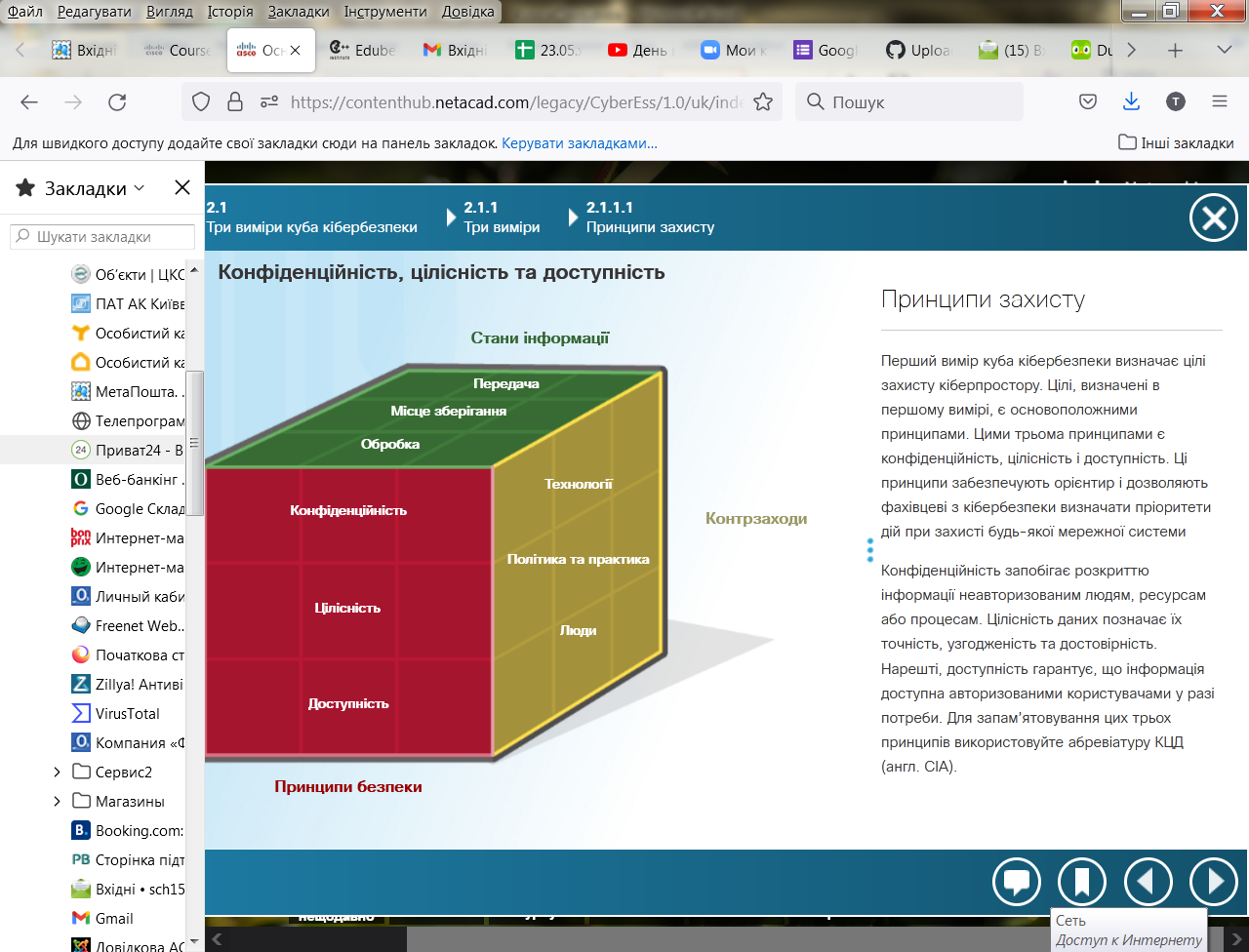
**Розділ 2. Куб кібербезпеки**

Фахівці з кібербезпеки - це експерти, які займаються захистом у кіберпросторі. Джон Мак-Камбер один з перших експертів з кібербезпеки, розробив широко використовувану конструкцію під назвою Куб Мак-Камбера або Куб кібербезпеки. Він використовується як інструмент для захисту мереж, доменів та Інтернету. Куб кібербезпеки чимось нагадує кубик Рубика.

Перший вимір Куба кібербезпеки визначає три принципи інформаційної безпеки. Фахівці з кібербезпеки називають ці три принципи (конфіденційність, цілісність, доступність) КЦД-тріадою (CIA Triad). Другий вимір визначає три стани інформації або даних. Третій вимір куба визначає необхідні дії для забезпечення захисту. Ці виміри часто називають трьома категоріями гарантованої кібербезпеки.

Ця глава також описує модель кібербезпеки ISO. Вона являє собою міжнародну основу стандартизації та керування інформаційними системами.

**Принципи захисту**

Перший вимір куба кібербезпеки визначає цілі захисту кіберпростору. Цілі, визначені в першому вимірі, є основоположними принципами. Цими трьома принципами є конфіденційність, цілісність і доступність. Ці принципи забезпечують орієнтир і дозволяють фахівцеві з кібербезпеки визначати пріоритети дій при захисті будь-якої мережної системи

Конфіденційність запобігає розкриттю інформації неавторизованим людям, ресурсам або процесам. Цілісність даних позначає їх точність, узгодженість та достовірність. Нарешті, доступність гарантує, що інформація доступна авторизованими користувачами у разі потреби. Для запам’ятовування цих трьох принципів використовуйте абревіатуру КЦД (англ. CIA).

**Стани даних**

Кіберпростір - це домен, що містить значну кількість критично важливих даних. Тому експерти з кібербезпеки зосереджені на захисті даних. Другий вимір куба кібербезпеки зосереджений на проблемах захисту даних, які знаходяться у кіберпросторі в різних станах. Дані мають три можливі стани:

* Дані в передачі
* Дані в стані спокою або зберігання
* Дані в обробці

Захист кіберпростору вимагає, щоб фахівці в області кібербезпеки гарантували безпеку даних у всіх трьох станах.

**Гарантії кібербезпеки**

Третій вимір куба кібербезпеки визначає навички і знання, які фахівець з кібербезпеки може використовувати для захисту у кіберпросторі. Фахівці з кібербезпеки повинні використовувати цілу низку наявних навичок і знань, коли захищають дані в кіберпросторі. Вони повинні це робити залишаючись при цьому на стороні закону.

Куб кібербезпеки визначає три типи навичок, які використовуються для забезпечення захисту. Перша навичка включає в себе технології, пристрої та продукти для захисту інформаційних систем і запобігання діям кіберзлочинців. Фахівці з кібербезпеки повинні володіти спеціалізованими технологічними інструментами. Проте, Мак-Камбер нагадує їм, що для перемоги над кіберзлочинцями недостатньо самих лише технологічних засобів. Професіонали з кібербезпеки також повинні вибудовувати потужний захист через налаштування політик, процедур та рекомендацій, які дозволяють користувачам кіберпростору залишатися у безпеці та дотримуватися принципів передової практики. Нарешті, користувачі кіберпростору повинні прагнути більшої обізнаності щодо загроз у кіберпросторі та виробити культуру навчання та усвідомлення у сфері інформаційної безпеки.

**Принципи конфіденційності**

Конфіденційність запобігає розкриттю інформації неавторизованим особам, ресурсам або процесам. Синонімом конфіденційності є приватність. Організації обмежують доступ, щоб гарантувати, що тільки уповноважені оператори можуть використовувати дані або інші мережні ресурси. Наприклад, програміст не повинен мати доступ до особистої інформації всіх співробітників.

Організації повинні навчати співробітників кращим методам захисту конфіденційної інформації, щоб захистити їх та себе від атак. Методи, які використовуються для забезпечення конфіденційності, включають шифрування даних, аутентифікацію і контроль доступу.

**Захист конфіденційності даних**

Організації накопичують великий обсяг даних. Значна частина цих даних є відкритою і не потребує захисту, наприклад, імена співробітників та номери їх телефонів. Проте деякі дані потребують особливого захисту. Конфіденційна інформація - це дані, захищені від несанкціонованого доступу для гарантування безпеки окремій особі або організації. Існує три типи конфіденційної інформації:

* Персональна інформація - це особиста інформація, а саме дані, за допомогою яких можна визначити особистість людини. На рисунку 2 наведена ця категорія даних.
* Ділова інформація - це інформація, яка у разі оприлюднення може створити проблеми для організації. На рисунку 3 наведена ця категорія даних.
* Секретна інформація - це інформація, що належить державним органам, засекречена через високий рівень конфіденційності. На рисунку 4 наведена ця категорія даних.

# 

# Керування доступом

Контроль доступу визначає ряд схем захисту, які запобігають несанкціонованому доступу до комп'ютера, мережі, бази даних або інших ресурсів даних. Концепція ААО (англ. AAA) включає в себе три служби безпеки: аутентифікація, авторизація та облік. Ці служби забезпечують основну структуру контролю доступу.

Перше «А» в ААО (ААА) позначає аутентифікацію. ***Аутентифікація*** перевіряє особу користувача для запобігання несанкціонованому доступу. Користувачі підтверджують свою особистість за ім'ям користувача або ідентифікатором. Окрім того, користувачі повинні підтвердити свою особу за одним із способів, як показано на рисунку 1.

