**Резервне розташування**

Організації може знадобитись резервне розташування в залежності від її потреб. Нижче описано три форми розміщення резервів.

**Синхронна**

* Синхронізує обидва місця в режимі реального часу
* Потребує високої пропускної здатності
* Місцеположення повинні бути близькими один до одного, щоб зменшити затримку

**Асинхронна реплікація**

* Не синхронізовано в реальному часі, але близько до цього
* Потребує меншої пропускної здатності
* Розташування можуть бути на більшій відстані, оскільки затримка не є проблемою

**Реплікація у певний момент часу**

* Періодично оновлює резервні копії даних
* Заощаджується більша частина пропускної здатності, оскільки схема не вимагає постійного з'єднання.

Належний баланс між вартістю та доступністю визначатиме правильний вибір для організації.

**Стійкий дизайн**

Стійкість - це методи і конфігурації, які використовуються для забезпечення стійкості системи або мережі до відмови. Наприклад, мережа може мати резервні зв'язки між комутаторами з запущеним STP. Хоча STP надає альтернативний шлях через мережу при виході з ладу з'єднання, перемикання може відбуватися не одразу, якщо конфігурація не оптимальна.

Протоколи маршрутизації також забезпечують стійкість, проте тонке налаштування може покращити перехід і зробити його непомітним для користувачів мережі. Адміністратори повинні досліджувати нестандартні налаштування в тестовій мережі, щоб дізнатися, чи можуть вони поліпшити час відновлення мережі.

Стійкий дизайн - це не просто додавання надлишковості. Дуже важливо розуміти бізнес-потреби організації, а потім включати резервність для створення стійкої мережі.

**Стійкість ПЗ**

Стійкість застосунків - це здатність застосунка реагувати на проблеми в одному зі своїх компонентів при роботі без припинення виконання. Час простою пов'язаний з відмовами, викликаними помилками застосунків або збоями інфраструктури. Адміністратор в кінцевому підсумку повинен закрити програми для виправлення, оновлення версій або для розгортання нових функцій. Час простою також може бути результатом пошкодження даних, збоїв обладнання, помилок застосунка і людських помилок.

Багато організацій намагаються збалансувати витрати на досягнення стійкості інфраструктури ПЗ ціною втрати клієнтів або бізнесу через збій програми. Висока доступність застосунка є складною і дорогою. На рисунку наведено три шляхи вирішення проблеми стійкості застосунків. Оскільки коефіцієнт доступності кожного рішення збільшується, складність і вартість також зростають.

# 

# Стійкість IOS

Cisco Internetwork Operating System (Cisco IOS) для маршрутизаторів і комутаторів включає в себе функцію стійкої конфігурації. Це дає змогу швидкого відновлення при зловмисному або ненавмисному форматуванні флеш-пам'яті або при видаленні конфігураційного файлу запуску. Ця функція підтримує безпечну робочу копію файлу образу IOS маршрутизатора і копію поточного файлу конфігурації. Користувач не може видалити ці захищені файли, також відомі як primary bootset.

Команди, показані на рисунку, захищають образ IOS та поточний файл конфігурації.

# 

**Підготовка**

Реакція на інцидент - це процедура, якій слідує організація після того, як подія виходить за рамки звичайного. Витік даних випускає інформацію до ненадійного середовища. Витік даних може виникнути в результаті випадкової або навмисної дії. Витік даних відбувається, коли неавторизована особа копіює, передає, переглядає, викрадає або отримує доступ до конфіденційної інформації.

Коли відбувається інцидент, організація повинна вміти реагувати на нього. Організація повинна розробити план реагування на інцидент та зібрати команду з реагування на інциденти в галузі комп'ютерної безпеки (Computer Security Incident Response Team) для керування реагуванням. Команда виконує наступні функції:

* Дотримується плану реагування на інцидент
* Турбується, щоб її члени знали про план
* Перевіряє план
* Отримує схвалення плану від керівництва

CSIRT може бути встановленою групою всередині організації або окремою організацією. Команда дотримується набору заздалегідь визначених кроків, щоб переконатись, що їхній підхід є рівномірним і що вони не пропускають жодних кроків. Національний CSIRT наглядає за інцидентами у країні.

**Виявлення та аналіз**

Виявлення починається, коли хтось помічає інцидент. Організації можуть придбати найсучасніші системи виявлення; однак, якщо адміністратори не переглядають журнали та моніторинг сповіщень, ці системи є марними. Правильне виявлення дає змогу зрозуміти як відбувався інцидент, які дані і системи він включає. Повідомлення про порушення поширюється на вище керівництво і керівників, відповідальних за дані і системи, щоб залучити їх до відновлення і ремонту. Виявлення та аналіз включають в себе наступне:

* Оповіщення та сповіщення
* Моніторинг та подальшу діяльність

Аналіз інциденту допомагає визначити джерело, ступінь, вплив та деталі витоку даних. Організація може вирішити, чи потрібно залучати команду експертів для проведення судової експертизи.

**Стримування і викорінення, а також відновлення**

Стримуючі зусилля включають негайні дії, такі як відключення системи від мережі, щоб зупинити витік інформації.

Після виявлення витоку організація повинна стримати та викорінити його. Це може потребувати додаткового простою для систем. Стадія відновлення включає в себе дії, які організація повинна вжити, щоб вирішити проблему та відновити задіяні системи. Після виправлення організація повинна відновити всі системи до їх первісного стану до інциденту.

**Спостереження за системою після інциденту**

Після відновлення нормального стану усіх операцій, організація повинна розглянути причину інциденту та поставити такі запитання:

* Які дії запобігатимуть повторенню інциденту?
* Які запобіжні заходи потребують зміцнення?
* Як це може покращити моніторинг системи?
* Як це може мінімізувати час простою під час процесу стримування, викорінення та відновлення?
* Як керування може мінімізувати вплив на бізнес?

Погляд на отриманий урок може допомогти організації краще підготуватися, вдосконалюючи свій план реагування на інциденти.

# Контроль доступу до мережі

Контроль доступу до мережі (Network Admission Control, NAC) дозволяє авторизованим користувачам з сумісними системами отримувати доступ до мережі. Сумісна система відповідає всім вимогам політики організації. Наприклад, ноутбук, який є частиною домашньої бездротової мережі, може не мати можливості дистанційного підключення до корпоративної мережі. NAC оцінює пристрій на відповідність політикам мережі. NAC також проводить карантин систем, які не відповідають вимогам та керує відновленням невідповідних систем.

