**Розділ 6. Концепція п'яти дев'яток**

Організації, які хочуть максимально збільшити доступність своїх систем і даних, можуть вживати надзвичайних заходів для мінімізації або усунення втрат даних. Мета полягає в тому, щоб звести до мінімуму час простою критично важливих процесів. Якщо працівники не можуть виконувати свої регулярні обов'язки, організація може втратити свої прибутки.

Організації вимірюють доступність у відсотках безперебійної роботи. Цей розділ починається з пояснення концепції п'яти дев'яток. Багато галузей повинні підтримувати найвищі стандарти доступності, оскільки час простою може означати різницю між життям і смертю.

У цьому розділі розглядаються різні підходи, які можуть вжити організації для досягнення їхніх цілей доступності. Резервування забезпечує резервне копіювання та містить додаткові компоненти для комп'ютерів або мережних систем, щоб забезпечити їх доступність. Резервні компоненти можуть включати в себе обладнання, таке як диски, сервери, комутатори і маршрутизатори або програмне забезпечення, таке як операційні системи, програми та бази даних. У розділі також обговорюється відмовостійкість, здатність сервера, мережі або центру обробки даних швидко відновлюватися і продовжувати роботу.

Організації повинні бути готові реагувати на інцидент, встановлюючи процедури, які вони виконують, після того, як відбулася подія. Наприкінці розділу обговорюється планування аварійного відновлення і безперервності бізнесу, яке має вирішальне значення для підтримки доступності ресурсів організації.

**Що означає п'ять дев'яток?**

П'ять дев'яток означають, що системи і служби доступні в 99,999% випадків. Це також означає, що як запланований, так і незапланований час простою становить менше 5,26 хвилин на рік. На рисунку наведено порівняння часу простоїв для різних відсотків доступності.

Висока доступність залежить від системи чи компонентів, які постійно працюють на певному проміжку часу. Для забезпечення високої доступності необхідно:

* Усунення окремих точок збою
* Дизайн для надійності
* Виявлення несправностей, коли вони виникають

Підтримка високої доступності за стандартом п'яти дев'яток може збільшити витрати та використовувати багато ресурсів. Збільшені витрати пов'язані з придбанням додаткового устаткування, такого як сервери та компоненти. Оскільки організація додає компоненти і, як результат, збільшується складність конфігурації. На жаль, підвищена складність конфігурації збільшує фактори ризику. Чим більше рухомих частин задіяно, тим більша ймовірність відмови компонентів.

# 

# Середовища, які вимагають п'яти дев'яток

Хоча витрати на підтримку високої доступності можуть бути надто великими для деяких галузей, для окремих організацій п'ять дев'яток є необхідними.

* Фінансовій індустрії необхідно підтримувати високу доступність для постійної торгівлі, відповідаючи довірі клієнтів. Натисніть [тут](http://www.datacenterdynamics.com/it-networks/new-york-stock-exchange-fails-due-to-configuration-problems/94401.article) щоб прочитати про чотири години простою на Нью-Йоркській фондовій біржі в 2015 році.
* Оздоровчі установи вимагають високої доступності, щоб забезпечити цілодобовий догляд пацієнтів. Натисніть [тут](http://www.fiercehealthit.com/story/data-center-downtime-cost-averages-7900-minute/2013-12-05) щоб прочитати про середні витрати, пов'язані з простоєм центру обробки даних в галузі охорони здоров'я.
* Індустрія охорони громадської безпеки включає в себе агентства, які забезпечують безпеку та обслуговування спільноти, держави чи нації. Натисніть [тут](http://www.nextgov.com/defense/2014/05/pentagon-police-agency-hit-catastrophic-network-outage/83842/) щоб прочитати про відключення мережі в поліцейському агентстві США Пентагону.
* Роздрібна торгівля залежить від ефективних ланцюгів постачання та доставки продуктів споживачам. Збитки можуть бути руйнівними, особливо під час періодів високого попиту, таких як святкові дні.
* Люди сподіваються, що галузь новин передаватиме інформацію про події, коли вони стаються. Цикл новин працює цілодобово, 24/7.

# 

# Загрози доступності

Наступні загрози представляють високий ризик доступності даних і інформації:

* Несанкціонований користувач успішно проникає і компрометує основну базу даних організації
* Успішна DoS атака значною мірою впливає на операції
* Організація страждає від значної втрати конфіденційних даних
* Критично важливе ПЗ перестає працювати
* Стається компрометація адміністратора або root користувача
* Виявлення міжсайтового скрипта або незаконного загального доступу до файлового сервера
* Пошкодження веб-сайту організації впливає на зв'язок з громадськістю
* Сильний шторм, такий як ураган або торнадо
* Катастрофічні події, такі як терористичні акти, підрив або підпал будівель
* Довгостроковий збій служб або постачальника послуг
* Збиток від води в результаті повені або відмови зрошувальної системи

Класифікація рівня впливу для кожної загрози допомагає організації оцінити вплив загрози у доларах. Натисніть на категорії загроз на рисунку, щоб побачити приклад кожної з них.

# 

# Проектування системи високої доступності

Висока доступність включає три основні принципи досягнення мети безперервного доступу до даних та послуг:

1. Ліквідація або зменшення одиничних точок відмови

2. Системна стійкість

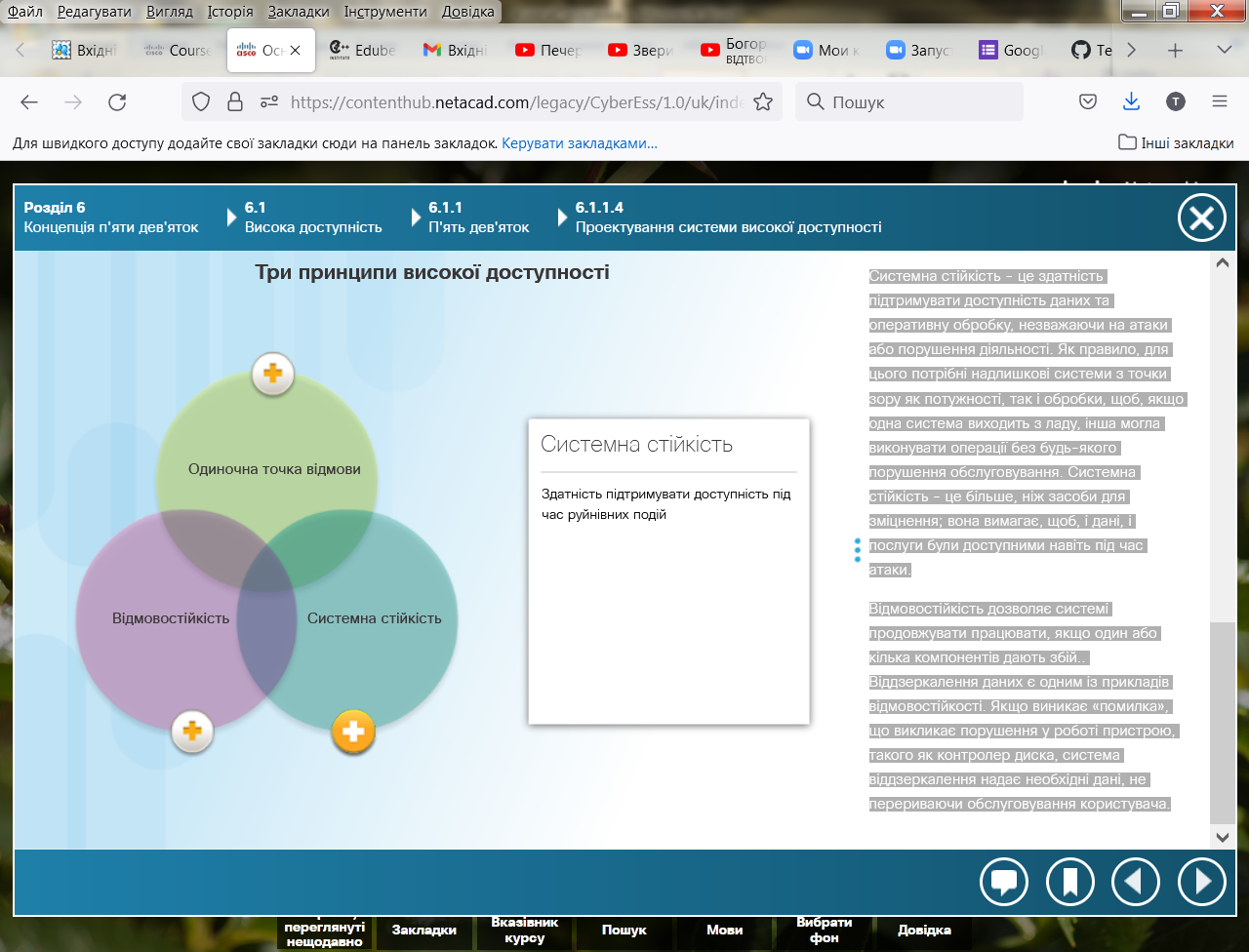
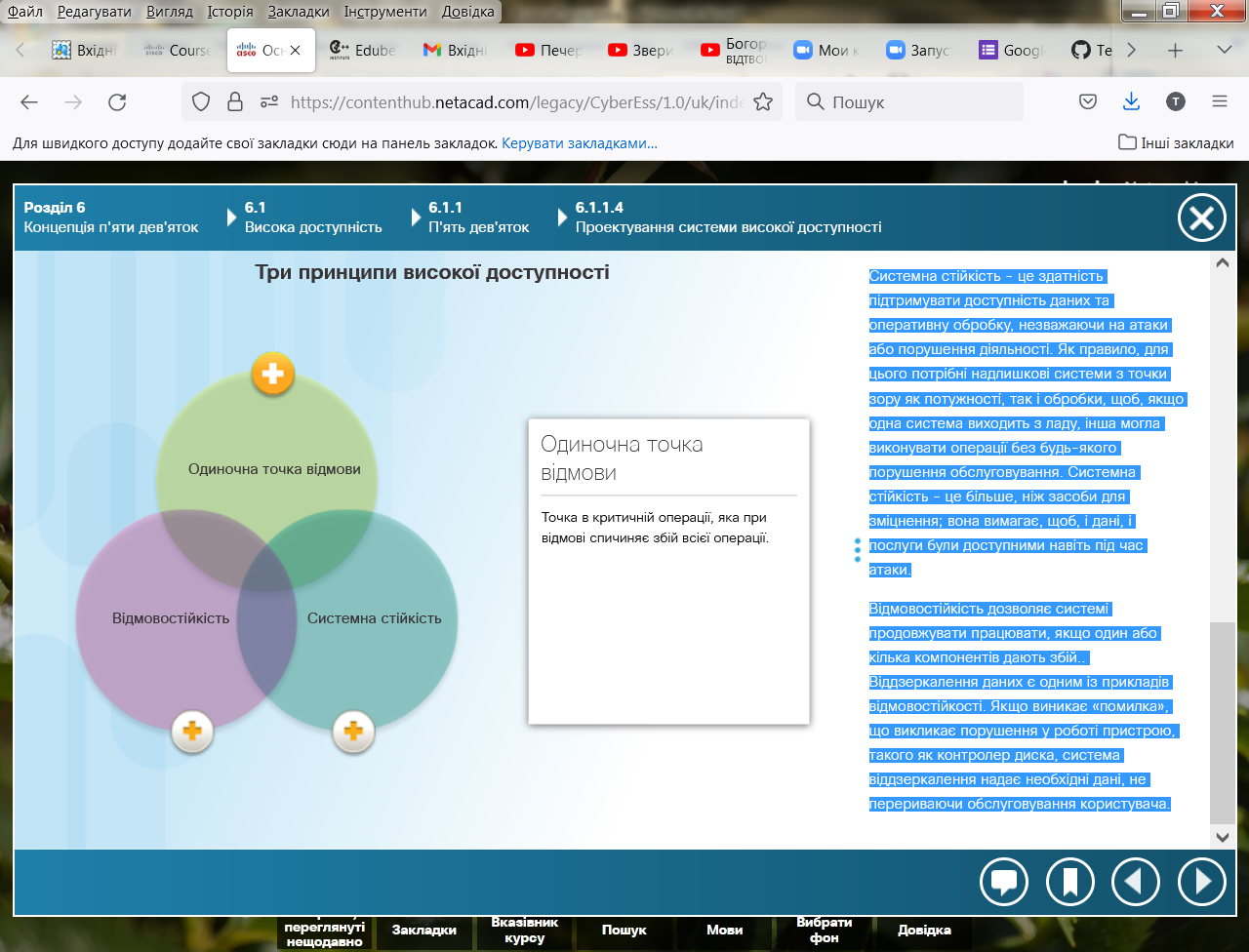
3. Відмовостійкість

Натисніть на кожен принцип на рисунку для короткого опису.

Важливо розуміти шляхи вирішення єдиної точки відмови. Одиничною точкою відмови може бути центральний маршрутизатор або комутатор, мережні служби та навіть висококваліфікований ІТ персонал. Ключовим є те, що втрата системи, процесу або людини може мати дуже руйнівний вплив на всю систему. Також ключовими є процеси, ресурси та компоненти, які зменшують кількість одиничних точок відмови. Кластери з високою доступністю - це один із способів забезпечення надлишковості. Ці кластери складаються з групи комп'ютерів, які мають доступ до спільного сховища та володіють ідентичними конфігураціями мережі. Всі сервери беруть участь у обробці служби одночасно. Зовні серверна група виглядає як один пристрій. Якщо сервер в кластері перестає працювати, інші сервери продовжують обробляти ту ж саму службу, що й пристрій, який вийшов з ладу.