* Надати інформацію яку вони знають (наприклад, пароль)
* Підтвердити наявність чогось (наприклад, токен або картка)
* Надати біометричну інформацію (наприклад, відбитки пальців)

Наприклад, для зняття готівки через банкомат, вам потрібна ваша банківська картка та PIN-код. Це також є прикладом багатофакторної аутентифікації. Для багатофакторної аутентифікації потрібно декілька типів аутентифікації. Найбільш популярною формою аутентифікації є використання паролів.

***Авторизація*** , визначає через свою службу до яких ресурсів можуть отримати доступ користувачі, а також операції, які вони можуть виконувати, як показано на рисунку 2. Деякі системи реалізують це за допомогою списку керування доступом або ACL (англ. Access Control List). ACL визначає, чи має користувач певні привілеї доступу після проходження аутентифікації. Те, що ви можете увійти в корпоративну мережу, не означає, що у вас є дозвіл на використання високошвидкісного кольорового принтера. Авторизація також може контролювати, коли користувач має доступ до певного ресурсу. Наприклад, співробітники можуть мати доступ до бази даних продажів в робочий час, але система блокує їх у неробочий час.

***Облік*** , відстежує дії користувача, а саме, до яких даних вони зверталися, тривалість використання ресурсів та будь-які зроблені зміни. Наприклад, банк відстежує облікові записи кожного клієнта. Аудит цієї системи може виявити час і кількість всіх транзакцій, а також співробітника або системи, які виконували транзакції. Служби обліку кібербезпеки працюють так само. Система відстежує кожну транзакцію даних і надає результати аудиту. Для запровадження аудиту системи адміністратор може налаштувати політики комп'ютера, як показано на рисунку 3.

Концепція ААО (AAA) аналогічна використанню кредитної картки, як показано на рисунку 4. Кредитна карта ідентифікує, хто може її використовувати, скільки може витратити цей користувач і веде облік товарів або послуг, які користувач придбав.

У сфері кібербезпеки облік виконується у режимі реального часу. Веб-сайти, такі як Norse, показують атаки в режимі реального часу на основі даних, зібраних в рамках системи обліку або відстеження. Натисніть [тут](http://map.norsecorp.com/) щоб відвідати веб-сайт Norse.

# 

Рисунок 1

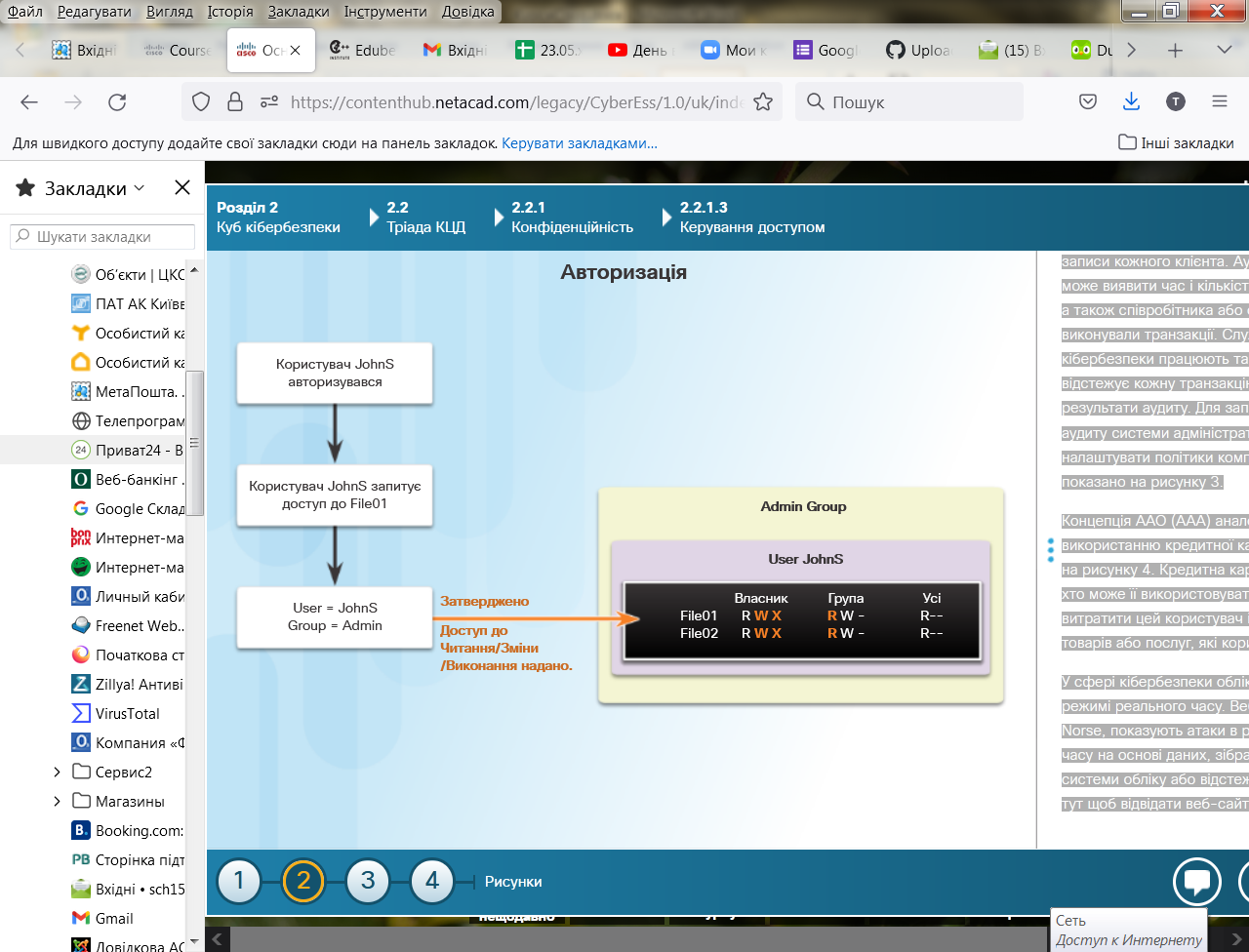


Рисунок 2

# 

Рисунок 3

# 

Рисунок 4

# Закони та відповідальність

Конфіденційність і приватність здаються взаємозамінними, але з юридичної точки зору вони означають різні речі. Більшість приватних даних конфіденційні, але не всі конфіденційні дані є приватними. Доступ до конфіденційної інформації відбувається після підтвердження правильної авторизації. Фінансові установи, лікарні, медичні працівники, юридичні фірми та підприємства обробляють конфіденційну інформацію. Конфіденційна інформація має непублічний статус. Збереження конфіденційності - це скоріше етичний обов’язок.

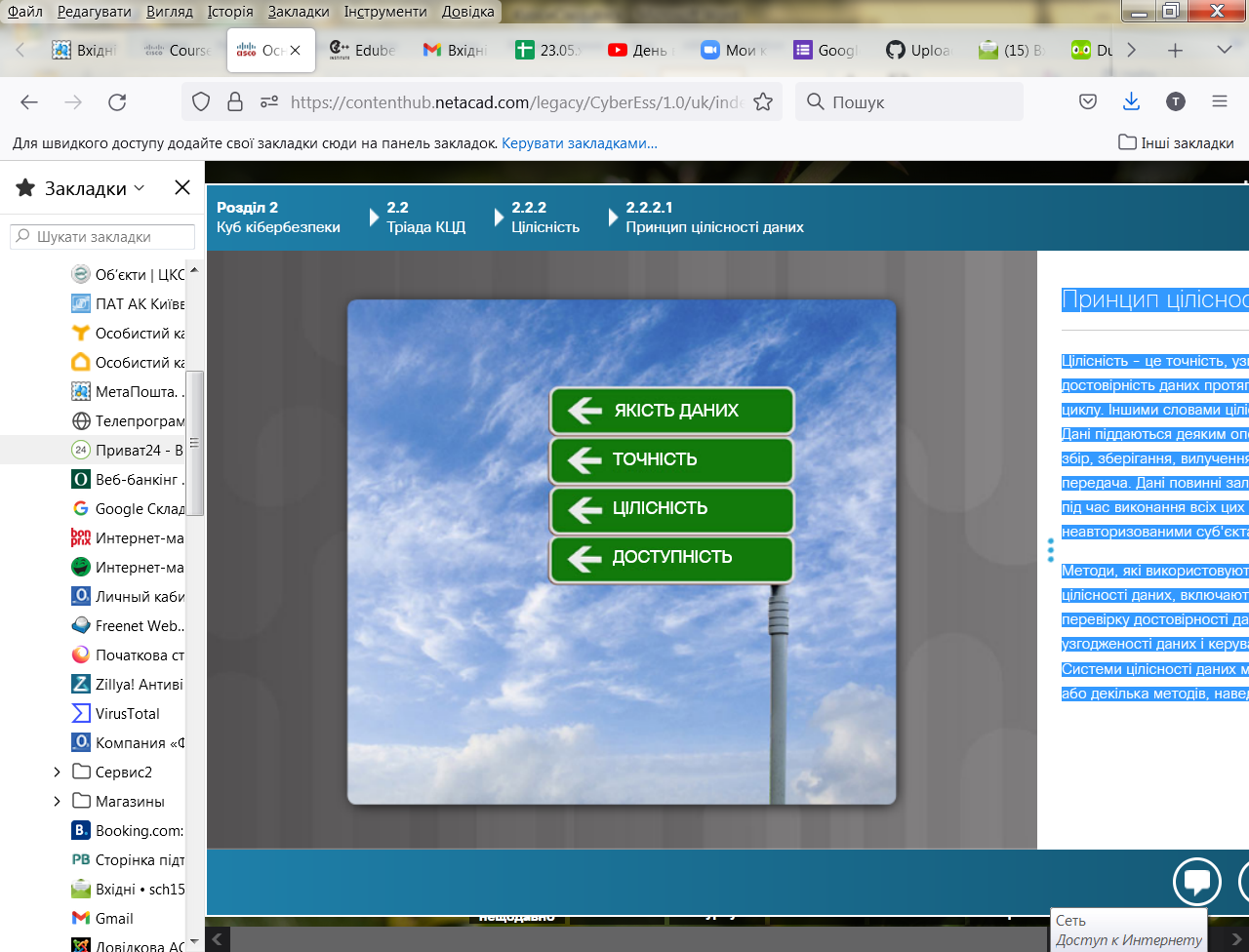
Приватність пов'язана з правильним використанням даних. Коли організації збирають інформацію, надану клієнтами або співробітниками, вони повинні використовувати ці дані лише за прямим призначенням. Більшість організацій зажадають, щоб клієнт або співробітник підписали необхідний документ, надавши організації право використовувати дані.