Структура NAC може використовувати існуючу мережну інфраструктуру і додаткове програмне забезпечення для запровадження політики безпеки для усіх кінцевих точок. Окрім того, пристрій NAC контролює доступ до мережі, оцінює відповідність і застосовує політику безпеки. Загальні перевірки систем NAC включають:

1. Оновлення антивірусу

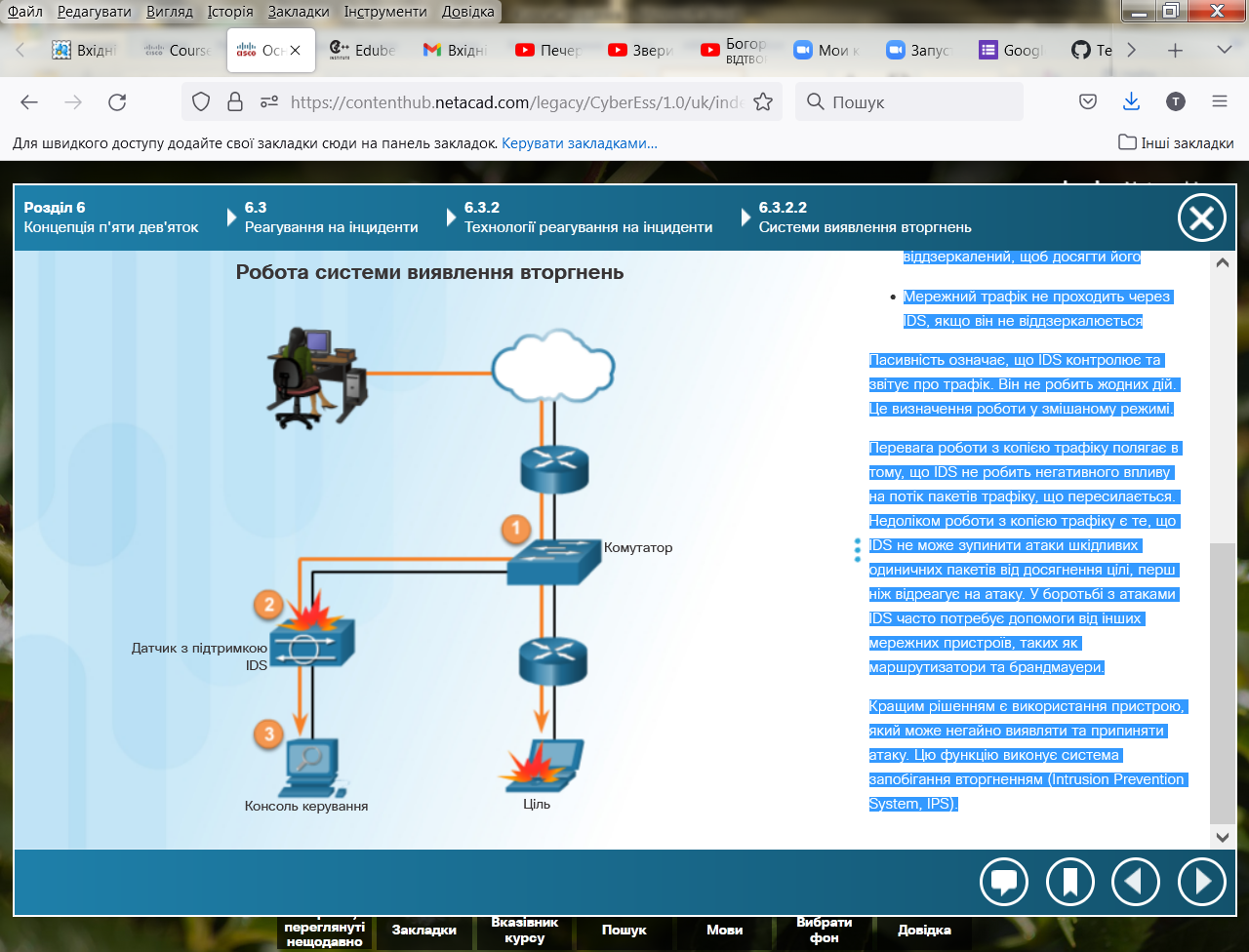
2. Патчі та оновлення операційних систем

3. Комплексний захист паролем

# 

# Системи виявлення вторгнень

Системи виявлення вторгнень (Intrusion Detection Systems) пасивно контролюють трафік у мережі. На рисунку показано, що пристрій з підтримкою IDS копіює потік трафіку та аналізує скопійований трафік, а не фактичні переадресовані пакети. Працюючи в автономному режимі, він порівнює захоплений потік трафіку з відомими шкідливими сигнатурами, аналогічно програмному забезпеченню, яке перевіряє наявність вірусів. Робота в автономному режимі означає кілька речей:

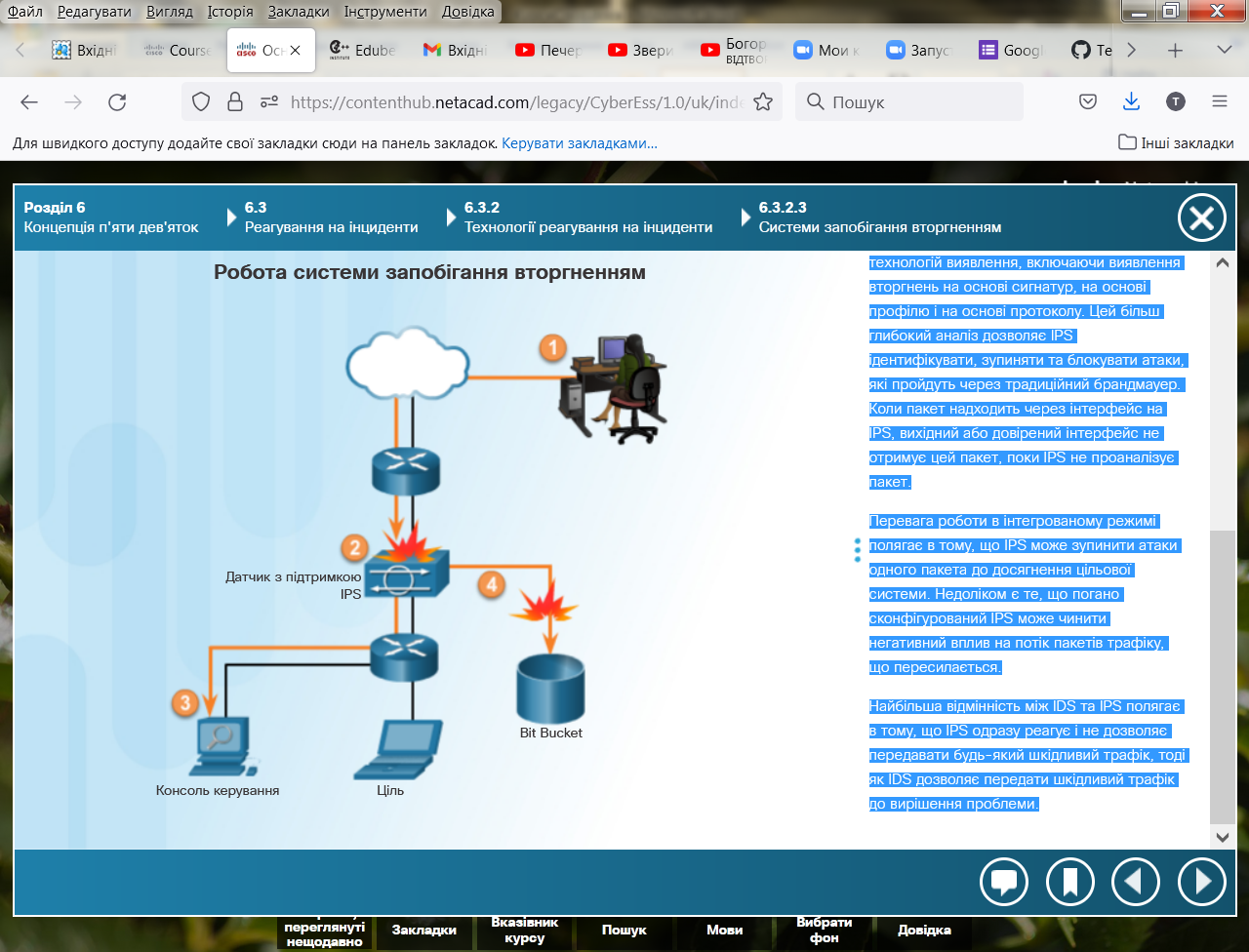
* IDS працює пасивно
* Пристрій IDS фізично розташований в мережі так, щоб трафік мав бути віддзеркалений, щоб досягти його
* Мережний трафік не проходить через IDS, якщо він не віддзеркалюється

Пасивність означає, що IDS контролює та звітує про трафік. Він не робить жодних дій. Це визначення роботи у змішаному режимі.

Перевага роботи з копією трафіку полягає в тому, що IDS не робить негативного впливу на потік пакетів трафіку, що пересилається. Недоліком роботи з копією трафіку є те, що IDS не може зупинити атаки шкідливих одиничних пакетів від досягнення цілі, перш ніж відреагує на атаку. У боротьбі з атаками IDS часто потребує допомоги від інших мережних пристроїв, таких як маршрутизатори та брандмауери.

Кращим рішенням є використання пристрою, який може негайно виявляти та припиняти атаку. Цю функцію виконує система запобігання вторгненням (Intrusion Prevention System, IPS).

# Системи запобігання вторгненням

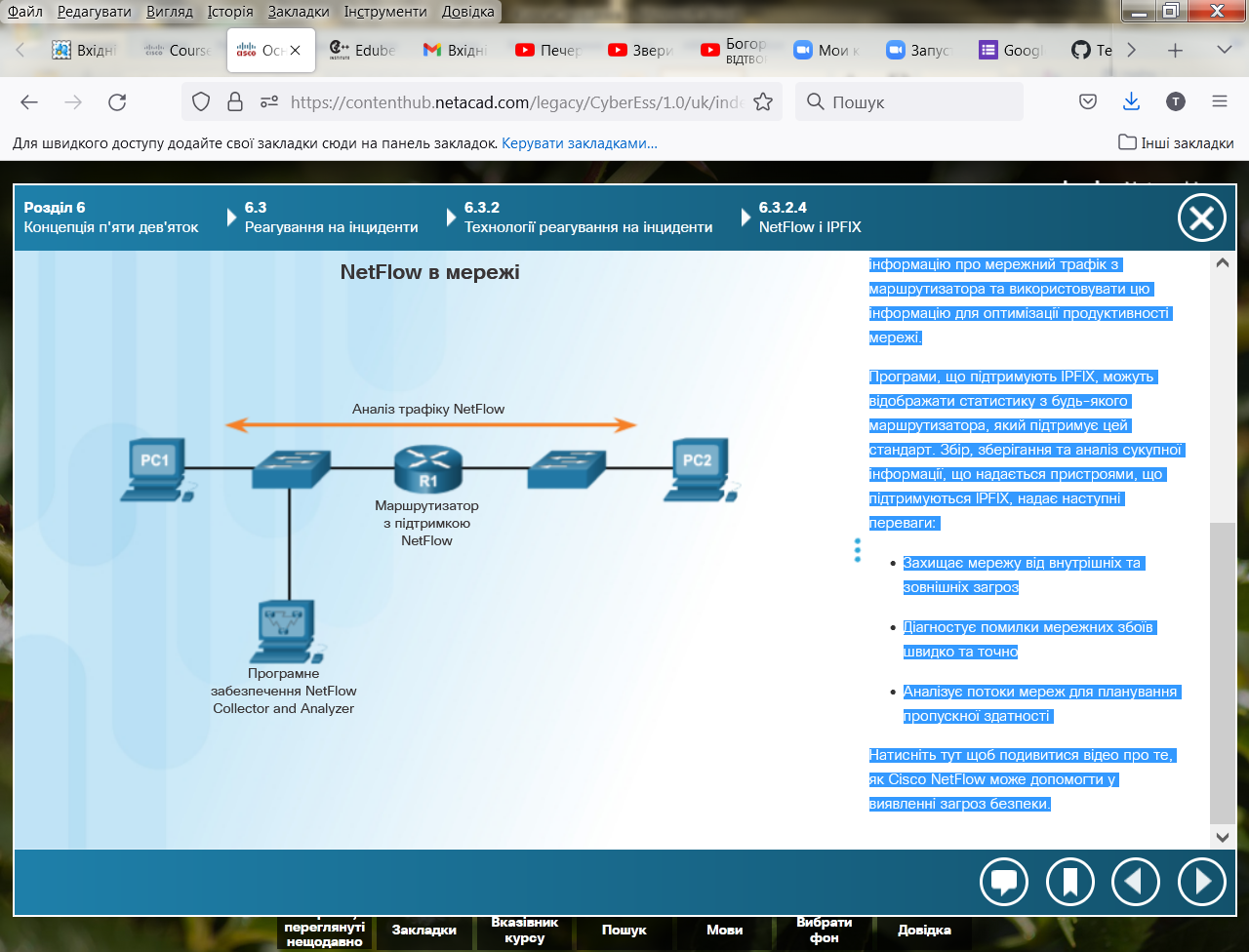
IPS будується на технології IDS. Однак пристрій IPS працює в режимі Inline. Це означає, що весь вхідний і вихідний трафік повинен проходити через нього для обробки. Як показано на рисунку, IPS не дозволяє пакетам входити до захищеної частини мережі, поки він не проаналізував пакети. Він може виявляти і негайно вирішувати мережну проблему.

