**Комутатори, маршрутизатори і мережні пристрої**

Мережні пристрої не мають паролів або мають пароль за замовчуванням. Змініть паролі за замовчуванням перед підключенням будь-якого пристрою до мережі. Документуйте і запишіть в журнал зміни в мережних пристроях. Нарешті, дослідіть всі журнали конфігурації.

У наступних розділах описані деякі заходи, які адміністратор може вжити для захисту різних мережних пристроїв.

**Комутатори**

Мережні комутатори є основою сучасної мережі передачі даних. Основною загрозою для мережних комутаторів є крадіжка, хакерство та віддалений доступ, атаки проти мережних протоколів, таких як ARP/STP, або атаки на продуктивність апарату та на його доступність. Засоби контролю і заходи захисту від загроз для мережних комутаторів включають поліпшену фізичну безпеку, розширену конфігурацію та введення відповідних системних оновлень та виправлень за потребою. Інший ефективний спосіб контролю - це реалізація безпеки портів. Адміністратор повинен захистити всі порти (інтерфейси) комутатора перед його використанням в робочих умовах. Один із способів захисту портів - це реалізація функції безпеки портів (функція Port Security). Безпека портів обмежує кількість дійсних MAC-адрес, дозволених на даний порт. Комутатор дозволяє отримувати доступ до пристроїв зі схваленими MAC-адресами, тоді як відхиляє всім іншим MAC-адресам.

**Мережі VLAN**

VLAN забезпечують спосіб групування пристроїв у локальній мережі та на окремих комутаторах. VLAN використовують логічні з'єднання замість фізичних. Окремі порти комутатора можуть бути призначені для конкретної VLAN. Інші порти можуть бути використані для фізичного взаємоз'єднання комутаторів один з одним і дозволяють пересилати трафік декількох VLAN. Ці порти називаються магістральними (trunks).

Наприклад, у відділі кадрів (HR) необхідно захистити конфіденційні дані. VLAN дозволяють адміністратору сегментувати мережі по функціям, проектним групам або застосуванням незалежно від фізичного розташування користувача або пристрою, як показано на рисунку 1. Пристрої всередині VLAN діють так, як ніби вони знаходяться у власній незалежній мережі, навіть якщо вони мають спільну інфраструктуру з іншими VLAN. VLAN може відокремити групи, які мають конфіденційні дані, від решти мереж, зменшуючи ймовірність витоку цих даних. Магістральні канали забезпечують можливість фізичного підключення користувачів мережі VLAN HR до кількох комутаторів.

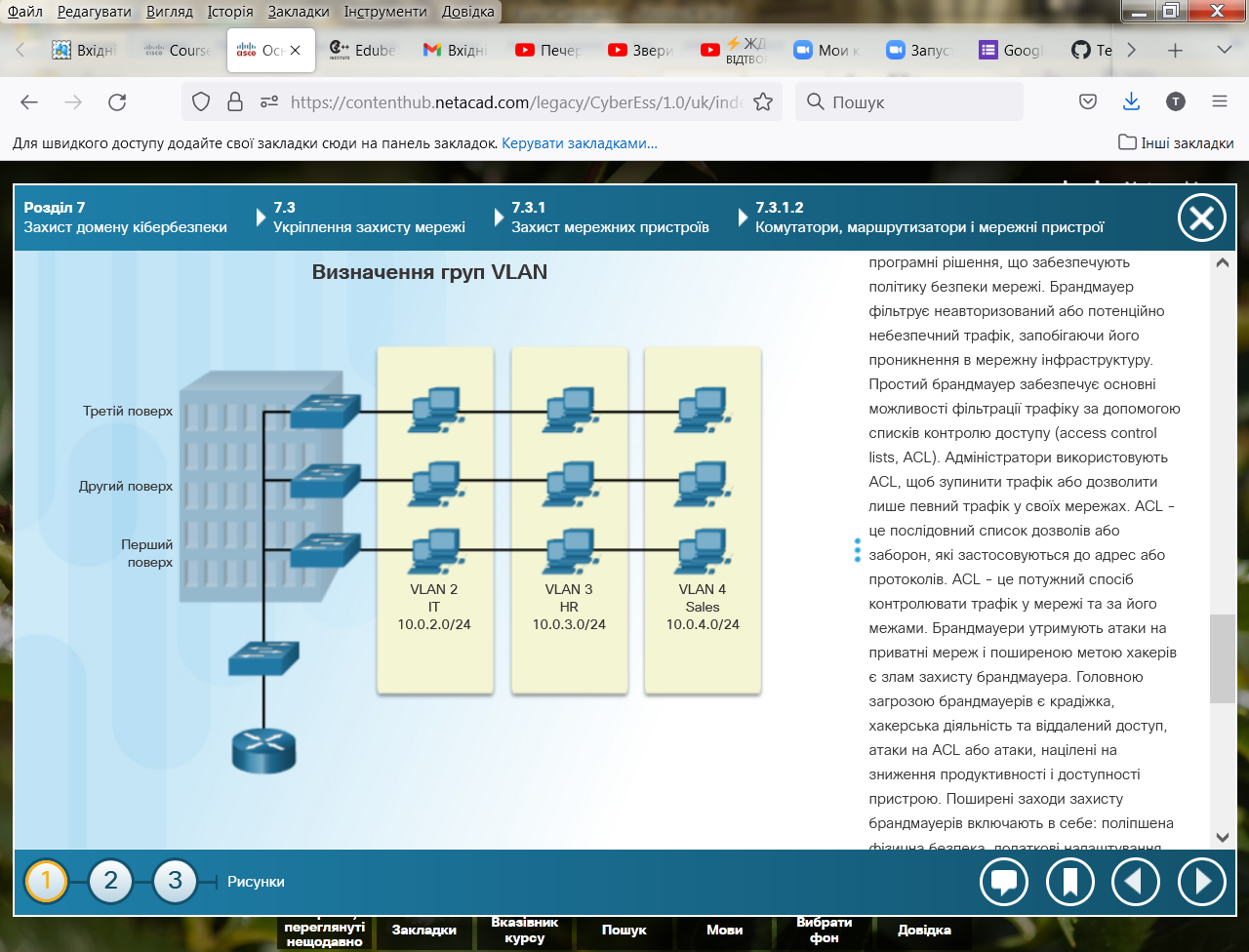
Існує багато різних типів вразливостей і атак на VLAN. Вони можуть включати в себе атаки на VLAN та "Trucking" протоколи. Деталі ціх атаки виходять за рамки цього курсу. Хакери також можуть організовувати атаки на продуктивність і доступність мереж VLAN. Поширені заходи захисту від загроз включають в себе моніторинг змін і показників VLAN, додаткові налаштування і регулярне оновлення IOS.