Всі закони закони США, які перераховані на рисунку 1, включають положення про захист приватного життя. На рисунку 2 наведена вибірка законів інших країн. Більшість з цих законів є відповіддю на масове зростання збору даних.

Зростаюче число законів, що стосуються приватності, створює величезне навантаження для організацій, які збирають і аналізують дані. Політика - кращий спосіб для організації дотримуватися законів, що стосуються конфіденційності. Політики дозволяють організаціям застосовувати певні правила, процедури і процеси при зборі, зберіганні та спільному використанні даних.

# 

# Принцип цілісності даних

Цілісність - це точність, узгодженість і достовірність даних протягом всього життєвого циклу. Іншими словами цілісність - це якість. Дані піддаються деяким операціям, таким як збір, зберігання, вилучення, оновлення та передача. Дані повинні залишатися незмінними під час виконання всіх цих операцій неавторизованими суб'єктами.

Методи, які використовуються для забезпечення цілісності даних, включають хешування, перевірку достовірності даних, перевірку узгодженості даних і керування доступом. Системи цілісності даних можуть включати один або декілька методів, наведених вище.

# Потреба в цілісності даних

Цілісність даних є фундаментальним компонентом інформаційної безпеки. Потреба в цілісності даних залежить від того, як організація використовує дані. Наприклад, Facebook не перевіряє дані, які користувач публікує в профілі. Банк або фінансова організація надають більшого значення цілісності даних, ніж Facebook. Транзакції і рахунки клієнтів повинні бути точними. В організації охорони здоров'я цілісність даних може бути питанням життя або смерті. Інформація в рецептах повинна бути точною.

Захист цілісності даних є постійною проблемою для більшості організацій. Втрата цілісності даних може привести до того, що всі дані будуть недостовірними або непридатними для використання.

# 

# Перевірка цілісності

Перевірка цілісності - це спосіб вимірювання узгодженості набору даних (файлу, зображення або записів). Перевірка цілісності виконується за допомогою такого процесу як хеш-функції для миттєвого формування відбитку даних. Перевірка цілісності використовує цей відбиток аби переконатися, що дані залишилися незмінними.

Контрольна сума є одним із прикладів хеш-функції. Контрольна сума підтверджує цілісність файлів або рядків символів до і після їх передачі з одного пристрою на інший через локальну мережу або Інтернет. Контрольна сума просто перетворює кожну частину інформації в значення і підсумовує їх. Щоб перевірити цілісність даних, система, яка отримала файл, повторює цей процес. Якщо дві суми рівні, дані дійсні (рисунок 1). Якщо вони не рівні, десь в процесі передачі відбулася зміна (рис. 2).

На сьогоднішній день популярні такі хеш-функції як MD5, SHA-1, SHA-256 і SHA-512. Ці хеш-функції використовують складні математичні алгоритми. Значення хешу використовується для порівняння. Наприклад, після завантаження файлу користувач може перевірити його цілісність, порівнюючи хеш-значення джерела з тим, яке генерується будь-яким хеш-калькулятором.

Організації використовують контроль версій для запобігання випадковим змінам від авторизованих користувачів. Два користувачі не можуть оновити один і той самий об'єкт. Об'єктами можуть бути файли, записи бази даних або транзакції. Наприклад, у першого користувача, який відкрив документ, є дозвіл на зміну цього документа. У другого - є версія лише для читання.

Точні резервні копії допомагають зберегти цілісність даних, якщо дані пошкоджені. Організації необхідно перевірити результат резервного копіювання, щоб забезпечити цілісність резервного копіювання до втрати даних.

Авторизація визначає, хто має доступ до ресурсів організації, виходячи з необхідності. Наприклад, дозвіл на доступ до файлів і засоби контролю доступу користувачів гарантують, що тільки деякі користувачі можуть змінювати дані. Адміністратор може встановлювати дозволи для файлу тільки для читання. В результаті користувач, який одержує доступ до цього файлу, не може вносити ніяких змін.

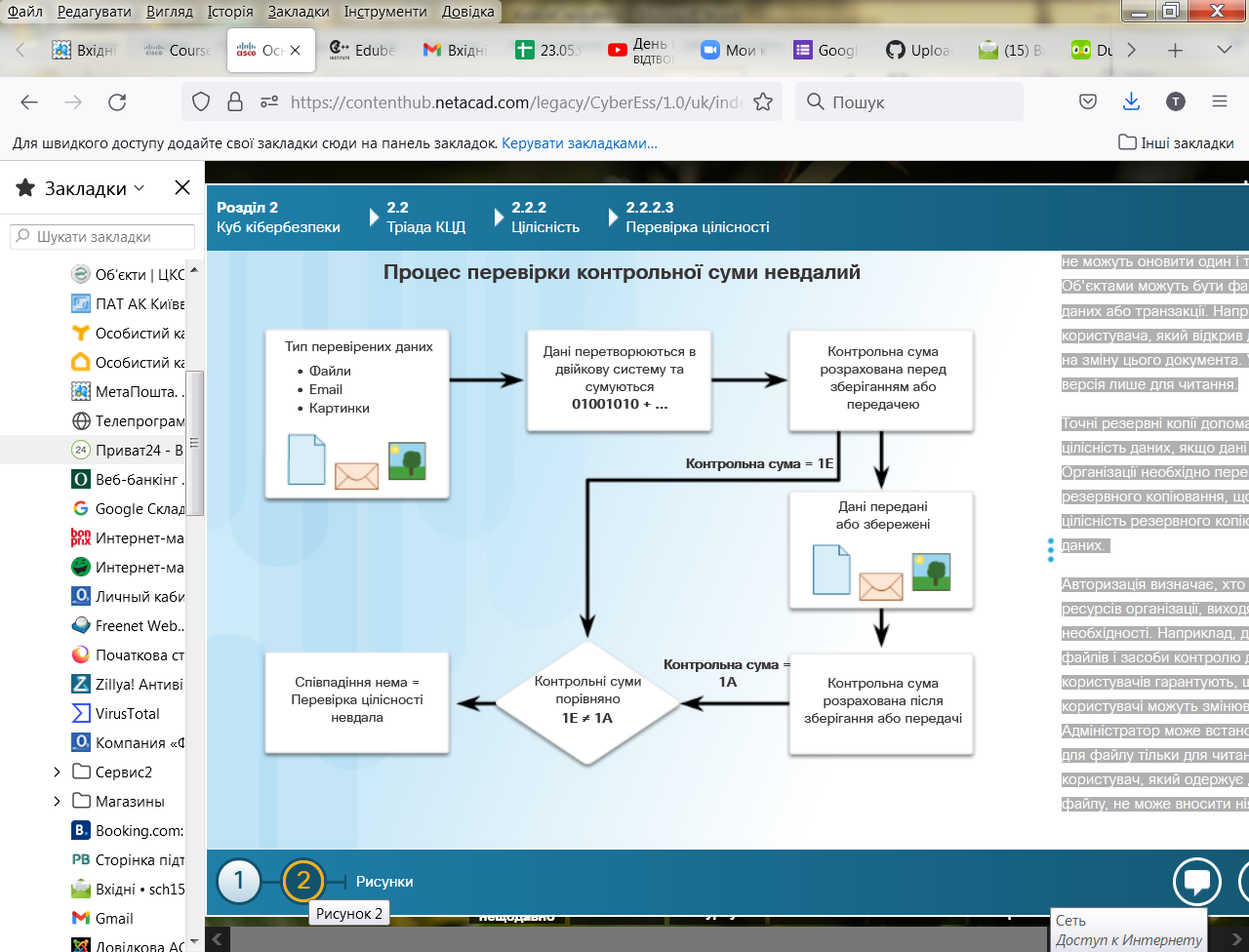


Рисунок 1

# 

# Рисунок 2

# Принцип доступності

Доступність даних - це принцип, який використовується для опису необхідності постійно підтримувати доступність інформаційних систем і послуг. Кібератаки і збої системи можуть перешкоджати доступу до інформаційних систем і служб. Наприклад, перериванням доступності веб-сайту шляхом виведення його з ладу можуть скористатися конкуренти. Ці атаки типу «відмова в обслуговуванні» (DoS) загрожують доступності системи і не дозволяють користувачам отримувати доступ до інформаційних систем і використовувати їх при необхідності.