Системна стійкість - це здатність підтримувати доступність даних та оперативну обробку, незважаючи на атаки або порушення діяльності. Як правило, для цього потрібні надлишкові системи з точки зору як потужності, так і обробки, щоб, якщо одна система виходить з ладу, інша могла виконувати операції без будь-якого порушення обслуговування. Системна стійкість - це більше, ніж засоби для зміцнення; вона вимагає, щоб, і дані, і послуги були доступними навіть під час атаки.

Відмовостійкість дозволяє системі продовжувати працювати, якщо один або кілька компонентів дають збій.. Віддзеркалення даних є одним із прикладів відмовостійкості. Якщо виникає «помилка», що викликає порушення у роботі пристрою, такого як контролер диска, система віддзеркалення надає необхідні дані, не перериваючи обслуговування користувача.



# 

# Ідентифікація активів

Організація повинна знати, яке апаратне і програмне забезпечення є в наявності, як передумова для визначення необхідних параметрів конфігурації. Керування активами включає в себе повну інвентаризацію апаратного та програмного забезпечення.

Це означає, що організація повинна знати всі компоненти, які можуть піддаватися ризикам безпеки, зокрема:

* Кожна апаратна система
* Кожна операційна система
* Кожний апаратний мережний пристрій
* Кожна операційна система мережного пристрою
* Кожний програмний застосунок
* Вся прошивка
* Усі мовні середовища виконання
* Всі окремі бібліотеки

Організація може вибрати автоматичне рішення для відстеження активів. Адміністратор повинен досліджувати будь-яку змінену конфігурацію, оскільки це може означати, що конфігурація не є актуальною. Це також може означати, що відбуваються несанкціоновані зміни.



**Класифікація активів**

Класифікація активів розподіляє всі ресурси організації у групи, засновані на спільних характеристиках. Організація повинна застосовувати систему класифікації активів до документів, записів даних, файлів та дисків. Найважливіша інформація повинна отримувати найвищий рівень захисту і навіть може вимагати спеціальної обробки.

Організація може прийняти систему маркування відповідно до того, наскільки цінною, чутливою і критичною є інформація. Щоб визначити та класифікувати активи організації, виконайте наступні кроки:

1. Визначити правильну категорію ідентифікації активів.

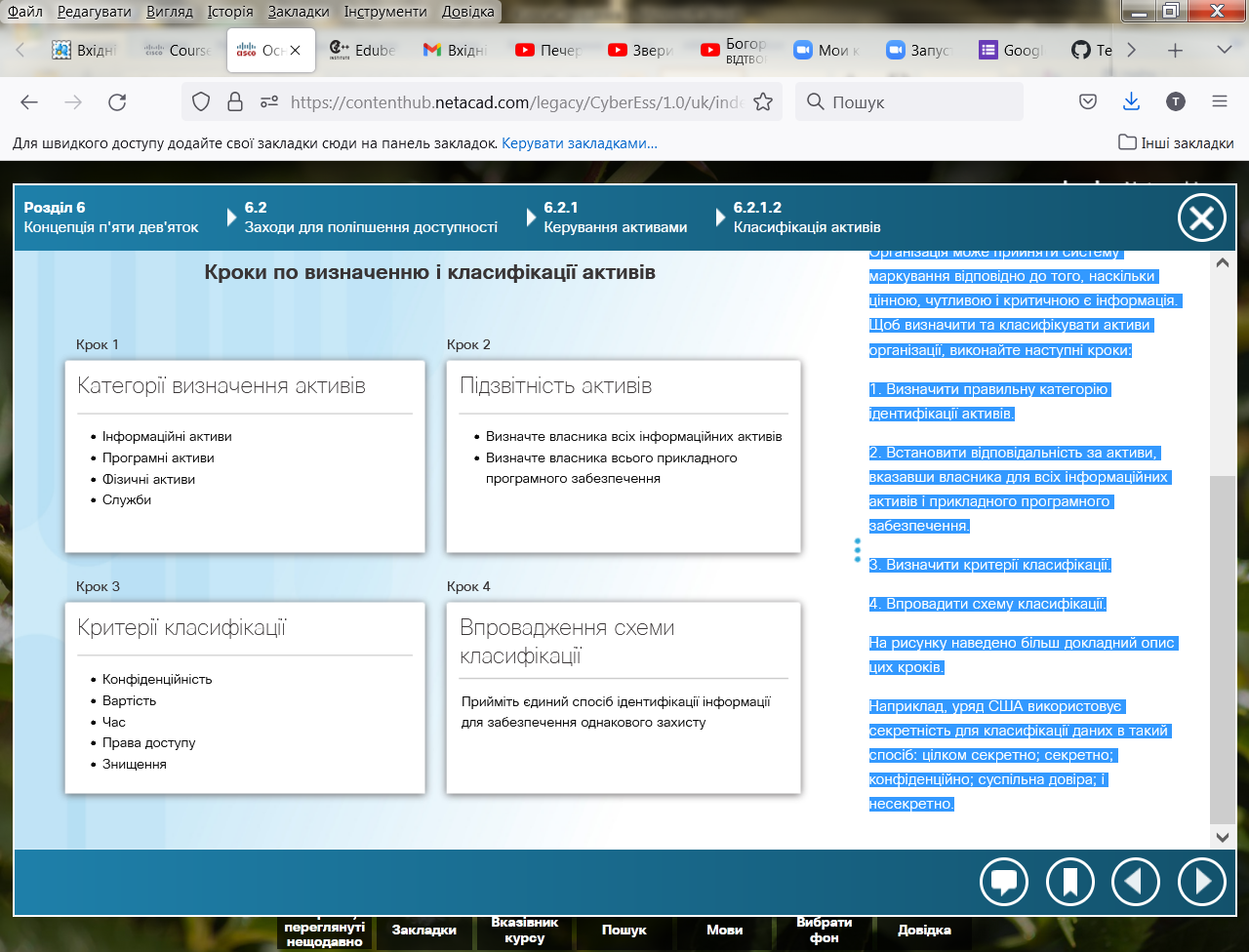
2. Встановити відповідальність за активи, вказавши власника для всіх інформаційних активів і прикладного програмного забезпечення.

3. Визначити критерії класифікації.

4. Впровадити схему класифікації.

На рисунку наведено більш докладний опис цих кроків.

Наприклад, уряд США використовує секретність для класифікації даних в такий спосіб: цілком секретно; секретно; конфіденційно; суспільна довіра; і несекретно.



# Стандартизація активів

Керування активами керує життєвим циклом і інвентаризацією технологічних активів, включаючи пристрої та програмне забезпечення. В рамках системи керування ІТ-активами організація визначає прийнятні ІТ-активи, які відповідають її цілям. Ця практика ефективно зменшує різні типи активів. Наприклад, організація буде встановлювати застосунки, що відповідатимуть їхнім рекомендаціям. Коли адміністратори вилучають програми, які не відповідають рекомендаціям, вони ефективно підвищують безпеку.