IPS контролює мережний трафік. Він аналізує вміст і корисне навантаження пакетів для більш складних вбудованих атак, які можуть включати шкідливі дані. Деякі системи використовують поєднання технологій виявлення, включаючи виявлення вторгнень на основі сигнатур, на основі профілю і на основі протоколу. Цей більш глибокий аналіз дозволяє IPS ідентифікувати, зупиняти та блокувати атаки, які пройдуть через традиційний брандмауер. Коли пакет надходить через інтерфейс на IPS, вихідний або довірений інтерфейс не отримує цей пакет, поки IPS не проаналізує пакет.

Перевага роботи в інтегрованому режимі полягає в тому, що IPS може зупинити атаки одного пакета до досягнення цільової системи. Недоліком є те, що погано сконфігурований IPS може чинити негативний вплив на потік пакетів трафіку, що пересилається.

Найбільша відмінність між IDS та IPS полягає в тому, що IPS одразу реагує і не дозволяє передавати будь-який шкідливий трафік, тоді як IDS дозволяє передати шкідливий трафік до вирішення проблеми.

# NetFlow і IPFIX

NetFlow - це технологія Cisco IOS, яка забезпечує статистику пакетів, що проходять через маршрутизатор Cisco або багаторівневий комутатор. NetFlow - це стандарт для збору операційних даних з мереж. Інженерна рада Інтернету (IETF) використовувала Cisco NetFlow Version 9 як основу для IP Flow Information Export (IPFIX).

IPFIX - це стандартний формат для експорту інформації про потоки мережного трафіку на основі даних маршрутизатора. IPFIX працює з маршрутизаторами та програмами керування, що підтримують протокол. Менеджери мереж можуть експортувати інформацію про мережний трафік з маршрутизатора та використовувати цю інформацію для оптимізації продуктивності мережі.

Програми, що підтримують IPFIX, можуть відображати статистику з будь-якого маршрутизатора, який підтримує цей стандарт. Збір, зберігання та аналіз сукупної інформації, що надається пристроями, що підтримуються IPFIX, надає наступні переваги:

* Захищає мережу від внутрішніх та зовнішніх загроз
* Діагностує помилки мережних збоїв швидко та точно
* Аналізує потоки мереж для планування пропускної здатності

Натисніть [тут](http://video.cisco.com/detail/videos/products/video/2534277650001/cybersecurity-enabled-by-flexible-netflow-in-campus-access) щоб подивитися відео про те, як Cisco NetFlow може допомогти у виявленні загроз безпеки.

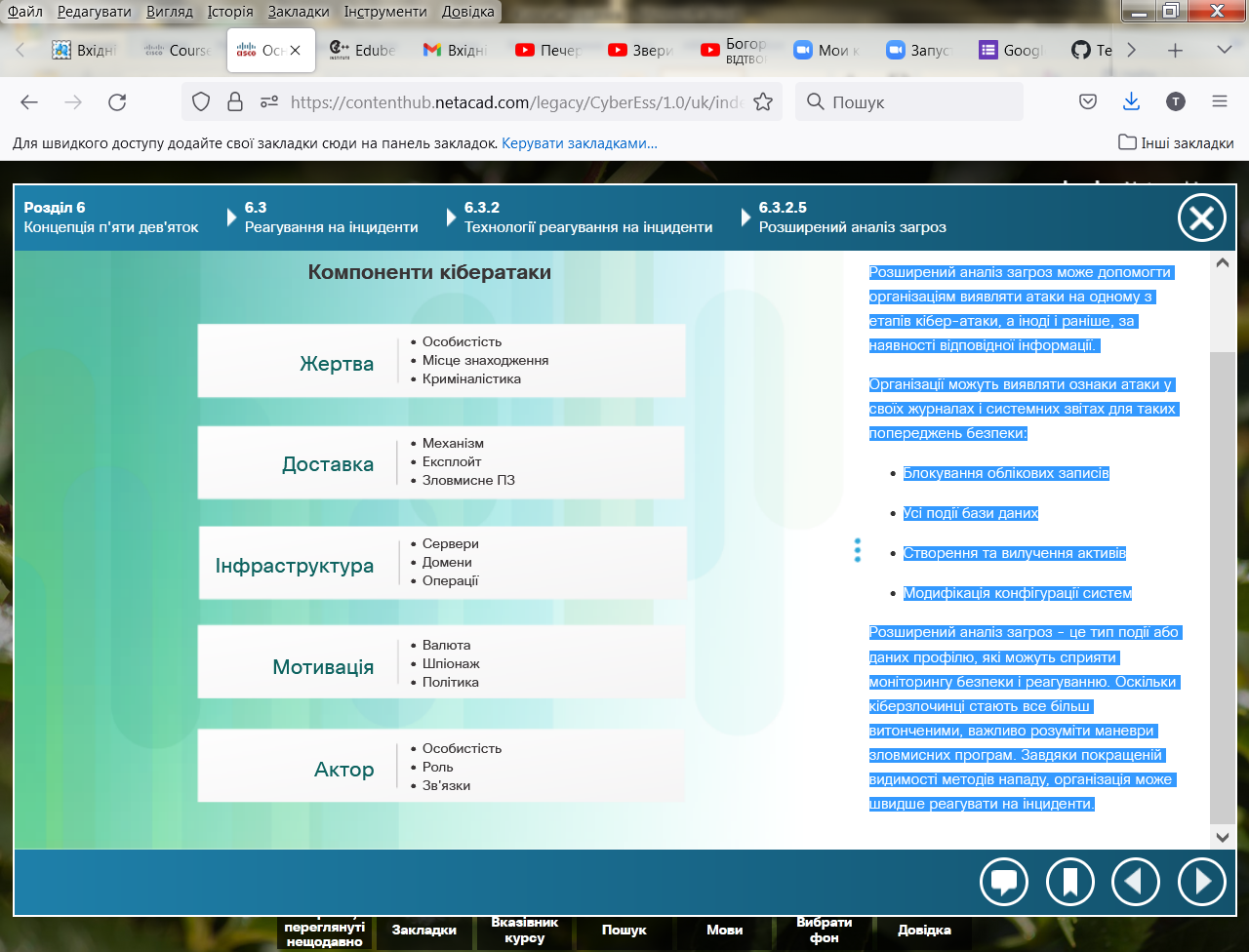
# Розширений аналіз загроз

Розширений аналіз загроз може допомогти організаціям виявляти атаки на одному з етапів кібер-атаки, а іноді і раніше, за наявності відповідної інформації.