Методи, які використовуються для забезпечення доступності, включають системне резервування, резервне копіювання системи, підвищену відмовостійкість системи, технічне обслуговування обладнання, сучасні операційні системи та програмне забезпечення і плани по швидкому відновленню від непередбачених лих.

# П'ять дев'яток

Люди використовують різні інформаційні системи в повсякденному житті. Комп'ютери та інформаційні системи контролюють зв'язок, транспорт і виробництво продукції. Постійна доступність інформаційних систем необхідна для сучасного життя. Термін «висока доступність» описує системи, призначені для запобігання простоям. Висока доступність забезпечує рівень продуктивності протягом більш тривалого, ніж зазвичай, періоду. Системи високої доступності найчастіше використовують три принципи проектування (рисунок 1):

* Усунути окремі точки відмови
* Забезпечити надійний план швидкого відновлення роботи на випадок надзвичайної ситуації
* Виявлення збоїв у міру їх виникнення

Мета полягає в тому, щоб продовжувати працювати в екстремальних умовах, наприклад під час атаки. Одна з найпопулярніших технологій високої доступності - п'ять дев'яток. Назва п'ять дев'яток пов’язана з доступністю ресурсу 99,999% часу. Це означає, що час простою становить менше 5,26 хвилин на рік. На рисунку 2 представлені три кроки для досягнення п'яти дев'яток.