Стандарти активів визначають конкретні апаратні та програмні продукти, які використовує та підтримує організація. Коли відбувається збій, оперативне реагування допомагає підтримувати як доступ, так і безпеку. Якщо організація не стандартизує вибір свого апаратного забезпечення, персоналу може бути потрібен час, щоб знайти компонент для заміни. Нестандартні середовища вимагають більшого досвіду для керування і вони збільшують вартість контрактів на технічне обслуговування та інвентаризацію. Натисніть [тут](http://mil-embedded.com/articles/the-cots-systems-play/) щоб прочитати про те, як військові перейшли на стандартні апаратні засоби для своїх військових комунікацій.

# Ідентифікація загроз

Комп'ютерна команда екстреної готовності США (US-CERT) та Міністерство внутрішньої безпеки США підтримують словник загальної уразливості і впливу (CVE). CVE містить стандартний ідентифікаційний номер з коротким описом і посилання на відповідні звіти про уразливості та рекомендації. Корпорація MITRE підтримує список CVE та його загальнодоступний веб-сайт.

Ідентифікація загрози починається з процесу створення ідентифікатора CVE для загальнодоступних вразливостей кібербезпеки. Кожен ідентифікатор CVE включає в себе наступне:

* Номер ідентифікатора CVE
* Короткий опис вразливості системи безпеки
* Будь-які важливі посилання

Натисніть [тут](http://cve.mitre.org/cve/identifiers/) щоб дізнатись більше про ідентифікатор CVE.

**Аналіз ризиків**

Аналіз ризиків - це процес аналізу небезпек, пов'язаних з природними та антропогенними подіями, для активів організації.

Користувач виконує ідентифікацію активів, щоб визначити, які активи захищати. Аналіз ризиків має чотири мети:

* Визначення активів та їх вартості
* Визначення вразливості та загроз
* Оцінити ймовірність та вплив виявлених загроз
* Збалансувати вплив загрози на вартість контрзаходів

Є два підходи до аналізу ризиків.

**Кількісний аналіз ризиків**

Кількісний аналіз присвоює числа процесу аналізу ризиків (Рисунок 1). Вартість активу - це вартість заміщення активу. Вартість активу також може бути виміряна доходами, отриманими за рахунок використання активу. Коефінієнт впливу (EF) являє собою суб'єктивне значення, виражене у відсотках, яке активи втрачають через конкретну загрозу. Якщо відбувається повна втрата, EF дорівнює 1,0 (100%). У кількісному прикладі, сервер має вартість активу 15 000 доларів США. Коли сервер не працює, відбувається загальна втрата (EF дорівнює 1,0). Вартість активу в розмірі 15 000 доларів, помножена на коефіцієнт впливу 1, призводить до одиночної очікуваної втрати у розмірі 15 000 доларів США.

Річна ставка виникнення (ARO) - ймовірність того, що збиток відбудеться протягом року (також виражається у відсотках). ARO може бути більшим, ніж 100%, якщо збиток може виникати більше одного разу на рік.

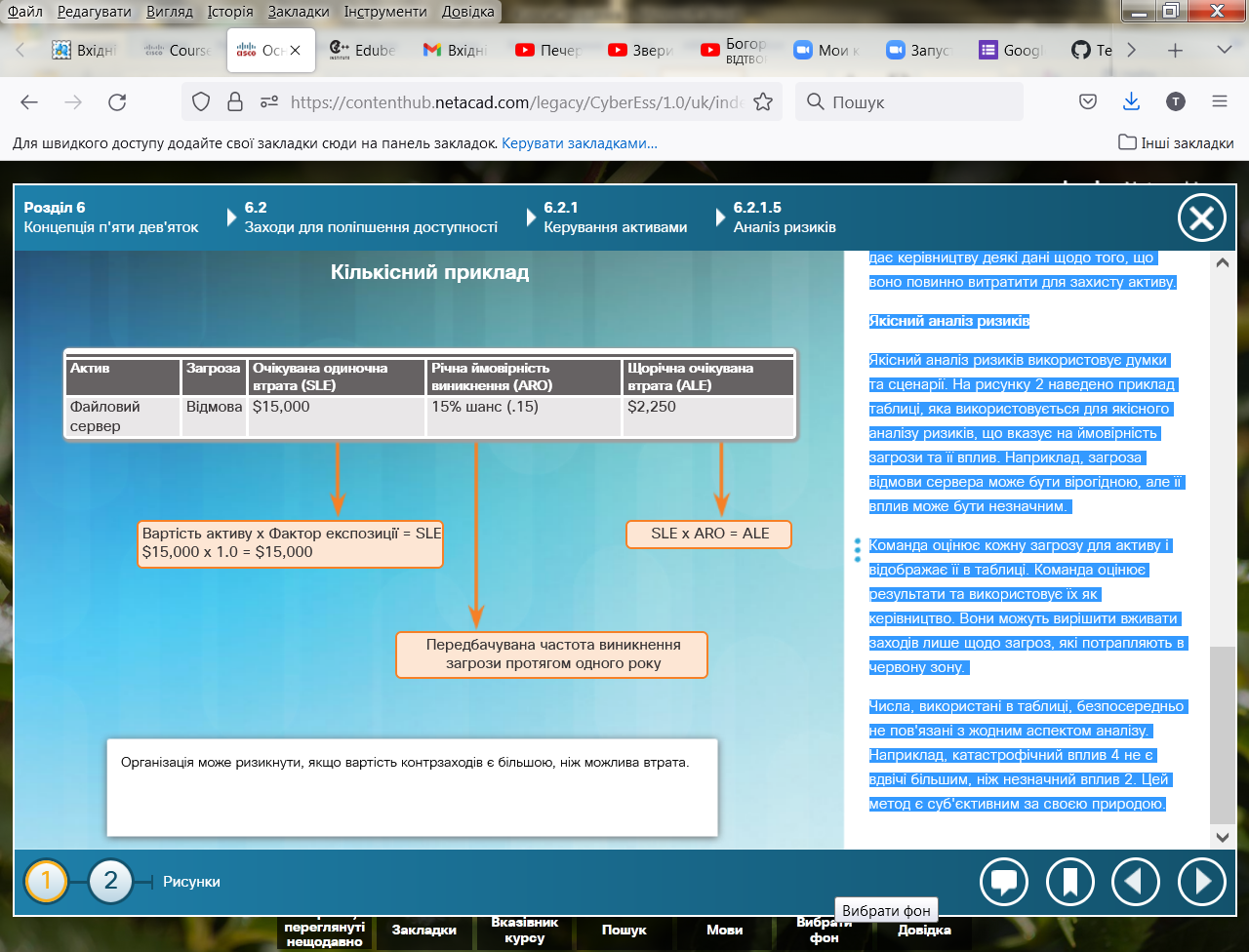
Розрахунок щорічної очікуваної втрати (ALE) дає керівництву деякі дані щодо того, що воно повинно витратити для захисту активу.