**Брандмауери**

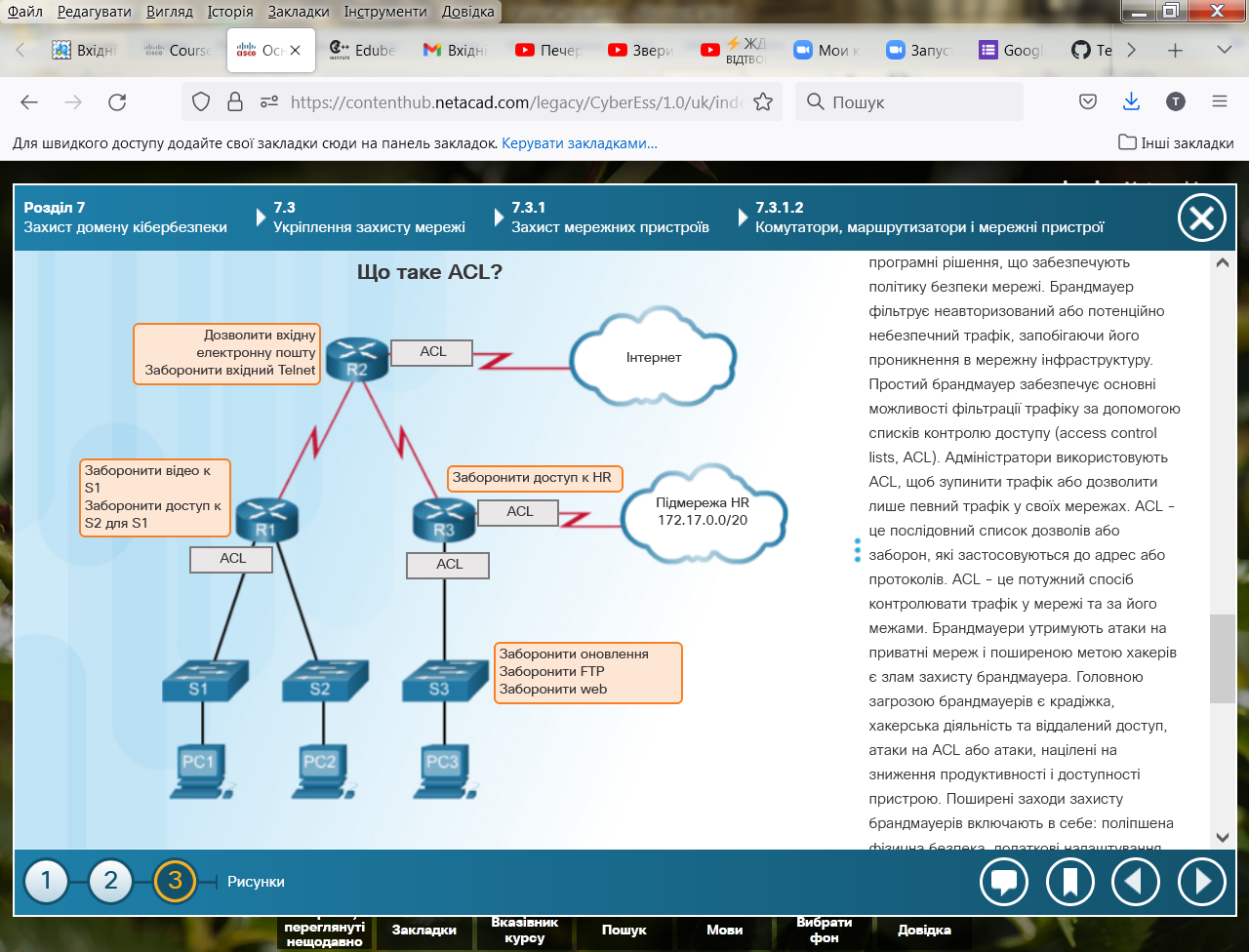
Брандмауери (Firewalls) - це апаратні або програмні рішення, що забезпечують політику безпеки мережі. Брандмауер фільтрує неавторизований або потенційно небезпечний трафік, запобігаючи його проникнення в мережну інфраструктуру. Простий брандмауер забезпечує основні можливості фільтрації трафіку за допомогою списків контролю доступу (access control lists, ACL). Адміністратори використовують ACL, щоб зупинити трафік або дозволити лише певний трафік у своїх мережах. ACL - це послідовний список дозволів або заборон, які застосовуються до адрес або протоколів. ACL - це потужний спосіб контролювати трафік у мережі та за його межами. Брандмауери утримують атаки на приватні мереж і поширеною метою хакерів є злам захисту брандмауера. Головною загрозою брандмауерів є крадіжка, хакерська діяльність та віддалений доступ, атаки на ACL або атаки, націлені на зниження продуктивності і доступності пристрою. Поширені заходи захисту брандмауерів включають в себе: поліпшена фізична безпека, додаткові налаштування, безпечний віддалений доступ та аутентифікація, а також відповідні системні оновлення та виправлення за потребою.