# 

# Рисунок 1

# 

# Рисунок 1 (продовження)

# 

# Рисунок 2

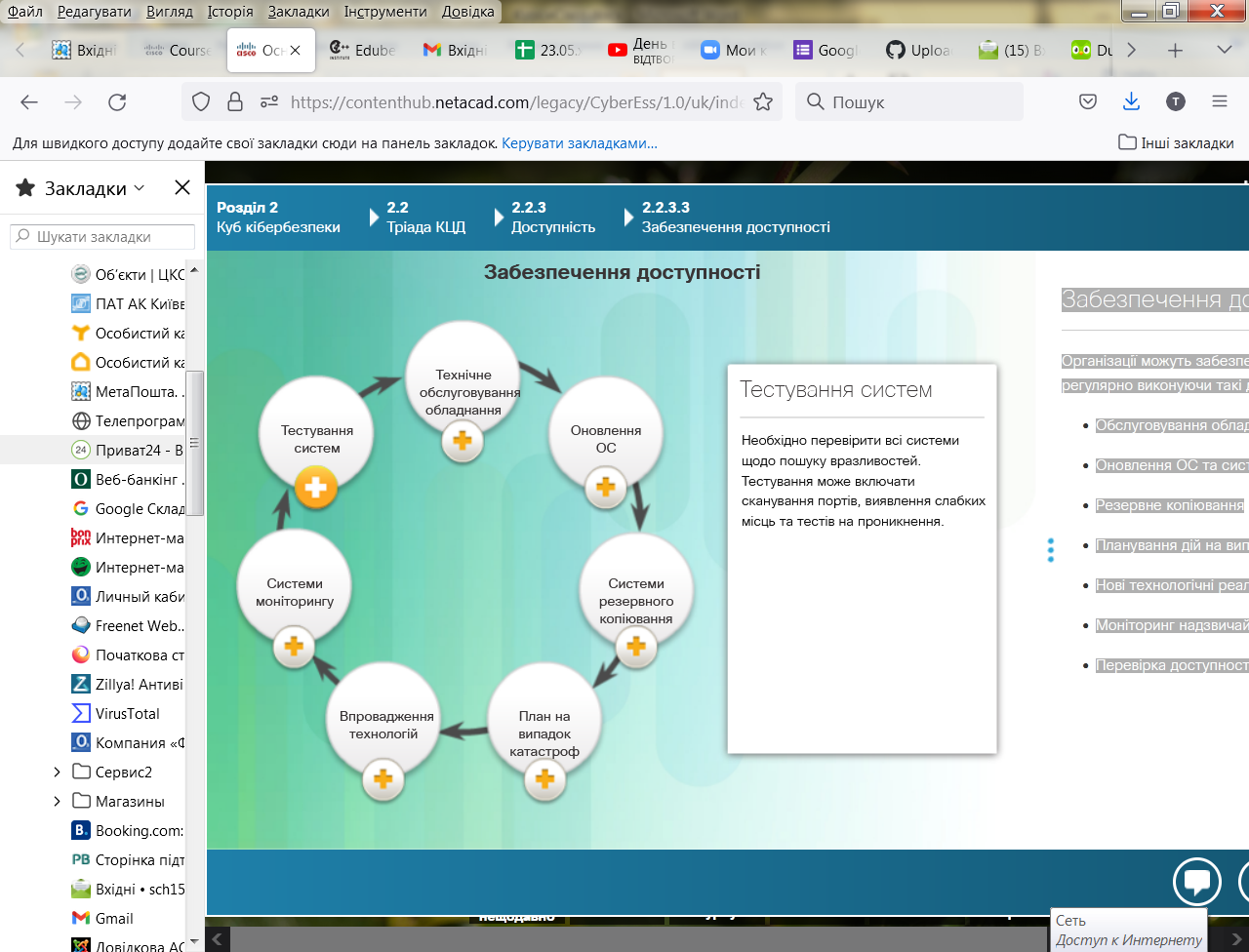
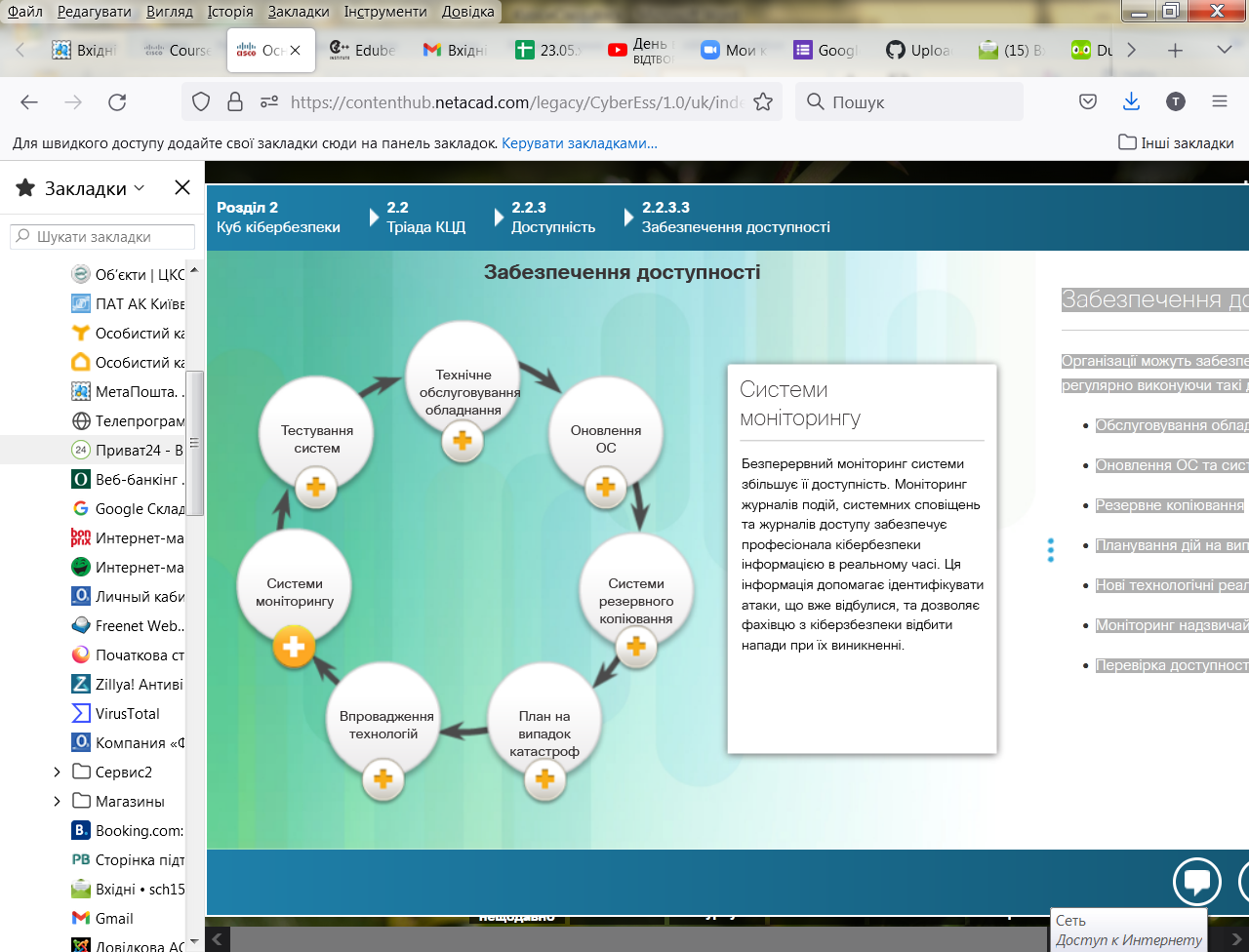
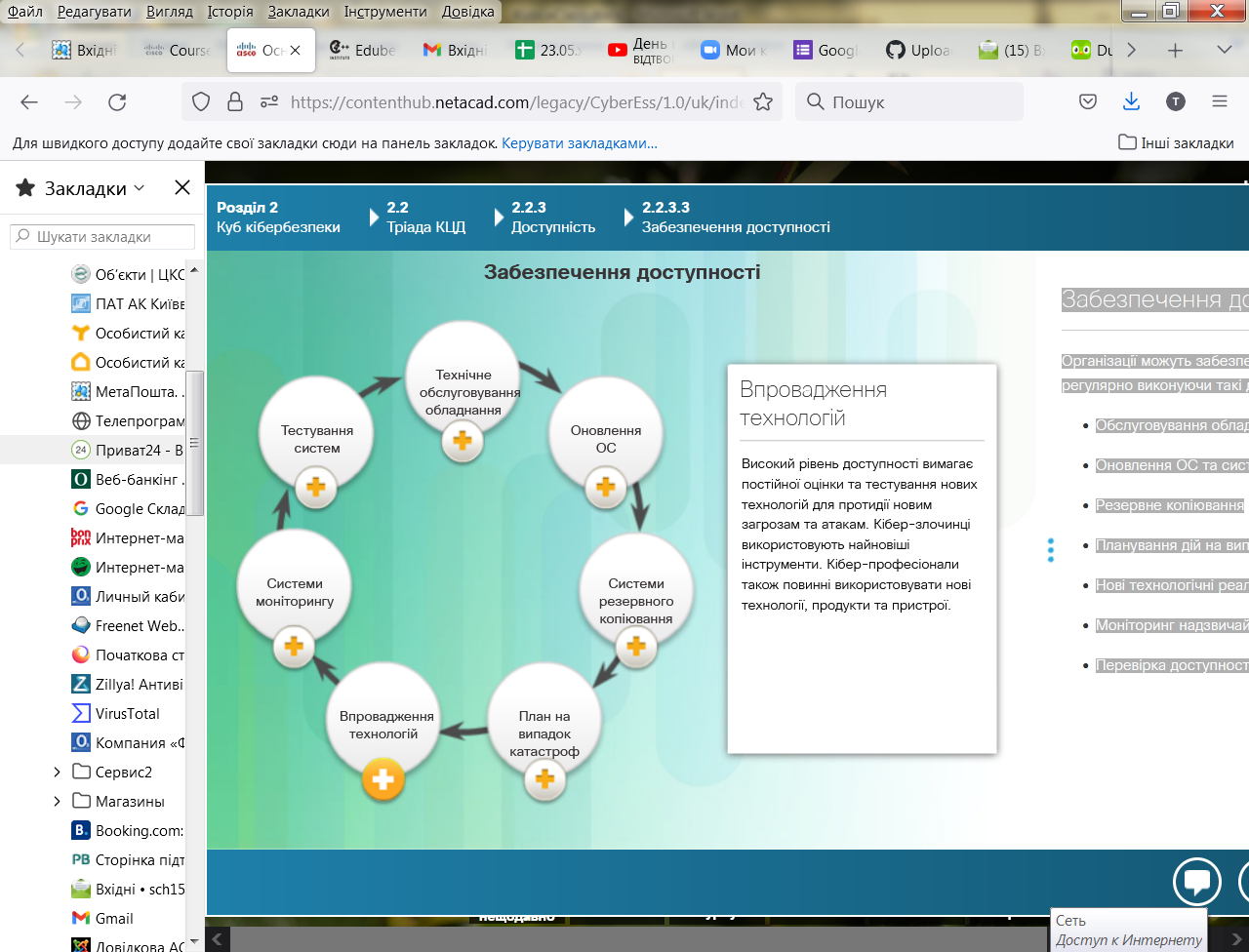