**Якісний аналіз ризиків**

Якісний аналіз ризиків використовує думки та сценарії. На рисунку 2 наведено приклад таблиці, яка використовується для якісного аналізу ризиків, що вказує на ймовірність загрози та її вплив. Наприклад, загроза відмови сервера може бути вірогідною, але її вплив може бути незначним.

Команда оцінює кожну загрозу для активу і відображає її в таблиці. Команда оцінює результати та використовує їх як керівництво. Вони можуть вирішити вживати заходів лише щодо загроз, які потрапляють в червону зону.

Числа, використані в таблиці, безпосередньо не пов'язані з жодним аспектом аналізу. Наприклад, катастрофічний вплив 4 не є вдвічі більшим, ніж незначний вплив 2. Цей метод є суб'єктивним за своєю природою.



# 

# Пом'якшення

Пом'якшення наслідків передбачає зменшення тяжкості чи ймовірності втрати. Багато технічних засобів керування знижують ризик, включаючи системи аутентифікації, дозволи на доступ до файлів і брандмауери. Спеціалісти з організації та безпеки повинні розуміти, що зменшення ризику може мати як позитивний, так і негативний вплив на організацію. Гарне пом'якшення ризиків знаходить баланс між негативним впливом контрзаходів і контролю і вигодою від зниження ризику. Існує чотири загальні способи зменшення ризику:

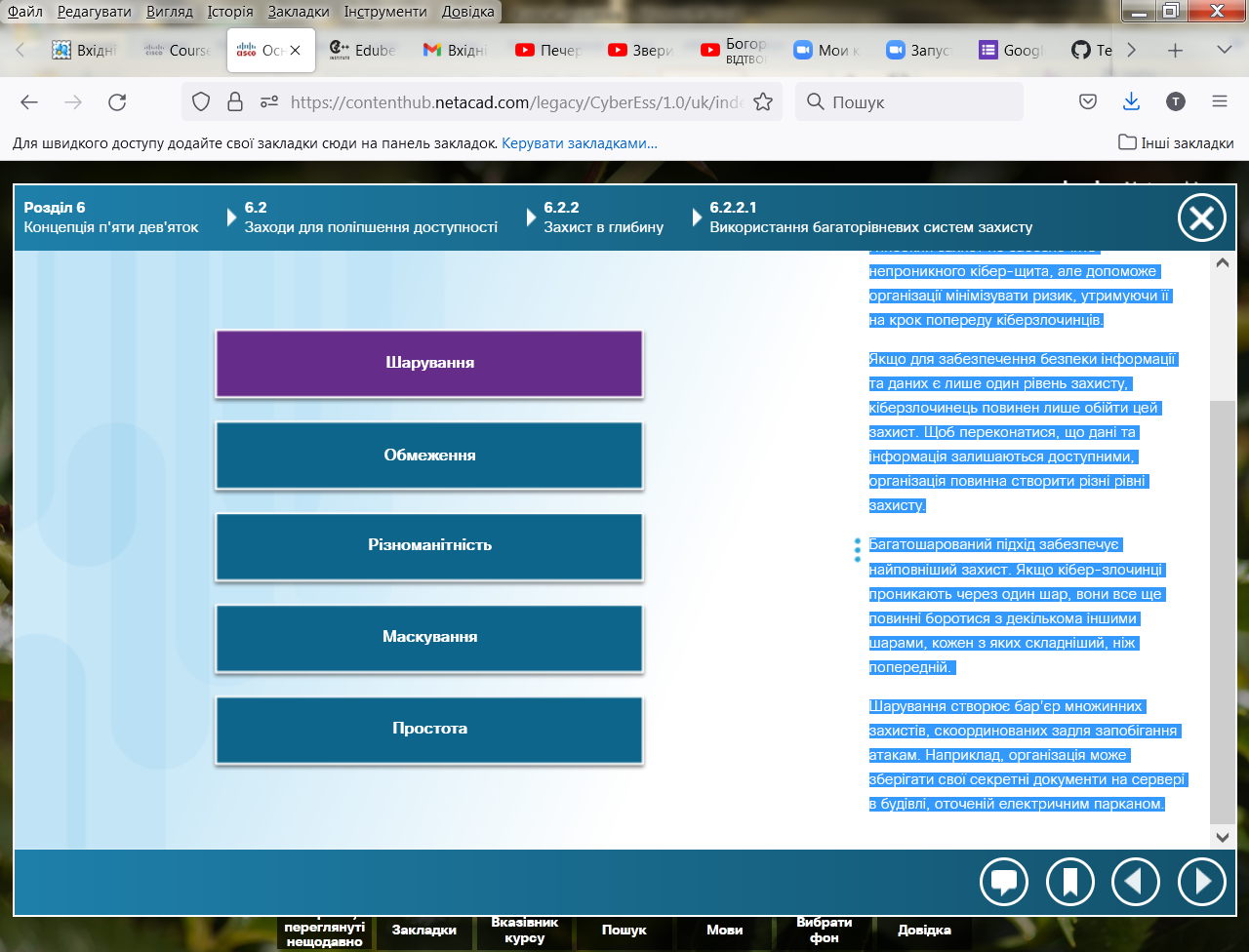
* Прийняти ризик і періодично повторно оцінювати його
* Знизити ризик шляхом впровадження засобів контролю
* Уникати ризику шляхом повної зміни підходу
* Передати ризик третій стороні

Короткострокова стратегія полягає у прийнятті ризику, що вимагає створення планів на випадок надзвичайних ситуацій для цього ризику. Люди та організації повинні приймати ризик на щоденній основі. Сучасні методології знижують ризик, розвиваючи програмне забезпечення поступово, надаючи регулярні оновлення та виправлення для усунення вразливостей та неправильних конфігурацій.

Аутсорсингові послуги, придбання страхування або контрактів на обслуговування - це все приклади передачі ризиків. Наймання фахівців для виконання критичних завдань для зменшення ризику може бути хорошим рішенням і забезпечувати кращі результати при менш довгострокових інвестиціях. Хороший план зменшення ризику може включати дві або більше стратегії.

# 

# Використання багаторівневих систем захисту

Глибокий захист не забезпечить непроникного кібер-щита, але допоможе організації мінімізувати ризик, утримуючи її на крок попереду кіберзлочинців.

Якщо для забезпечення безпеки інформації та даних є лише один рівень захисту, кіберзлочинець повинен лише обійти цей захист. Щоб переконатися, що дані та інформація залишаються доступними, організація повинна створити різні рівні захисту.

Багатошарований підхід забезпечує найповніший захист. Якщо кібер-злочинці проникають через один шар, вони все ще повинні боротися з декількома іншими шарами, кожен з яких складніший, ніж попередній.

Шарування створює бар'єр множинних захистів, скоординованих задля запобігання атакам. Наприклад, організація може зберігати свої секретні документи на сервері в будівлі, оточеній електричним парканом.