Організації можуть виявляти ознаки атаки у своїх журналах і системних звітах для таких попереджень безпеки:

* Блокування облікових записів
* Усі події бази даних
* Створення та вилучення активів
* Модифікація конфігурації систем

Розширений аналіз загроз - це тип події або даних профілю, які можуть сприяти моніторингу безпеки і реагуванню. Оскільки кіберзлочинці стають все більш витонченими, важливо розуміти маневри зловмисних програм. Завдяки покращеній видимості методів нападу, організація може швидше реагувати на інциденти.



# Типи катастроф

Вкрай важливо підтримувати функціонування організації, коли відбувається лихо. Катастрофа включає в себе будь-яку природну або антропогенну подію, яка шкодить майну, і погіршує здатність організації продовжувати свою діяльність.

**Стихійні лиха**

Стихійні лиха відрізняються залежно від місця розташування. Деякі з цих подій важко передбачити. Стихійні лиха поділяються на такі категорії:

* Геологічні катастрофи включають землетруси, зсуви, вулкани та цунамі
* Метеорологічні катастрофи включають урагани, торнадо, сніжні бурі, молнії та град
* До лих зі здоров'ям відносяться широко поширені хвороби, карантини і пандемії
* До числа інших лих відносяться пожежі, повені, сонячні бурі і лавини

**Антропогенні катастрофи**

Антропогенні катастрофи пов'язані з людьми або організаціями і поділяються на такі категорії:

* Сфера трудових відносин включає страйки, прогули і уповільнення діяльності
* Соціально-політичні події включають вандалізм, блокади, протести, саботаж, тероризм та війну
* До матеріальних подій включають розливи небезпечних речовин та пожежі
* Комунальні збої включають збої живлення і зв'язку, брак палива і радіоактивні опади

Натисніть [тут](http://www.nytimes.com/interactive/2011/03/13/world/asia/satellite-photos-japan-before-and-after-tsunami.html) щоб переглянути супутникові фотографії Японії до та після землетрусу та цунамі 2011 року.

**План відновлення після стихійних лих**

Організація втілює план аварійного відновлення (Disaster Recovery Plan, DRP) під час катастрофи і співробітники намагаються забезпечити роботу критично важливих систем. DRP включає в себе заходи організації, що проводяться для оцінки, усунення та відновлення пошкоджених об'єктів або активів.

Щоб створити DRP, відповідайте на наступні питання:

* Хто відповідає за цей процес?
* Що робити людині для виконання цього процесу?
* Де особа виконує цей процес?
* Який процес?
* Чому процес критичний?

DRP повинен визначити, які процеси в організації є найбільш критичними. У процесі відновлення організація відновлює свої критично важливі системи в першу чергу.