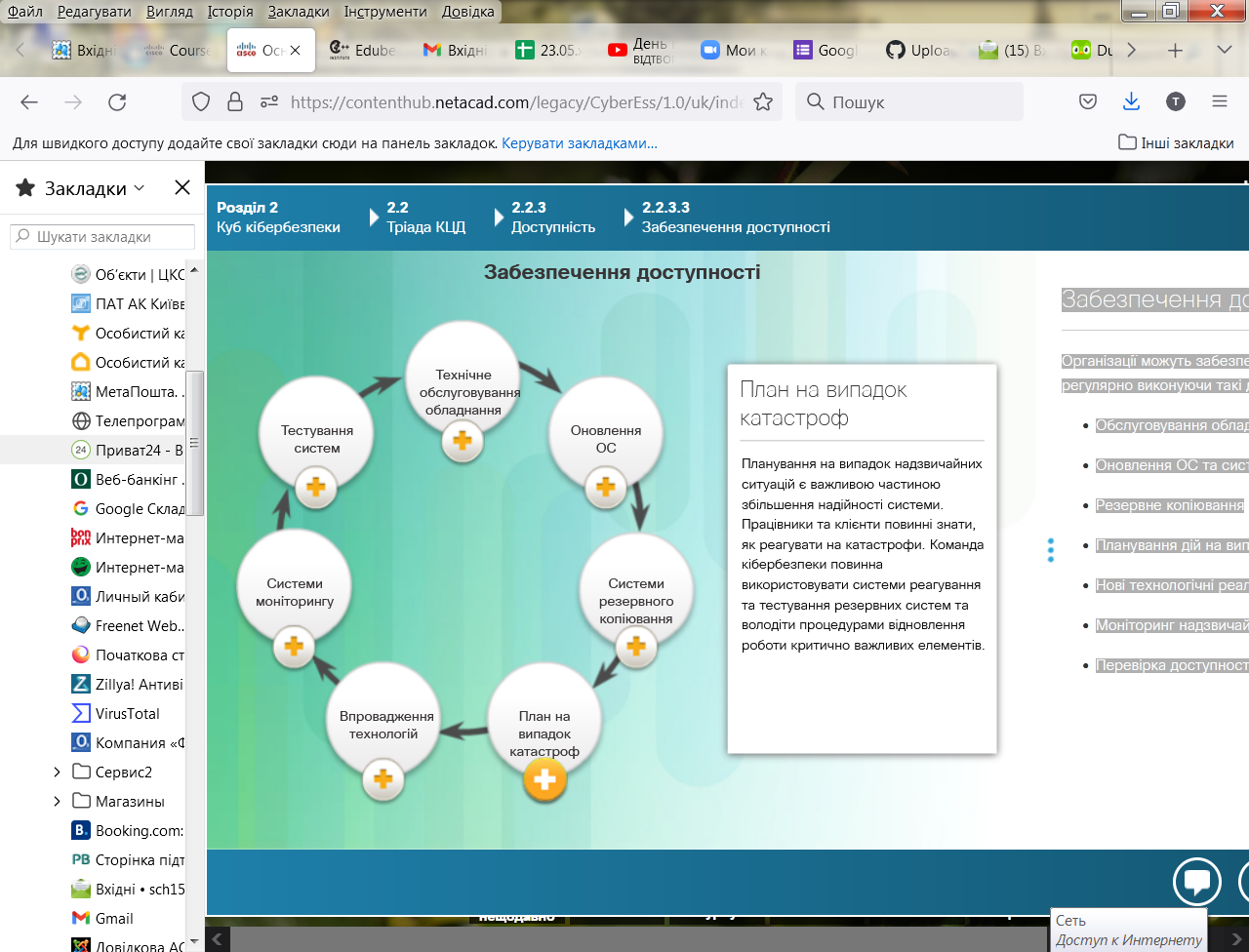
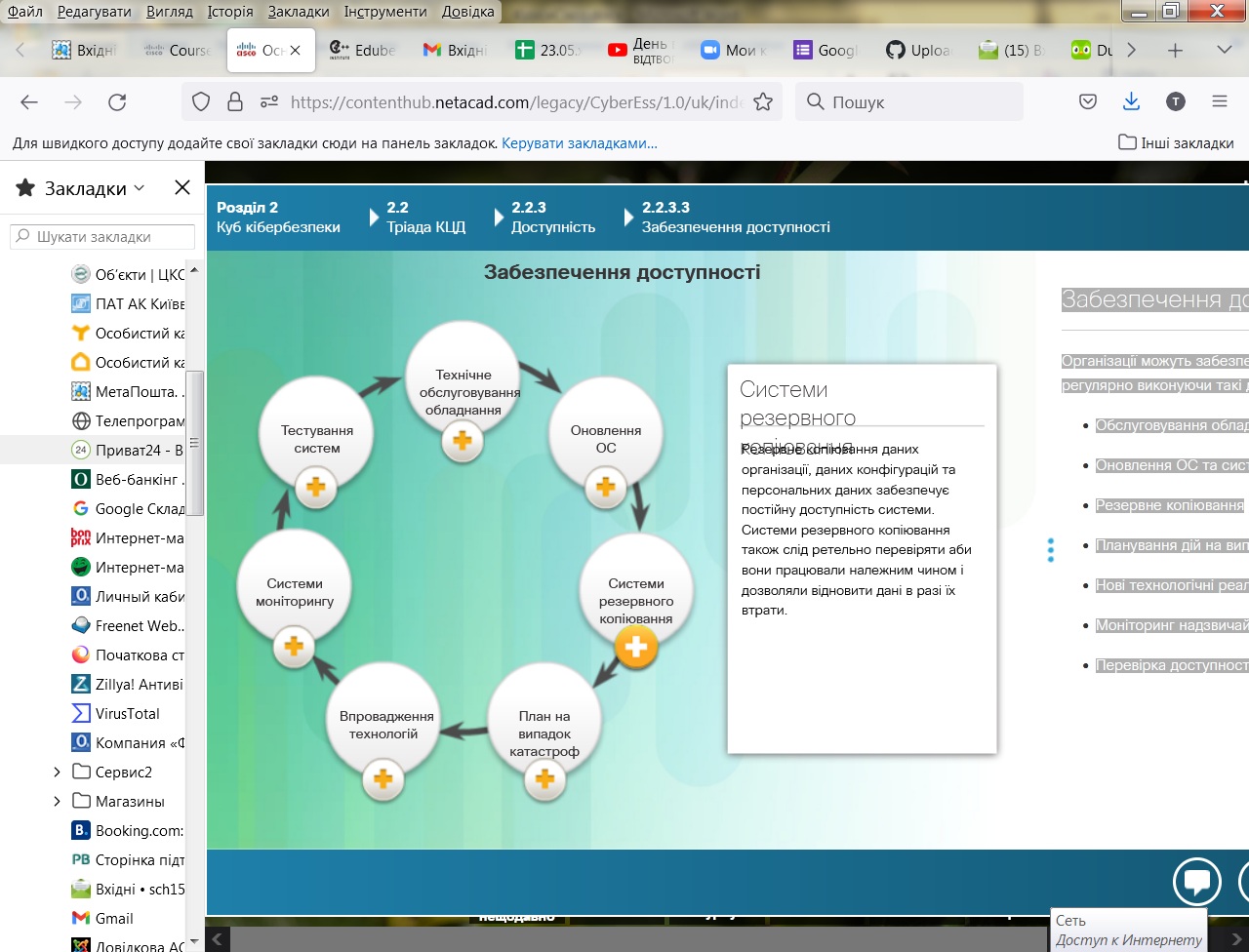
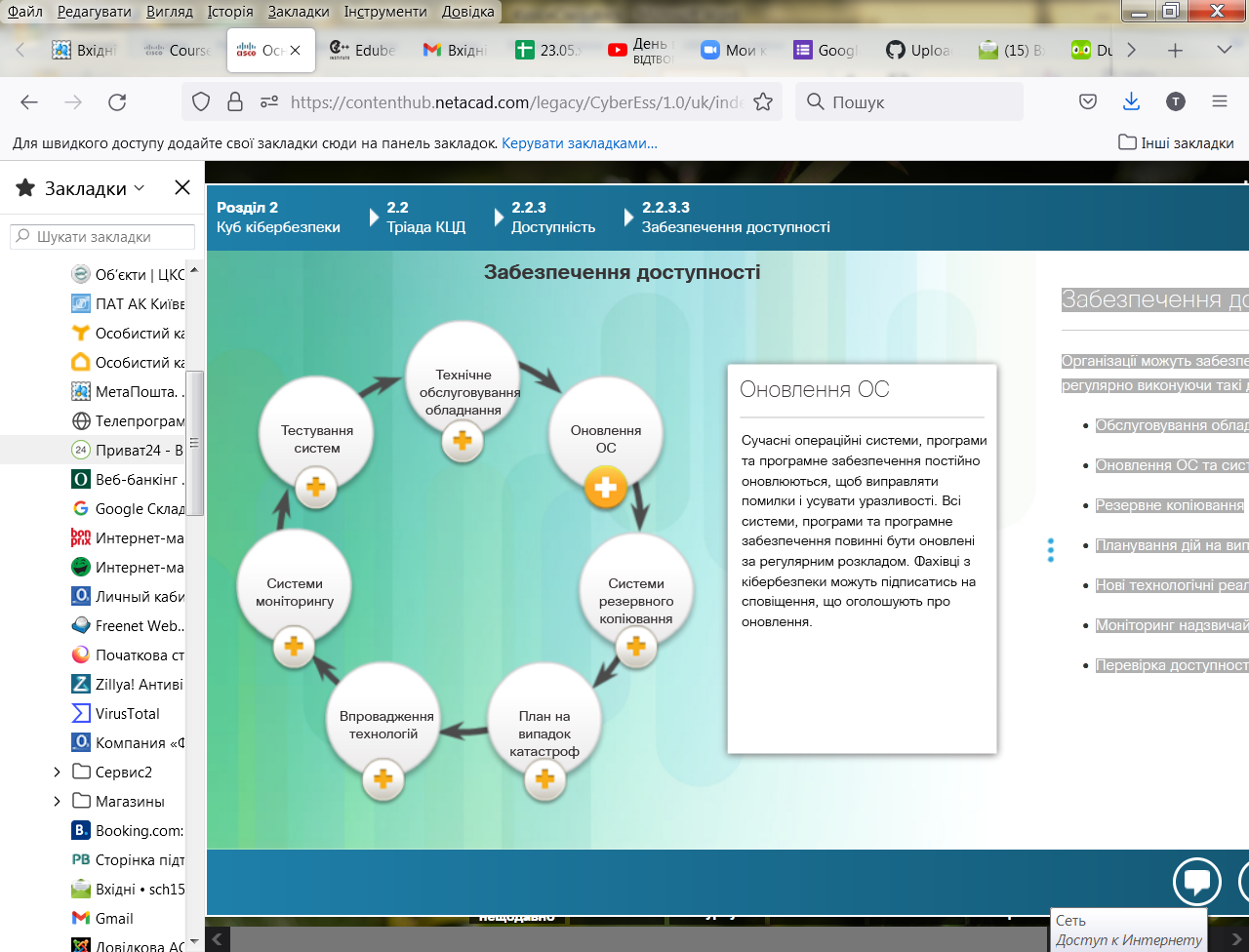
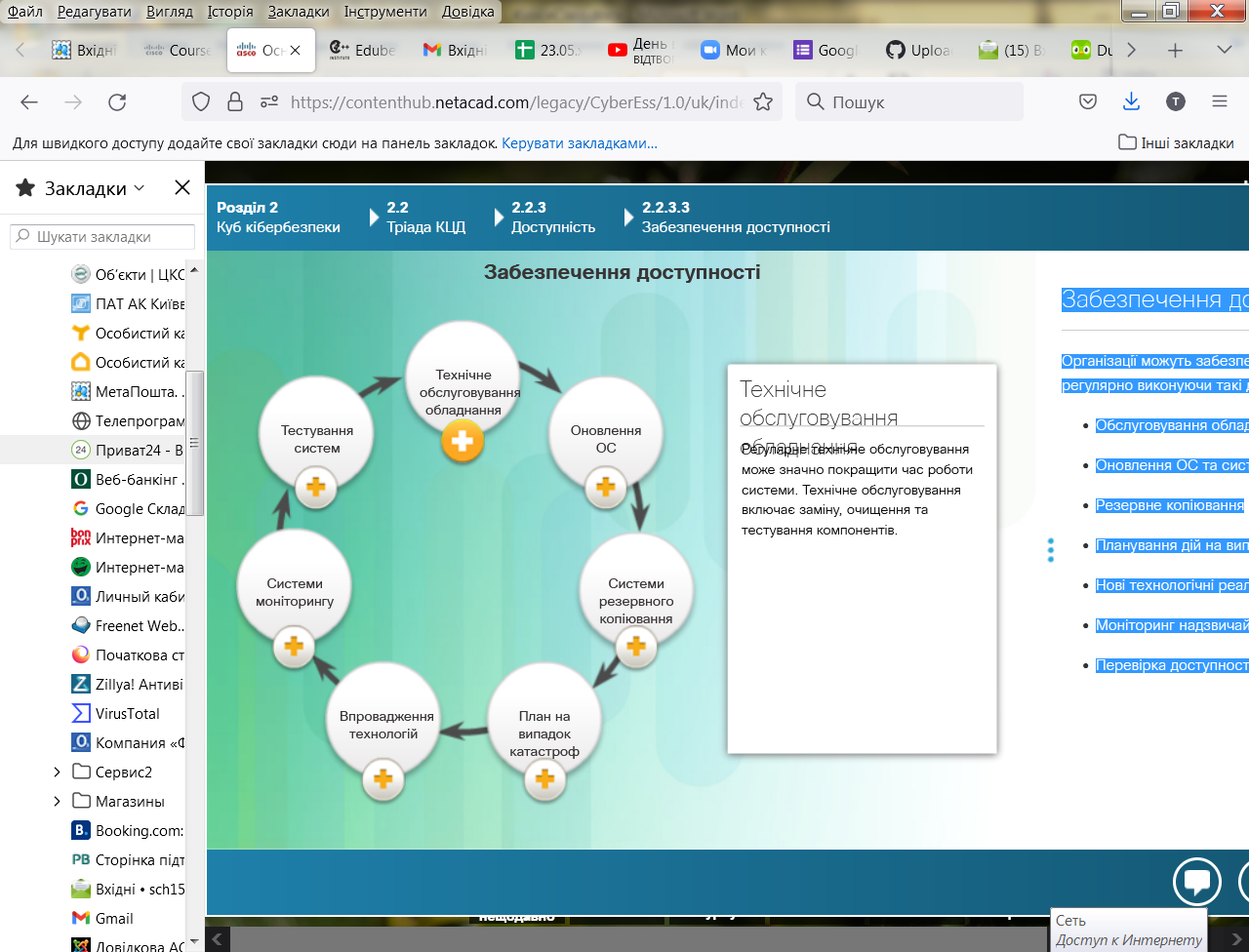
# 