# Обмеження

Обмеження доступу до даних та інформації зменшує можливість загрози. Організація повинна обмежувати доступ, щоб користувачі мали лише рівень доступу, необхідний для виконання своєї роботи. Наприклад, люди в відділі маркетингу не потребують доступу до записів заробітної плати для виконання своїх робочих обов’язків.

Технологічні рішення, такі як використання дозволів файлів, є одним із способів обмеження доступу; організація також повинна виконувати процедурні заходи. Повинна бути передбачена процедура, яка забороняє працівникові виносити конфіденційні документи з приміщення.

# Різноманітність

Якби всі захищені шари були однаковими, для кіберзлочинців було б дуже просто провести успішну атаку. Тому шари повинні бути різними. Якщо кібер-злочинці проникнуть в один шар, то ж техніка не буде працювати на всіх інших шарах. Порушення одного рівня безпеки не ставить під загрозу всю систему. Організація може використовувати різні алгоритми шифрування або системи автентифікації для захисту даних у різних станах.

Для досягнення різноманітності організації можуть використовувати продукти безпеки, вироблені різними компаніями, для багатофакторної аутентифікації. Наприклад, сервер, що містить надзвичайно секретні документи, знаходиться в заблокованій кімнаті, де потрібна swipe-картка від однієї компанії та біометрична автентифікація, надана іншою компанією.

# Маскування

Маскування інформації також може захистити дані та інформацію. Організація не повинна розкривати будь-яку інформацію, яку кіберзлочинці можуть використовувати, щоб з'ясувати, яка версія операційної системи працює на сервері або тип використовуваного ним обладнання. Наприклад, повідомлення про помилки не повинні містити жодних відомостей, які кіберзлочинці могли б використати для визначення наявних вразливостей. Приховування певних типів інформації ускладнює зловмисникам боротьбу з системою.

# Простота

Складність не обов'язково гарантує безпеку. Якщо організація запроваджує складні системи, які важкі для зрозуміння і усування несправностей, це може значно послабити систему. Якщо працівники не розуміють, як належним чином налаштовувати складні рішення, може статися так, що кібер-злочинці зможуть скомпрометувати ці системи. Щоб забезпечити доступність, рішення безпеки має бути простим зсередини, але складним ззовні.

# Одиночні точки відмови

Єдина точка відмови - це критична операція всередині організації. Інші операції можуть залежати від неї, а відмова припиняє цю критичну операцію. Єдиною точкою відмови може бути конкретна частина апаратного забезпечення, процес, конкретний фрагмент даних або навіть найважливіша утиліта. Точками відмови є слабкі ланки ланцюга, які можуть спричинити зрив роботи організації. Як правило, для вирішення проблеми єдиної точки відмови потрібно змінити критичну операцію так, щоб вона не покладалася лише на один елемент. Також при виконанні критичних операцій організація може вбудовувати резервні компоненти, які б могли перебрати на себе процес, якщо одна з цих точок відмовить

**N + 1 Резервування**

Резервування за принципом N + 1 забезпечує доступність системи у разі відмови компонента. Компоненти (N) повинні мати щонайменше один резервний компонент (+1). Наприклад, в автомобілі є чотири шини (N) та запасна шина у багажнику на випадок проколу (+1).

У центрі обробки даних N + 1 означає, що конструкція системи може протистояти втраті компонента. N відноситься до багатьох різних компонентів, які складають центр обробки даних, включаючи сервери, блоки живлення, комутатори та маршрутизатори. +1 є додатковим компонентом або резервною системою, яка зможе долучитися до роботи, якщо буде потрібно.

Прикладом резервування N + 1 в центрі обробки даних є генератор енергії, який починає працювати, коли щось трапляється з основним джерелом живлення. Хоча система N + 1 містить резервне обладнання, вона не є повністю резервованою системою.

# RAID

Надлишковий масив незалежних дисків (RAID) поєднує в собі декілька фізичних жорстких дисків в єдиний логічний блок, що забезпечує надмірність даних та покращує продуктивність. RAID приймає дані, які зазвичай зберігаються на одному диску і поширює їх на декілька дисків. Якщо деякий диск вийде з ладу, користувач зможе відновити дані з інших дисків, які також містять ці дані.