**Маршрутизатори**

Маршрутизатори утворюють основу Інтернету та зв'язок між різними мережами. Маршрутизатори взаємодіють один з одним, щоб визначити найкращий шлях доставки трафіку до різних мереж. Маршрутизатори використовують протоколи маршрутизації для прийняття рішення маршрутизації. В маршрутизатори також можуть бути інтегровані інші сервіси, такі як функції комутаторів і брандмауерів. В результаті маршрутизатори стають першочерговою метою зловмисників. Основною загрозою для мережних маршрутизаторів є крадіжка, хакерська діяльність та віддалений доступ, атаки на протоколи маршрутизації, такі як RIP/OSPF, або атаки націлені на зниження продуктивності і доступності пристрою. Поширені заходи захисту мережних маршрутизаторів включають в себе: поліпшена фізична безпека, додаткові налаштування, використання протоколів безпечної маршрутизації з аутентифікацією та відповідні оновлення системи та виправлення за потребою.



1



3

2

**Бездротові та мобільні пристрої**

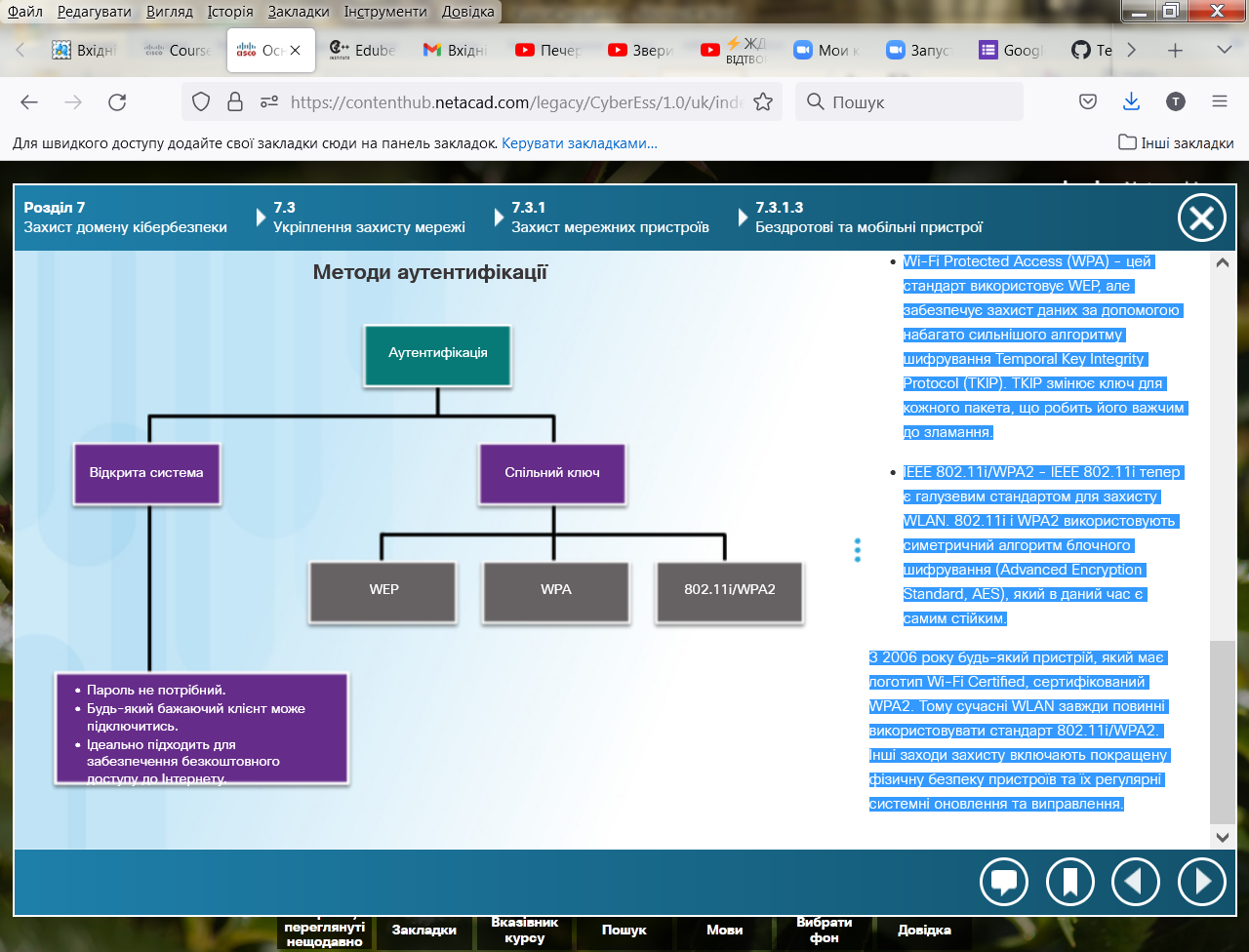
Бездротові і мобільні пристрої стали переважаючим типом пристроїв в більшості сучасних мереж. Вони забезпечують мобільність та зручність, але створюють безліч вразливостей. До таких вразливостей відносяться крадіжки, хакерська діяльність та несанкціонований віддалений доступ, сніффінг (аналіз трафіку), атаки man-in-the-middle (“Людина посередині”) та атаки націлені на зниження продуктивності і доступності пристрою. Найкращий спосіб захистити бездротову мережу - використання аутентифікації та шифрування. Початковий бездротовий стандарт 801.11 ввів два типи аутентифікації, як показано на рисунку:

* Аутентифікація відкритої системи - будь-який бездротовий пристрій може підключитися до бездротової мережі. Використовуйте цей метод у ситуаціях, коли безпека не викликає занепокоєння.
* Авторизація спільного ключа - надає механізми аутентифікації та шифрування даних, переданих між бездротовим клієнтом і точкою доступу (АР) або бездротовим маршрутизатором.

У мережах WLAN доступні три варіанти аутентифікації за допомогою спільного ключа:

* Wired Equivalent Privacy (WEP) - це початкова специфікація 802.11 забезпечення безпеки WLAN. Однак, ключ шифрування ніколи не змінюється при обміні пакетами, тому його легко зламати.
* Wi-Fi Protected Access (WPA) - цей стандарт використовує WEP, але забезпечує захист даних за допомогою набагато сильнішого алгоритму шифрування Temporal Key Integrity Protocol (TKIP). TKIP змінює ключ для кожного пакета, що робить його важчим до зламання.
* IEEE 802.11i/WPA2 - IEEE 802.11i тепер є галузевим стандартом для захисту WLAN. 802.11i і WPA2 використовують симетричний алгоритм блочного шифрування (Advanced Encryption Standard, AES), який в даний час є самим стійким.

З 2006 року будь-який пристрій, який має логотип Wi-Fi Certified, сертифікований WPA2. Тому сучасні WLAN завжди повинні використовувати стандарт 802.11i/WPA2. Інші заходи захисту включають покращену фізичну безпеку пристроїв та їх регулярні системні оновлення та виправлення.