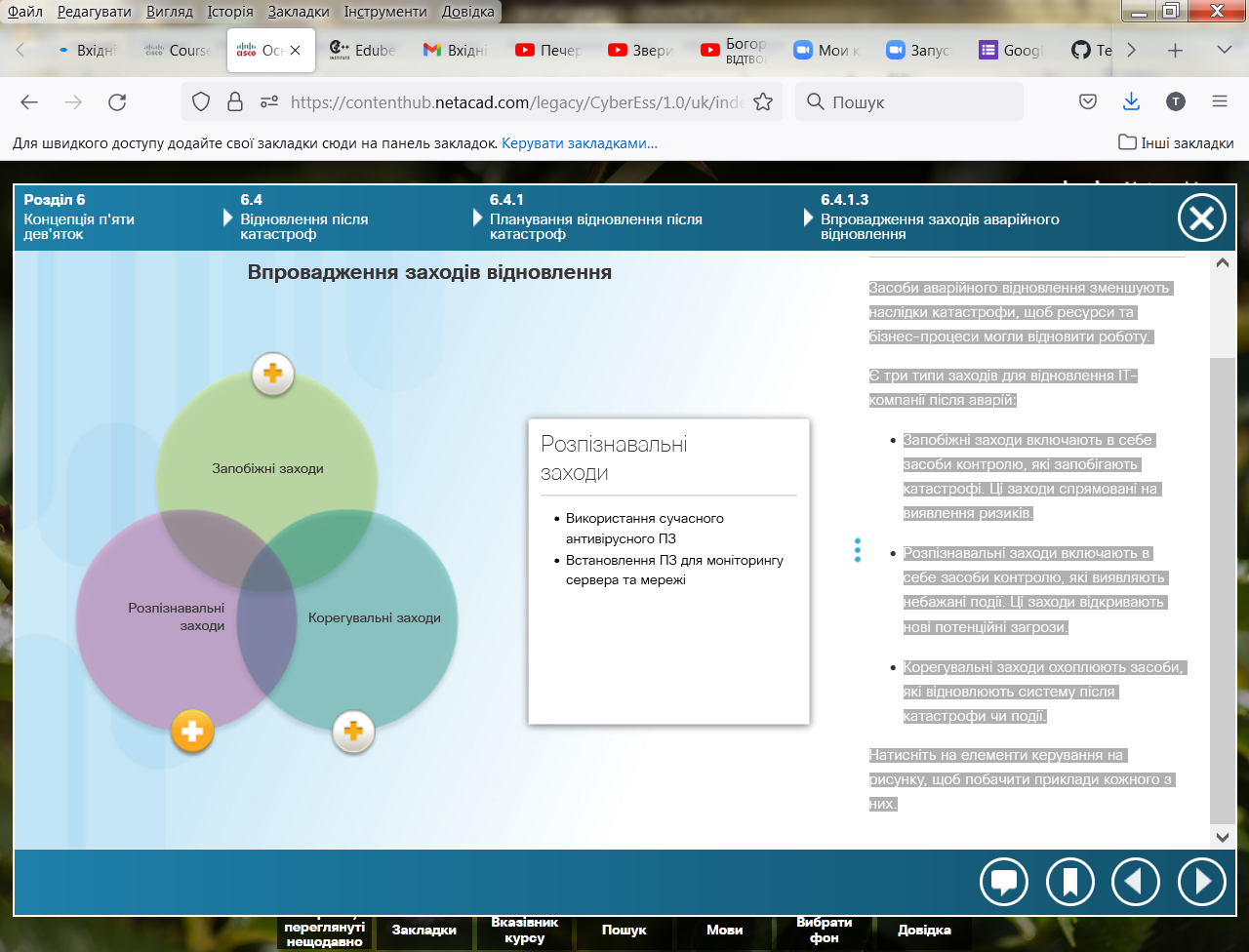
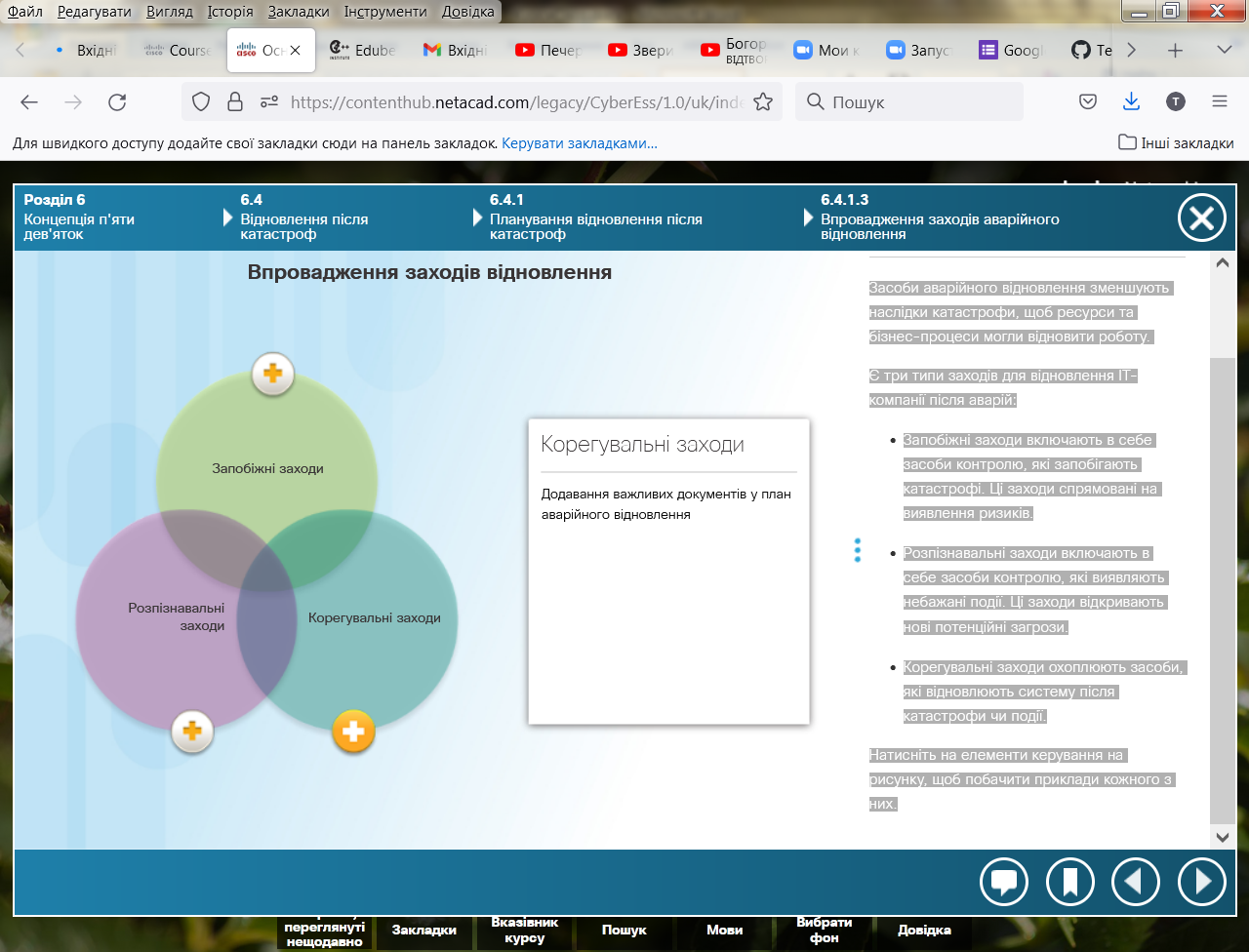
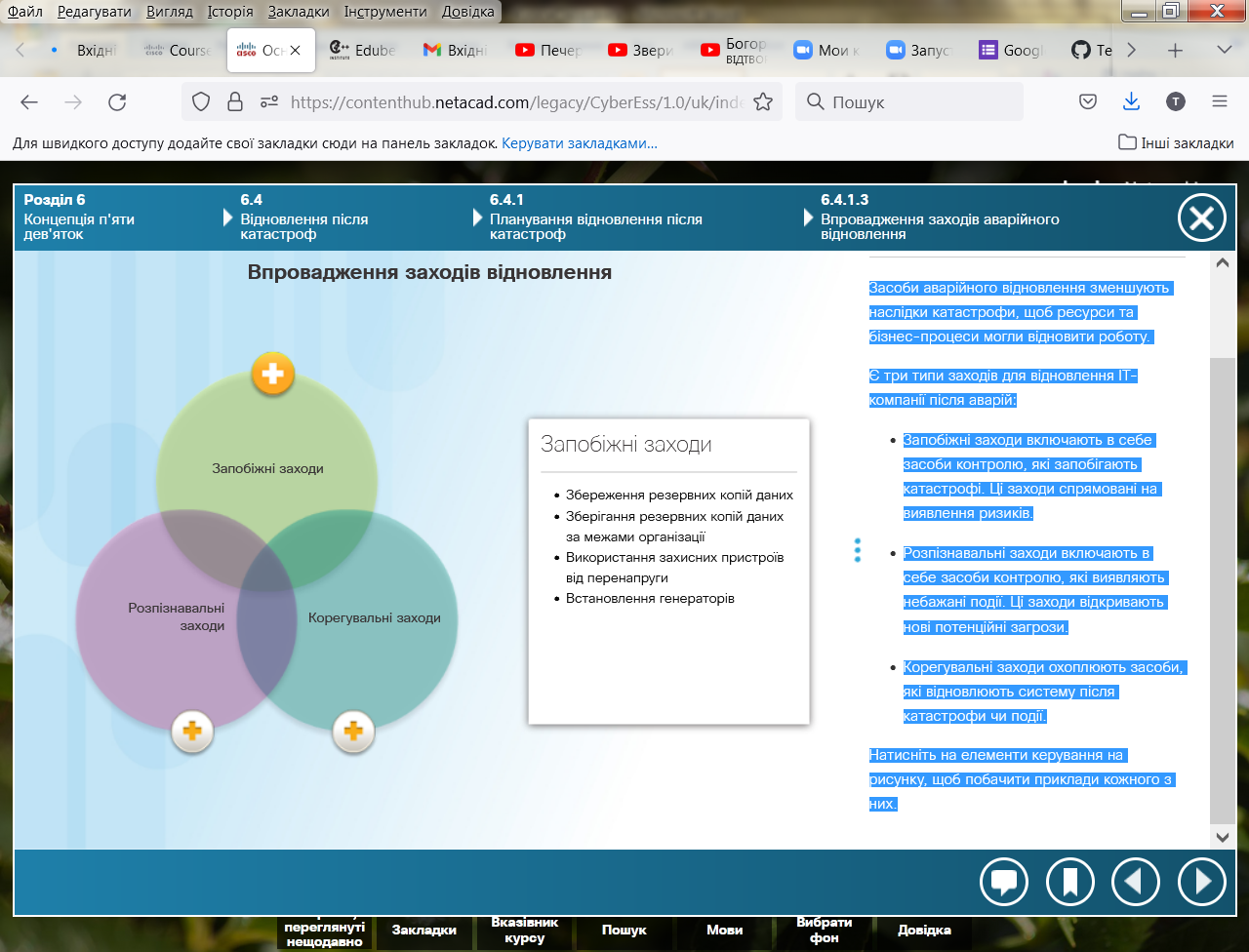
**Впровадження заходів аварійного відновлення**