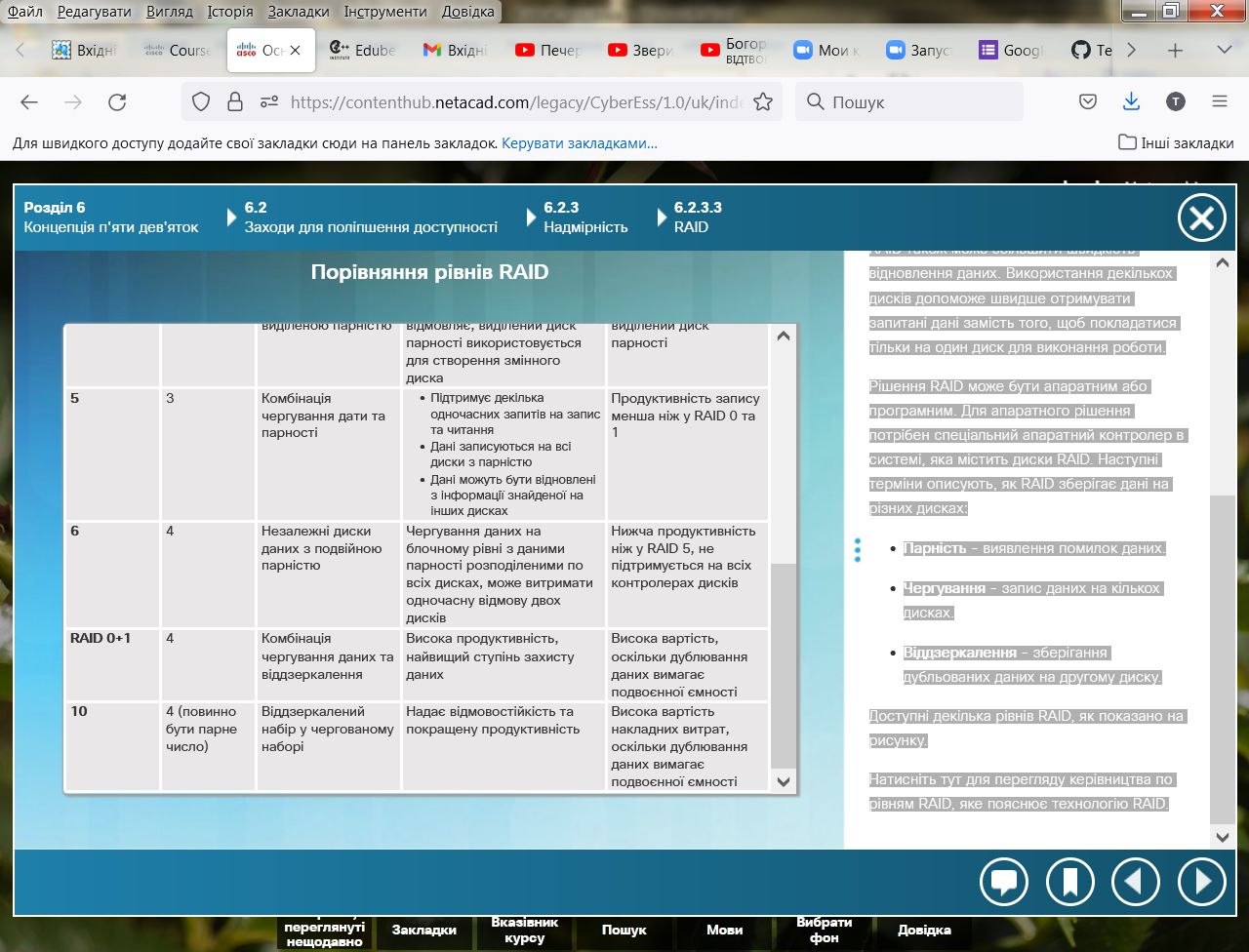
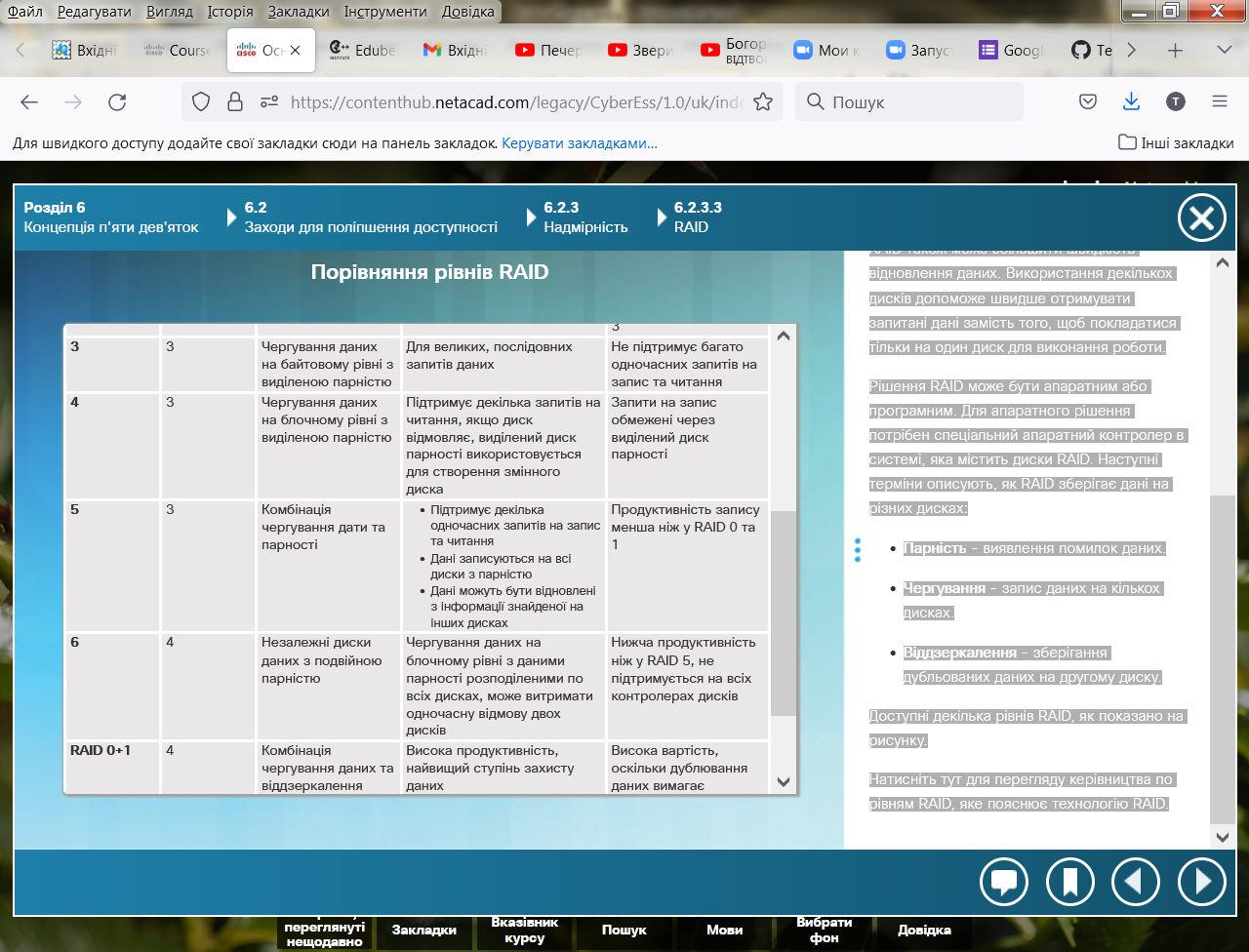
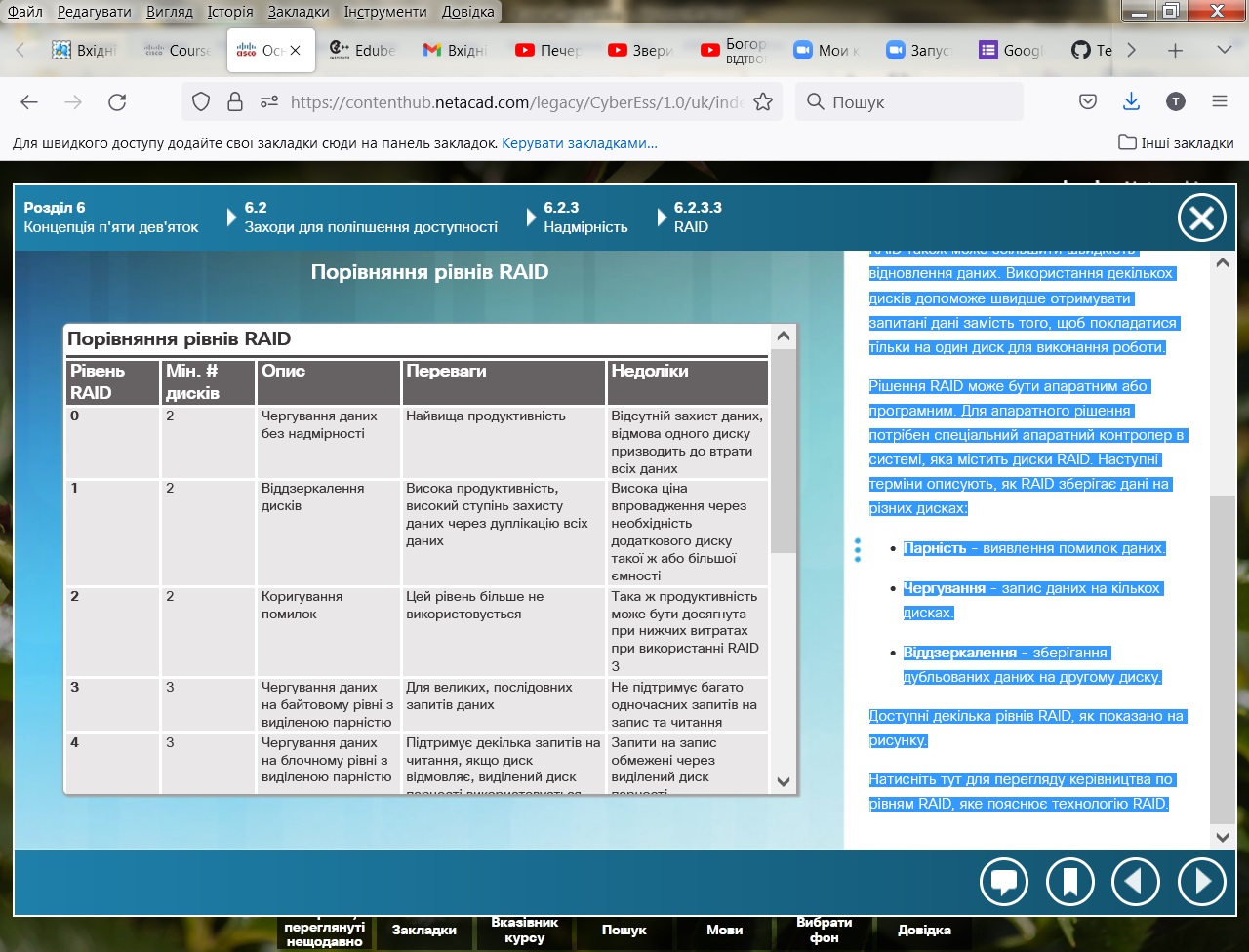
RAID також може збільшити швидкість відновлення даних. Використання декількох дисків допоможе швидше отримувати запитані дані замість того, щоб покладатися тільки на один диск для виконання роботи.