**Мережні служби та служби маршрутизації**

Кібер злочинці використовують уразливі мережні служби для атаки на пристрій або використовують їх як частину атаки. Щоб перевірити наявність незахищених мережних служб, використовуйте сканер портів для пошуку відкритих портів на пристрої. Порт-сканер - це програма, перевіряє на пристрої відкриті порти, відправивши повідомлення на кожний порт і чекаючи відповіді. Відповідь вказує, як використовується порт. З цією ж метою кіберзлочинці також використовують сканери портів. Для безпеки мережних сервісів тільки необхідні порти повинні бути доступні для використання і виявлення.

**Протокол динамічної конфігурації хоста (DHCP)**

DHCP використовує сервер, щоб автоматично призначати IP-адресу та інші параметри конфігурації мережним пристроям. По суті, пристрій отримує від сервера DHCP дозвіл на використання мережної інфраструктури. Зловмисники можуть атакувати DHCP-сервери, щоб заборонити доступ до пристроїв у мережі. На рисунку 1 наведено контрольний перелік безпеки для DHCP.

**Доменна система імен (DNS)**

DNS (Domain Name System) перетворює URL-адресу універсального ресурсу або адресу веб-сайту (наприклад, http://www.cisco.com) в IP-адрес сайту. Коли користувачі вводять веб-адресу в адресний рядок, DNS-сервери перетворюють його в фактичну IP-адресу призначення. Зловмисники можуть атакувати DNS-сервери, щоб заборонити доступ до мережних ресурсів або перенаправляти трафік на шахрайські веб-сайти. Клацніть на рисунок 2, щоб переглянути контрольний список безпеки для DNS. Для захисту від атак використовуйте безпечні служби та аутентифікацію між DNS-серверами.

**Міжмережний протокол керуючих повідомлень (ICMP)**

Мережні пристрої використовують ICMP (Internet Control Messaging Protocol ) для надсилання повідомлень про помилки, наприклад, якщо запитувана служба недоступна або хосту не вдалося зв'язатися з маршрутизатором. Команда ping - це мережна утиліта, яка використовує ICMP для перевірки доступності хоста в мережі. Ping надсилає ICMP-повідомлення на хост і чекає відповіді. Кіберзлочинці можуть втручатися в роботу ICMP для зловмісних цілей, перерахованих на рисунку 3. DoS-атака використовує ICMP, тому багато мереж фільтрує певні запити ICMP для запобігання подібних атак.