Засоби аварійного відновлення зменшують наслідки катастрофи, щоб ресурси та бізнес-процеси могли відновити роботу.

Є три типи заходів для відновлення IT-компанії після аварій:

* Запобіжні заходи включають в себе засоби контролю, які запобігають катастрофі. Ці заходи спрямовані на виявлення ризиків.
* Розпізнавальні заходи включають в себе засоби контролю, які виявляють небажані події. Ці заходи відкривають нові потенційні загрози.
* Корегувальні заходи охоплюють засоби, які відновлюють систему після катастрофи чи події.

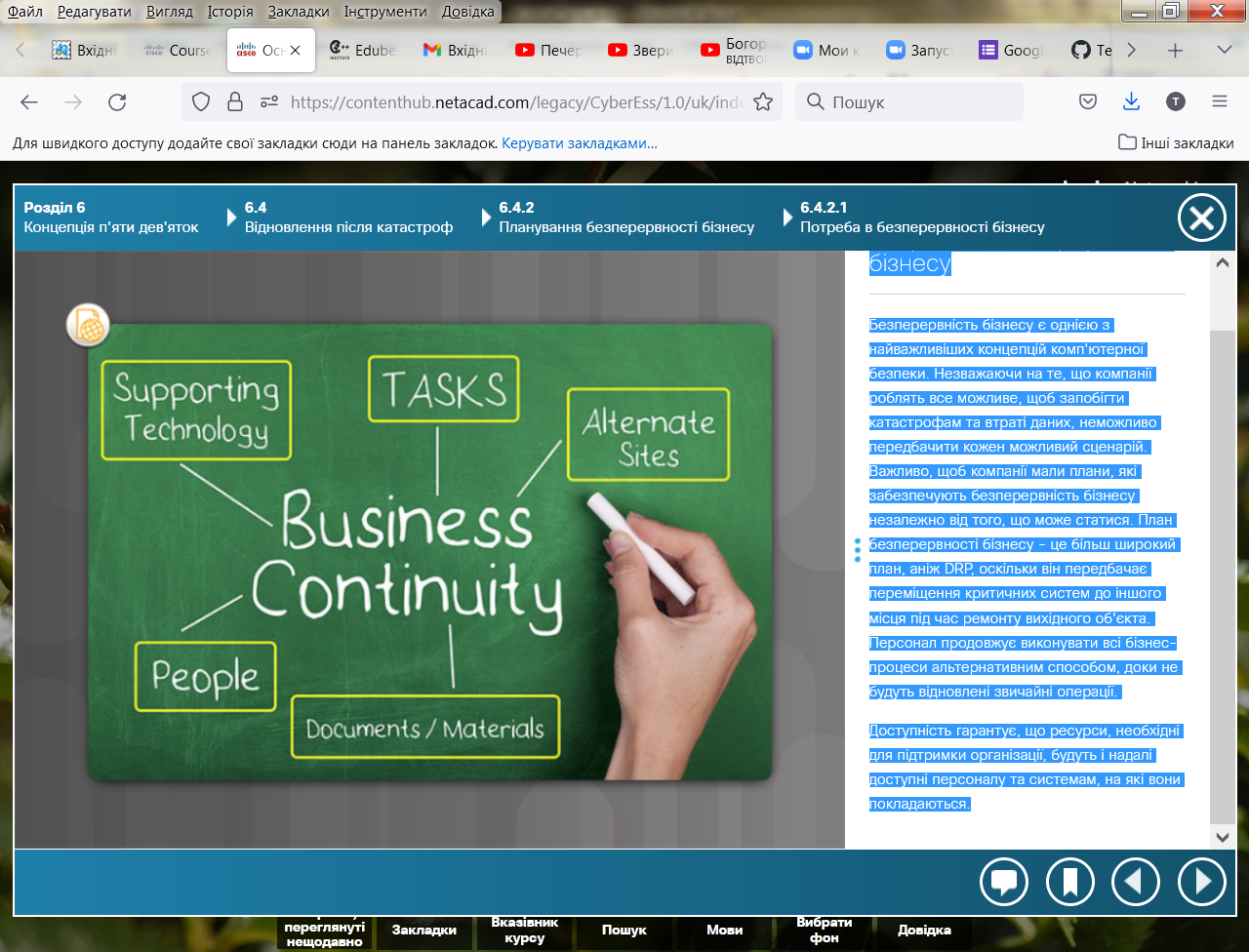
Натисніть на елементи керування на рисунку, щоб побачити приклади кожного з них.