Рисунок 1 (продовження)

# Забезпечення доступності

Організації можуть забезпечити доступність, регулярно виконуючи такі дії:

* Обслуговування обладнання
* Оновлення ОС та системи
* Резервне копіювання
* Планування дій на випадок стихійних лих
* Нові технологічні реалізації
* Моніторинг надзвичайної активності
* Перевірка доступності



**Типи сховищ даних**

Збережені дані належать до даних у стані спокою. Дані в стані спокою означають, що пристрій зберігання зберігає дані, коли жоден користувач або процес не використовує їх. Пристрій зберігання може бути локальним (на обчислювальному пристрої) або централізованим (в мережі). Існує багато опцій для зберігання даних.

Пряме сховище (direct-attached storage, DAS) - це сховище, що під'єднане до комп'ютера. Жорсткий диск або USB-накопичувач - приклад сховища з прямим підключенням. За замовчуванням системи не налаштовані для спільного використання сховища з прямим підключенням.

Резервний масив незалежних дисків (Redundant array of independent disks, RAID) використовує кілька жорстких дисків у масиві і являє собою об'єднання декількох дисків, які розглядаються операційною системою як один. RAID забезпечує підвищену продуктивність і відмовостійкість.

Мережний пристрій зберігання даних (network attached storage, NAS) - це пристрій, підключений до мережі, який дозволяє авторизованим користувачами зберігати та отримувати дані з централізованого сховища. Пристрої NAS гнучкі і масштабовані, що дозволяє адміністраторам збільшувати ємність у разі необхідності.

Мережа зберігання даних ( storage area network, SAN) - це мережна система зберігання, яка під'єднується до мережі за допомогою високошвидкісних інтерфейсів. Це дозволяє підвищити продуктивність і забезпечує можливість підключення декількох серверів до централізованого дискового сховища.

Хмарне сховище (Cloud storage) - це вид віддаленого сховища, при якому використовується простір на накопичувачах в дата-центрі провайдера, доступ до даних може бути організований з будь-якого комп'ютера з доступом до мережі Інтернет. Google Drive, iCloud і Dropbox - все це приклади постачальників хмарних сховищ.

**Проблеми захисту збережених даних**

Збереження даних - це складне завдання для організацій. Для покращення зберігання даних організації можуть вдатися до автоматизації та виконувати централізоване резервне копіювання даних.

Сховище з прямим підключенням може бути одним з найскладніших типів зберігання даних з точки зору контролю та керування. Воно найбільш вразливе до шкідливих атак на локальний хост. Збережені дані можуть також містити дані резервного копіювання. Резервні копії можуть створюватися вручну або автоматично. Організації повинні обмежувати типи даних, що зберігаються в сховищі з прямим підключенням. Зокрема, на них не слід зберігати критично важливі дані.

Мережні системи зберігання пропонують більш безпечний варіант. Такі мережні системи зберігання даних як RAID, SAN і NAS забезпечують більшу продуктивність та надлишковість. Проте мережні системи зберігання складніші для налаштування та керування. Також вони обробляють більші обсяги даних, що створює значний ризик для організації при виході пристрою з ладу. Особливу увагу при використанні мережних систем зберігання даних слід приділяти налаштуванню, тестуванню і моніторингу системи.

**Методи передачі даних**

Передача даних - це надсилання інформації з одного пристрою на інший. Існує багато способів передачі інформації між пристроями:

* **Sneaker net** - використовує знімні носії для фізичного переміщення даних з одного комп'ютера на інший
* **Дротові мережі** - використовують кабелі для передачі даних
* **Бездротові мережі** - використовують радіохвилі для передачі даних

Організації ніколи не зможуть уникнути використання Sneaker net.

Дротові мережі включають в себе мідні та волоконно-оптичні кабелі. Дротові мережі можуть обслуговувати місцеву географічну зону (локальна мережа), або прокладатися на великі відстані (глобальні мережі).

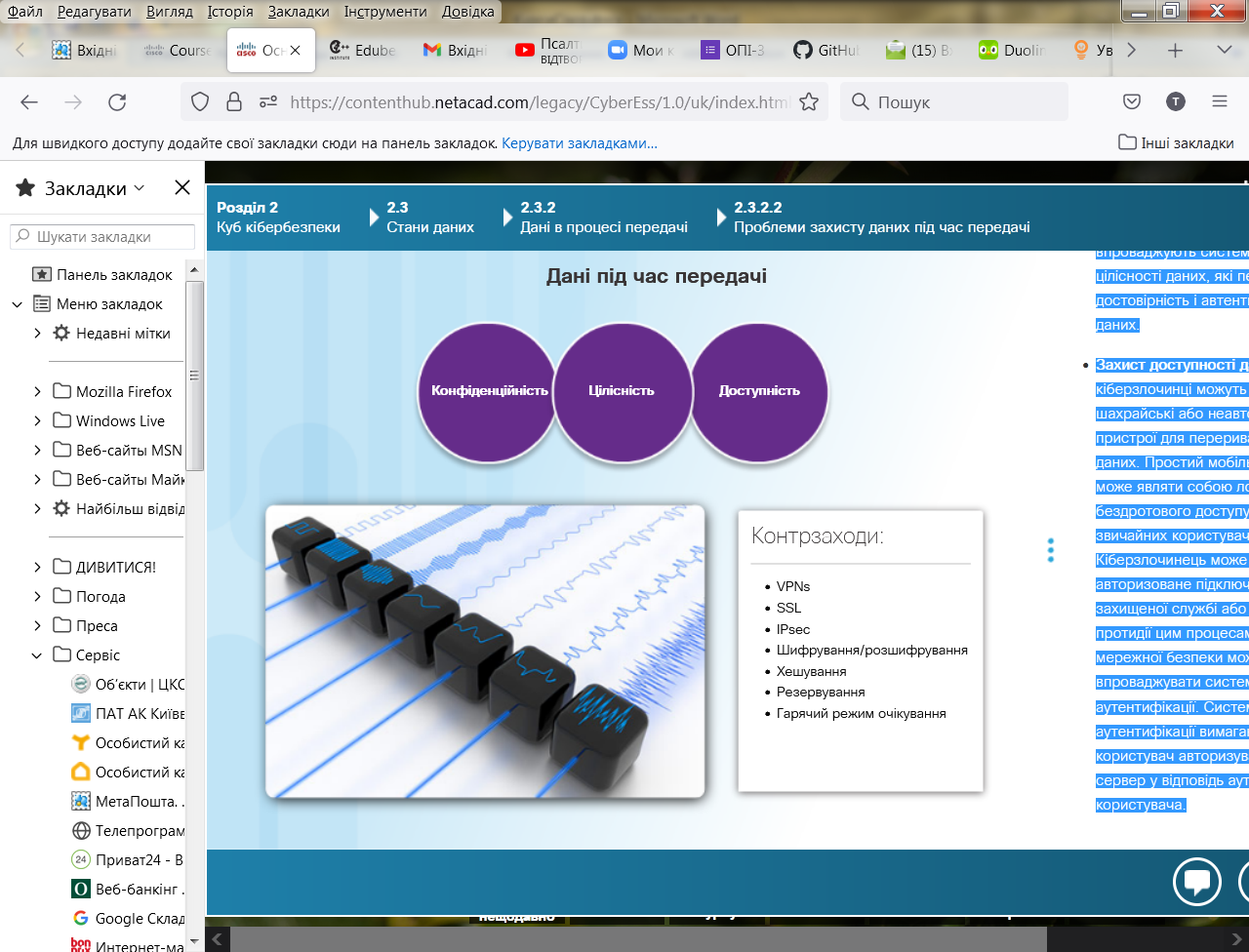
Бездротові мережі замінюють дротові , стають швидшими і здатні забезпечити більшу пропускну здатність. Бездротові мережі збільшують кількість користувачів, які під’єднуються до них з мобільних пристроїв у невеликих офісах і корпоративних мережах.

У дротових і бездротових мережах використовуються пакети або блоки даних. Термін «пакет» означає одиницю даних, яка переміщується між джерелом і пунктом призначення в мережі. Стандартні протоколи, такі як протокол Інтернету (IP) і протокол передачі гіпертексту (HTTP), визначають структуру і формат пакетів даних. Ці стандарти мають відкриті вихідні коди і є загальнодоступними. Захист конфіденційності, цілісності та доступності переданих даних - один з найважливіших обов'язків фахівця в області кібербезпеки.

