуп за їх розблокування.
Кейлогер	Програма, що записує натискання клавіш.
Хакер	Людина, яка зламує системи — не завжди злочинець.
Black hat	Зловмисник, що зламує з метою шкоди або викрадення.
White hat	Етичний хакер, який тестує безпеку на користь організацій.

ТЕРМІН	ПОЯСНЕННЯ
Інцидент безпеки	Подія, яка загрожує конфіденційності або цілісності даних.
Порушення даних (Data Breach)	Несанкціонований доступ до персональної інформації.
Резервне копіювання (Backup)	Створення копій важливих файлів для відновлення.
Соціальна інженерія	Маніпуляція людиною для отримання даних (не технічна атака).
Скімінг	Зчитування картки або паролю за допомогою технічних пристроїв.
Shoulder surfing	Підглядання пароля або PIN-коду через плече.
DDoS-атака	Масова атака на сайт або сервер з метою перевантаження.
Фільтрація контенту	Блокування небажаних сайтів або типів інформації.
IDS (система виявлення вторгнень)	Аналізує трафік і повідомляє про підозрілу активність.
IPS (система запобігання вторгнень)	Автоматично блокує підозрілу активність.
Хмарні сервіси	Сайти або системи, які зберігають дані «в інтернеті», а не на комп'ютері.
IoT (Інтернет речей)	Пристрої, підключені до мережі (камери, датчики, годинники).
BYOD (Bring Your Own Device)	Політика дозволу роботи з особистих пристроїв.
Zero Trust	Підхід: не довіряти автоматично навіть своїм пристроям чи мережам.
Патч / оновлення	Виправлення вразливостей у програмному забезпеченні.
Біометрія	Ідентифікація за відбитком пальця, обличчям тощо.
Інформаційна політика	Внутрішні правила організації щодо даних і технологій.
Регламент доступу	Хто і до чого має право доступу (рольовий контроль).
Найменші привілеї	Принцип: кожен має тільки той доступ, який дійсно потрібен.
Компрометація акаунту	Отримання доступу до чужого облікового запису.
GDPR	Загальний регламент захисту даних у ЄС.
Закон «Про захист персональних даних» (Україна)	Основний український закон щодо обробки даних.

ЩОДЕННИЙ ЧЕК-ЛИСТ БЕЗПЕКИ

Виконуй перед початком роботи або навчання

ПРИСТРІЙ ГОТОВИЙ:

- Заряджено не менше 50%
- Підключення до Wi-Fi захищене
- Антивірус активний
- Встановлено всі оновлення
- Камера/мікрофон вимкнені (якщо не потрібні)
- Bluetooth і геолокація вимкнені
- VPN увімкнено (у публічних мережах)
- Пристрій заблоковано паролем або біометрією

ЦИФРОВА ГІГІЄНА:

- Усі паролі складні, різні
- 2FA активовано для важливих акаунтів
- Зайві застосунки видалено
- Зроблено резервну копію важливих файлів
- Жодних підозрілих листів не відкривалось
- Соцмережі не містять конфіденційної інформації
- У браузері не збережено паролі
- Дозволи застосунків переглянуто

ЧЕК-ЛИСТ: ПОВЕДІНКА В ІНТЕРНЕТІ

Самооцінка цифрової культури

Обміркуй і познач: Так / Ні

СИТУАЦІЯ	✓ / ✗
Я перевіряю джерела інформації	☐ ☐
Не поширюю підозрілий контент	☐ ☐
Читаю умови перед встановленням додатків	☐ ☐
Не вводжу персональні дані на сумнівних сайтах	☐ ☐
Уникаю обговорення конфліктних тем у публічних чатах	☐ ☐
Не публікую фото документів або екранів	☐ ☐
Маю окремі акаунти для навчання та особистого	☐ ☐
Вмію розпізнати фейкові сайти та листи	☐ ☐
Не беру участі в онлайн-опитуваннях без перевірки	☐ ☐
Дотримуюсь етичної поведінки в соцмережах	☐ ☐

ЧЕК-ЛИСТ: ЯК НЕ СТАТИ ЖЕРТВОЮ ФІШИНГУ

Перевір електронний лист або сайт за цими ознаками

ПОДИВИСЬ УВАЖНО:

- Домен не збігається з офіційним сайтом (напр. g00gle.com)
- Відправник виглядає підозріло (дивна адреса або ім’я)
- Є орфографічні помилки, дивний стиль
- Є тиск: “терміново”, “зміни пароль зараз”, “виконай дію негайно”
- Є вкладення або посилання на незнайомі сайти
- Просять ввести пароль або код підтвердження
- Сторінка копіює дизайн відомого сервісу, але адреса — інша
- Запити виглядають неформально, без підпису або пояснень
- Вкладення має розширення .exe / .zip / .scr
- Схожий лист ніколи не приходив раніше

ЯКЩО ПОЗНАЧЕНО 3 І БІЛЬШЕ — ЦЕ МОЖЕ БУТИ ФІШИНГ!