Рішення RAID може бути апаратним або програмним. Для апаратного рішення потрібен спеціальний апаратний контролер в системі, яка містить диски RAID. Наступні терміни описують, як RAID зберігає дані на різних дисках:

* **Парність** - виявлення помилок даних.
* **Чергування** - запис даних на кількох дисках.
* **Віддзеркалення** - зберігання дубльованих даних на другому диску.

Доступні декілька рівнів RAID, як показано на рисунку.

Натисніть [тут](http://www.acnc.com/raid) для перегляду керівництва по рівням RAID, яке пояснює технологію RAID.



**Остовне дерево**

Надлишковість покращує доступність інфраструктури, захищаючи мережу від єдиної точки відмови, наприклад, відімкнення мережного кабелю або несправності комутатора. При проектуванні фізичної надлишковості у мережі, можуть виникати зациклювання та дублювання кадрів , які матимуть серйозні негативні наслідки для комутованої мережі.

Протокол остовного дерева (Spanning Tree Protocol) вирішує ці проблеми. Основна функція STP полягає в тому, щоб запобігти циклічності в мережі, коли комутатори з'єднуються через кілька шляхів. STP гарантує, що надмірні фізичні канали не мають петель. Це гарантує наявність лише одного логічного шляху між усіма пунктами призначення в мережі. STP навмисно блокує резервні шляхи, які можуть спричинити цикл.

Блокування надлишкових шляхів має вирішальне значення для запобігання циклів у мережі. Фізичні шляхи все ще існують для забезпечення надмірності, але STP вимикає ці шляхи, щоб запобігти виникненню циклів. Якщо мережний кабель або комутатор виходить з ладу, STP перераховує шляхи і розблоковує необхідні порти для активування резервного шляху.

Натисніть кнопку «Переглянути» на рисунку, щоб переглянути роботу STP, коли трапляється помилка:

* PC1 відправляє широкомовне повідомлення в мережу.
* Магістральна лінія між S2 та S1 вийшла з ладу, що призвело до порушення основного шляху.
* S2 розблоковує попередньо заблокований порт для Магісталі 2 і дозволить передавати широкомовний трафік альтернативним шляхом, не перериваючи з’єднання.
* Якщо зв'язок між S2 і S1 починає працювати знову, STP знову блокує зв'язок між S2 і S3.

# 

# Резервування маршрутизатора

Шлюз за замовчуванням (default gateway) зазвичай є маршрутизатором, який забезпечує доступ до іншої частини мережі або до Інтернету. Якщо як шлюз за замовчуванням використовується лише один маршрутизатор, він становить єдину точку відмови. Організація може встановити додатковий маршрутизатор в режим очікування.

На рисунку 1, маршрутизатор в режимі переадресації та маршрутизатор в режимі очікування використовують протокол резервування для визначення того, який маршрутизатор повинен відігравати активну роль при переадресації трафіку. На кожному маршрутизаторі налаштовується фізична IP-адреса та IP-адреса віртуального маршрутизатора. Кінцеві пристрої використовують віртуальну IP-адресу як шлюз за замовчуванням. Маршрутизатор, що передає трафік, очікує на дані, які прямують за адресою 192.0.2.100. Маршрутизатор переадресації та маршрутизатор очікування використовують свої фізичні IP-адреси для надсилання періодичних повідомлень. Ці повідомлення допомагають переконатися, що обидва маршрутизатори доступні і залишаються на зв'язку. Якщо резервний маршрутизатор у режимі очікування не отримує ці періодичні повідомлення від основного маршрутизатора, він перейде до виконання функції переадресації, як показано на рисунку 2.

Здатність мережі динамічно відновлюватися після відмови пристрою, який виконує функції шлюзу, відома як надлишковість першого кроку.

# 

2

1

# Параметри резервування маршрутизатора

Наведений нижче список визначає параметри доступні для резервування маршрутизатора на основі протоколу, який забезпечує зв'язок між мережними пристроями:

* **Hot Standby Router Protocol(HSRP)** - HSRP гарантує високу доступність мережі, забезпечуючи надлишковість маршрутизації першого кроку. Група маршрутизаторів використовує HSRP для вибору активного пристрою та пристрою очікування. У групі інтерфейсів пристрою активним вважається той пристрій, що направляє пакети, а резервним – той, що починає працювати при виході з ладу активного пристрою. Резервний маршрутизатор HSRP контролює робочий статус групи HSRP та швидко бере на себе відповідальність за переадресацію пакетів, якщо активний маршрутизатор відмовляє.
* **Virtual Router Redundancy Protocol (VRRP)** - маршрутизатор VRRP запускає протокол VRRP разом з одним або кількома іншими маршрутизаторами, підключеними до локальної мережі. У конфігурації VRRP обраний маршрутизатор є головним віртуальним маршрутизатором, а інші маршрутизатори є запасними на випадок відмови головного віртуального маршрутизатора.
* **Gateway Load Balancing Protocol (GLBP)** - GLBP захищає трафік даних від відмов маршрутизатора або схеми, наприклад HSRP і VRRP, а також дозволяє балансувати навантаження (також відоме як розподіл навантаження) між елементами групи резервних маршрутизаторів.