**Проблеми захисту даних під час передачі**

Захист переданих даних є однією з найскладніших задач фахівця з кібербезпеки. Зі зростання кількості мобільних і бездротових пристроїв фахівці в області кібербезпеки несуть відповідальність за щоденний захист даних, які перетинають їх мережу. Фахівець з кібербезпеки повинен вирішити кілька проблем захисту цих даних:

* **Захист конфіденційності даних** - кіберзлочинці можуть перехоплювати, зберігати і викрадати дані під час їх передачі між пристроями. Кібер-професіонали повинні вжити заходів для протидії цим процесам.
* **Захист цілісності даних** - кіберзлочинці можуть перехоплювати і змінювати дані в момент їх передачі. Для запобігання цим діям фахівці з кібербезпеки впроваджують системи підтримки цілісності даних, які перевіряють достовірність і автентичність переданих даних.
* **Захист доступності даних** - кіберзлочинці можуть використовувати шахрайські або неавторизовані пристрої для переривання доступ до даних. Простий мобільний пристрій може являти собою локальну точку бездротового доступу і вводити в оману звичайних користувачів. Кіберзлочинець може перехопити авторизоване підключення до захищеної службі або пристрою. Для протидії цим процесам фахівці з мережної безпеки можуть впроваджувати системи взаємної аутентифікації. Системи взаємної аутентифікації вимагають, щоб користувач авторизувався на сервері, а сервер у відповідь аутентифікував користувача.



**Форми обробки і обчислення даних**

Третій стан даних - це дані в обробці. У цьому стані дані перебувають під час початкового введення, зміни, обчислення або виведення.

Захист цілісності даних починається з початкового введення даних. Організації використовують кілька методів для збору даних, таких як ручне введення даних, форми сканування, завантаження файлів і зчитування даних з датчиків. Кожен з цих методів створює потенційну загрозу цілісності даних. Прикладом пошкодження даних під час введення є помилки введення даних або відключені, несправні або непрацюючі системні датчики. До помилок введення належать також неправильне маркування і невірні або неузгоджені формати даних.

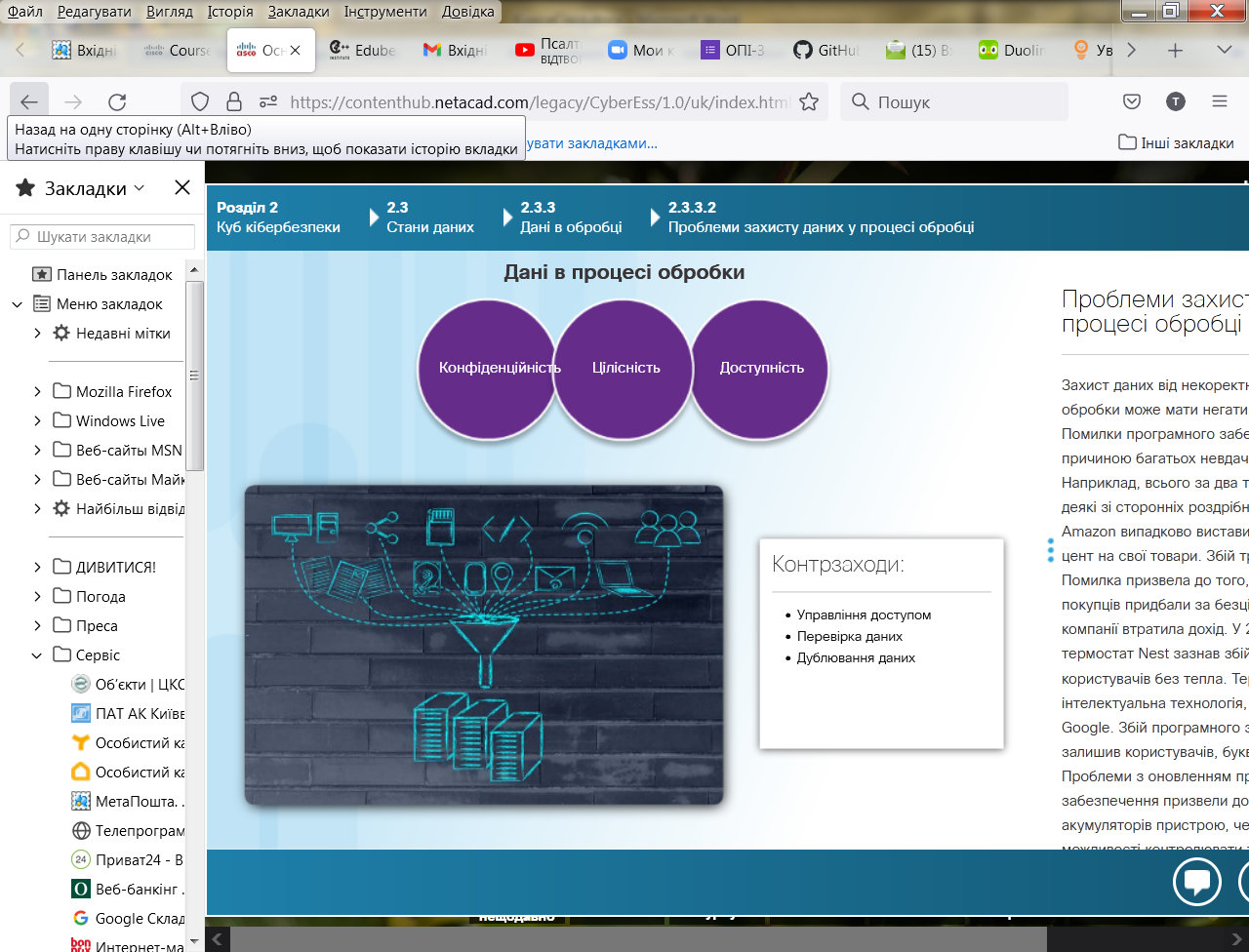
Модифікація даних - це будь-яка зміна вихідних даних. Наприклад, коли користувач вручну змінює дані або програма обробляє та оновлює дані, або коли дані змінюються внаслідок відмови обладнання. Процеси, такі як кодування/декодування, компресія/декомпресія і шифрування/дешифрування, є прикладами модифікації даних Шкідливий код також призводить до пошкодження даних.

Пошкодження даних також відбувається під час процесу виведення даних. Вивід даних відповідає передачі даних на принтери, електронні дисплеї або безпосередньо на інші пристрої. Точність вихідних даних має вирішальне значення, оскільки вивід інформації впливає на прийняття рішень. Прикладами пошкодження вихідних даних можуть бути неправильне використання обмежувачів даних, невірні параметри з’єднання і невідповідно налаштовані принтери.

**Проблеми захисту даних у процесі обробці**

Захист даних від некоректних змін під час обробки може мати негативний вплив. Помилки програмного забезпечення є причиною багатьох невдач і катастроф. Наприклад, всього за два тижні до Різдва деякі зі сторонніх роздрібних продавців Amazon випадково виставили ціну в один цент на свої товари. Збій тривав одну годину. Помилка призвела до того, що тисячі покупців придбали за безцінь товари, а компанії втратила дохід. У 2016 році термостат Nest зазнав збій і залишив користувачів без тепла. Термостат Nest - це інтелектуальна технологія, що належить Google. Збій програмного забезпечення залишив користувачів, буквально, на холоді. Проблеми з оновленням програмного забезпечення призвели до розрядки акумуляторів пристрою, через що не було можливості контролювати температуру. В результаті клієнти не змогли нагріти свої будинки або отримати гарячу воду в один з найхолодніших вихідних в році.

Для захисту даних під час обробки потрібні ретельно спроектовані системи. Фахівці з кібербезпеки розробляють політики та процедури, які вимагають тестування, обслуговування та оновлення систем, щоб вони працювали з найменшою кількістю помилок.



**Технології захисту на основі програмного забезпечення**

Програмні засоби захисту - це програми і служби, які захищають операційні системи, бази даних та інші служби, що працюють на робочих станціях, портативних пристроях і серверах. Адміністратори встановлюють програмні запобіжні засоби на окремих хостах або серверах. Існує кілька програмних технологій, які використовуються для захисту даних організації:

* Брандмауери керують віддаленим доступом до системи. Зазвичай брандмаурер входить до складу операційних систем, або користувач може придбати чи завантажити брандмауер від інших виробників.
* Сканери мережі та портів виявляють і контролюють відкриті порти на хості або сервері.
* Аналізатори протоколів або аналізатори сигнатур - це пристрої, які збирають і досліджують мережний трафік. Вони виявляють проблеми з продуктивністю, неправильні конфігурації, додатки, що некоректно працюють, визначають шаблони типового та нормального трафіку і усувають (налагоджують) проблеми зі зв'язком.
* Сканери вразливостей - це комп'ютерні програми, призначені для оцінки слабких місць комп'ютерів або мереж.
* Системи виявлення вторгнень на базі хоста (IDS) перевіряють активність тільки на хост-системах. IDS генерує лог-файли (записи у системному журналі) та попереджувальні повідомлення при виявленні незвичної активності. Система, яка зберігає конфіденційні дані або надає критично важливі, може бути цільовою для використання системи виявлення вторгнень на базі хостів (IDS).

**Апаратні засоби захисту**

Існує кілька апаратних технологій, що використовуються для захисту даних організацій:

* Брандмауер (апаратний) блокує небажаний трафік на основі правил, які визначають вхідний і вихідний трафік, дозволений у мережі.
* Спеціалізовані системи виявлення вторгнень (IDS) виявляють ознаки атак або незвичного трафіку в мережі і надсилають сповіщення.
* Системи запобігання вторгненням (Intrusion Prevention Systems - IPS) виявляють ознаки атак або незвичного трафіку в мережі, генерують попередження і вживають коригувальних дій.
* Служби фільтрування контенту контролюють доступ і передачу небажаного або образливого вмісту.