**Потреба в безперервності бізнесу**

Безперервність бізнесу є однією з найважливіших концепцій комп'ютерної безпеки. Незважаючи на те, що компанії роблять все можливе, щоб запобігти катастрофам та втраті даних, неможливо передбачити кожен можливий сценарій. Важливо, щоб компанії мали плани, які забезпечують безперервність бізнесу незалежно від того, що може статися. План безперервності бізнесу - це більш широкий план, аніж DRP, оскільки він передбачає переміщення критичних систем до іншого місця під час ремонту вихідного об'єкта. Персонал продовжує виконувати всі бізнес-процеси альтернативним способом, доки не будуть відновлені звичайні операції.

Доступність гарантує, що ресурси, необхідні для підтримки організації, будуть і надалі доступні персоналу та системам, на які вони покладаються.

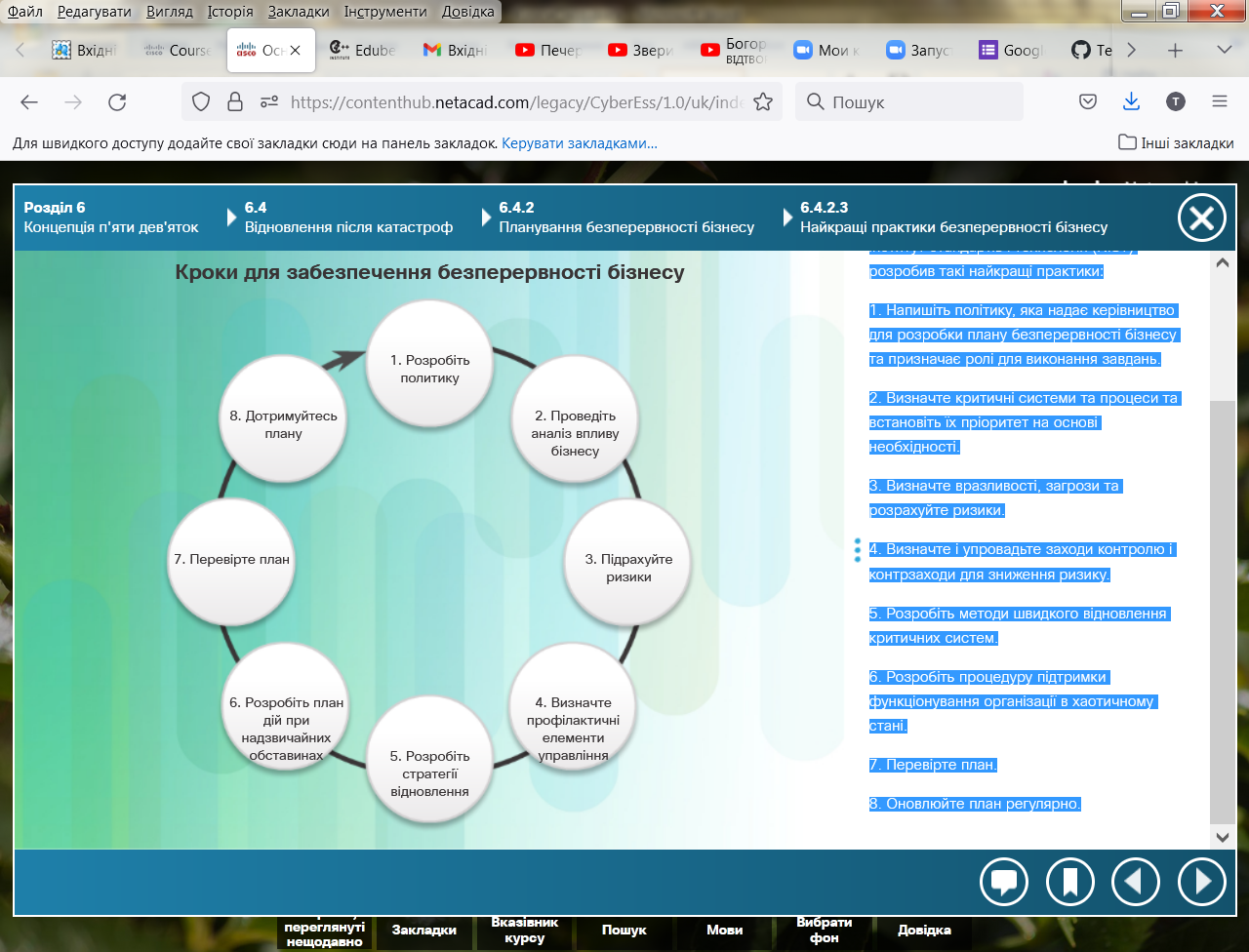


**Міркування про безперервність бізнесу**

Контроль безперервності бізнесу - це не просто резервне копіювання даних та надання резервного обладнання. Організаціям потрібні працівники для належного налаштування та управління системами. Дані можуть бути марними до тих пір, поки вони не нададуть інформацію. Організація повинна розглянути наступне:

* Перебування потрібних людей у потрібних місцях
* Документування конфігурацій
* Створення альтернативних каналів зв'язку для передачі голосу та даних
* Забезпечення живлення
* Визначення всіх залежностей для програм та процесів, щоб їх можна було правильно зрозуміти
* Розуміння того, як виконувати вручну автоматичні завдання

**Найкращі практики безперервності бізнесу**

Як показано на рисунку, Національний інститут стандартів і технологій (NIST) розробив такі найкращі практики:

* 1. Напишіть політику, яка надає керівництво для розробки плану безперервності бізнесу та призначає ролі для виконання завдань.
* 2. Визначте критичні системи та процеси та встановіть їх пріоритет на основі необхідності.
* 3. Визначте вразливості, загрози та розрахуйте ризики.
* 4. Визначте і упровадьте заходи контролю і контрзаходи для зниження ризику.
* 5. Розробіть методи швидкого відновлення критичних систем.
* 6. Розробіть процедуру підтримки функціонування організації в хаотичному стані.
* 7. Перевірте план.
* 8. Оновлюйте план регулярно.

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

Цей розділ почався з пояснення концепції п'яти дев'яток, стандарту високої доступності, що дозволяє скоротити час простою до 5,26 хвилин на рік. У розділі обговорювалися різні підходи, які використовують організації для забезпечення доступності систем. Належна конструкція системи включає в себе заходи, що забезпечують надлишковість і відмовостійкість для швидкого відновлення та продовження роботи організації.

У розділі також було обговорено, як організація реагує на інцидент, встановивши процедури, яких слід дотримуватися після виникнення події. Розділ завершився обговоренням аварійного відновлення та планування безперервності бізнесу.