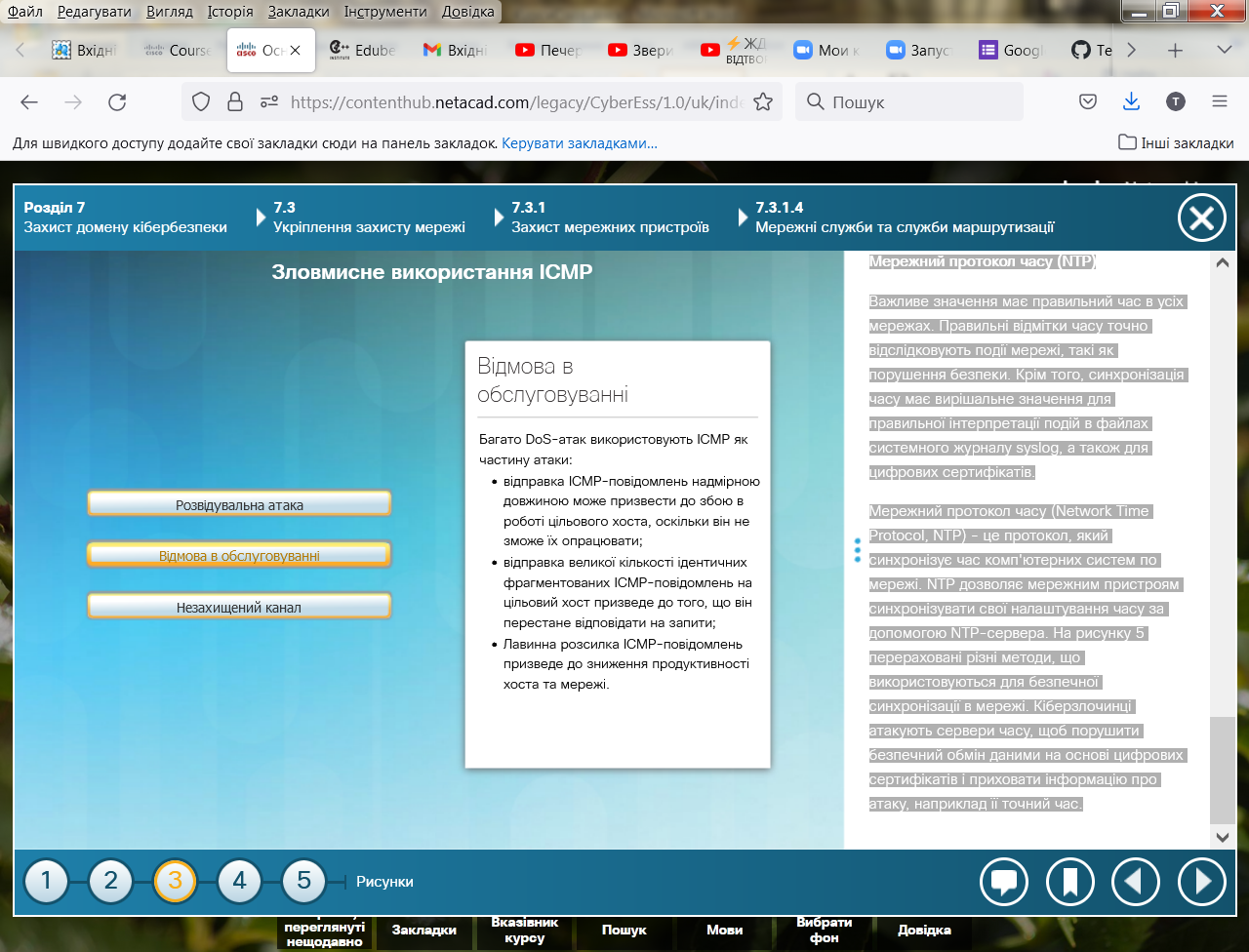
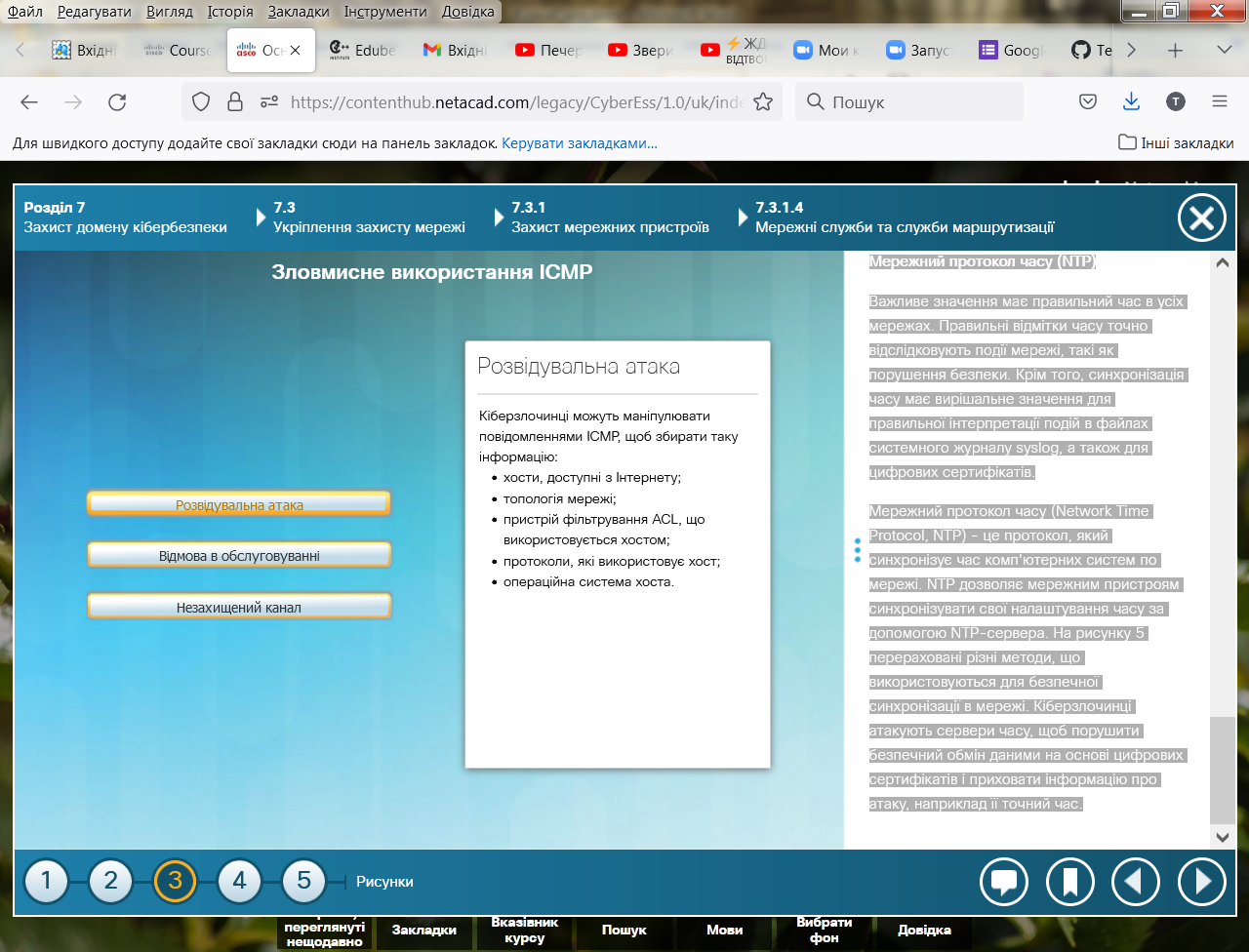
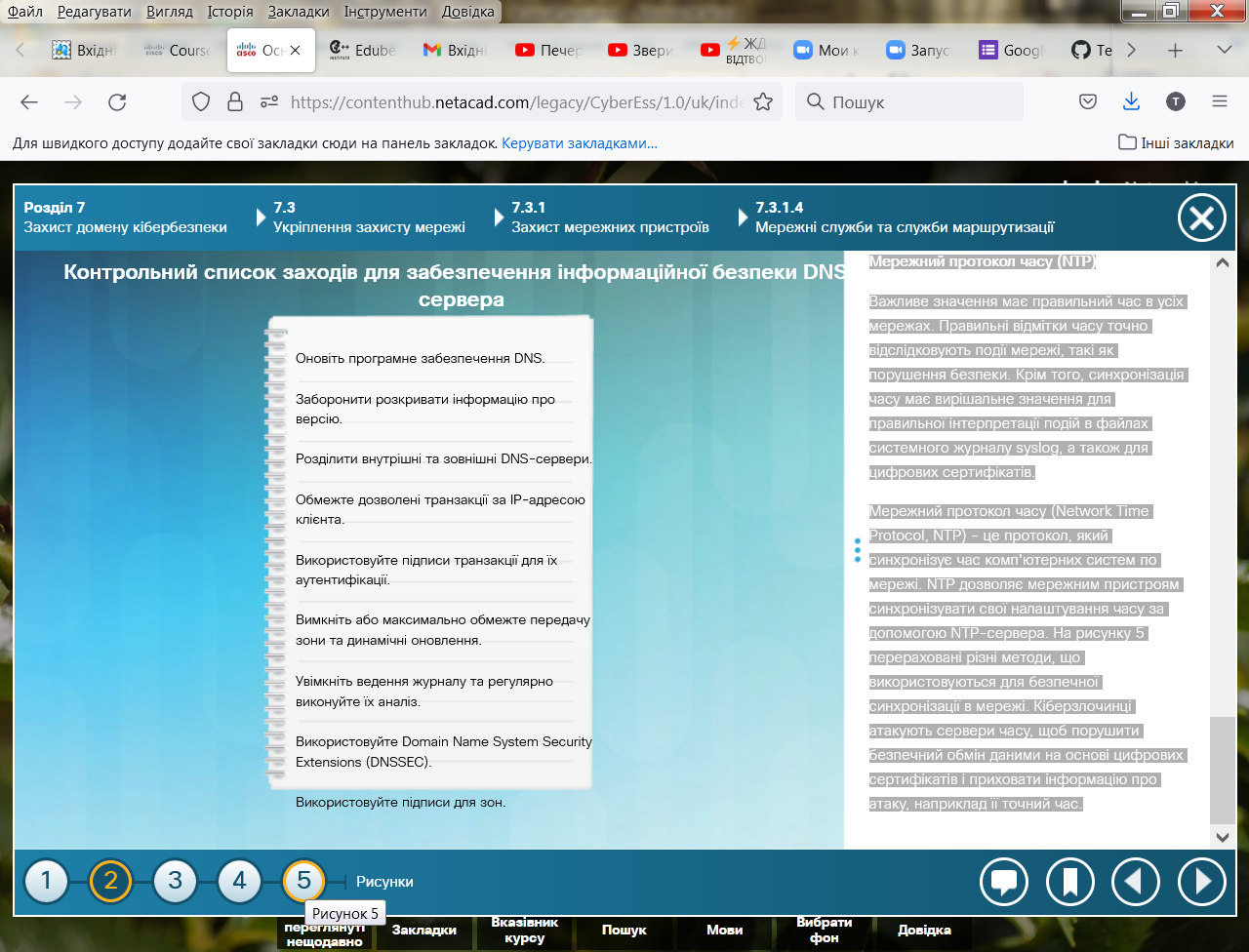
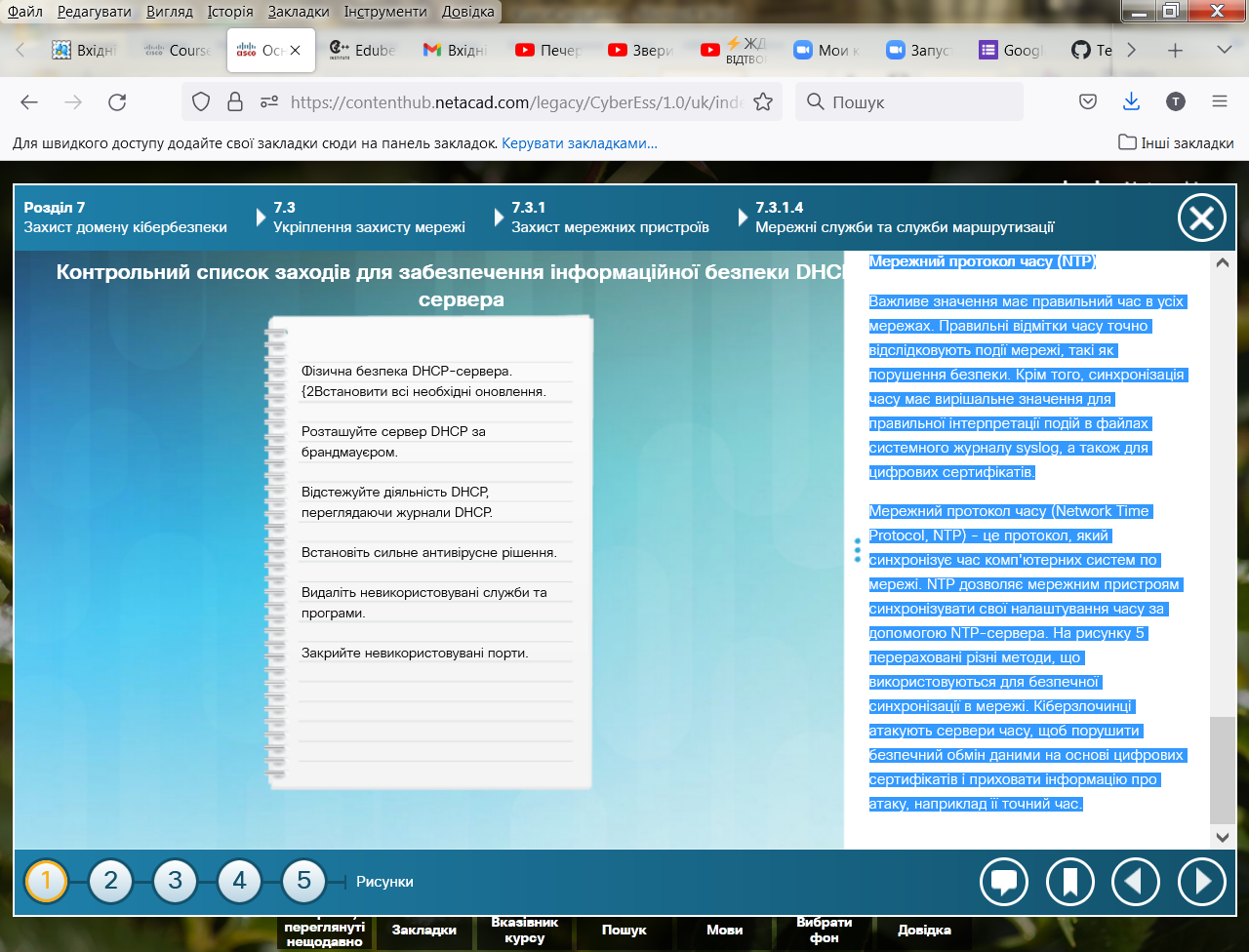
**Протокол маршрутизації RIP**

RIP (Routing Information Protocol ) обмежує кількість транзитних ділянок по мережі від вихідного пристрою до місця призначення. RIP допускає не більше 15 транзитних ділянок. RIP - це протокол маршрутизації, який використовується для обміну даними маршрутизації, в тому числі, які мережі може досягти кожен маршрутизатор і як далеко розташовані ці мережі. RIP обчислює найкращий маршрут на основі кількості переходів. На рисунку 4 наведено вразливості RIP та засоби захисту від атак на нього. Хакери можуть атакувати маршрутизатори та протокол RIP. Атаки на служби маршрутизації можу вплинути на продуктивність і доступність. Деякі атаки можуть навіть призвести до перенаправлення трафіку. Для захисту служб маршрутизації, таких як RIP, використовуйте безпечні служби з аутентифікацією та здійснюйте системні оновлення та виправлення.

**Мережний протокол часу (NTP)**

Важливе значення має правильний час в усіх мережах. Правильні відмітки часу точно відслідковують події мережі, такі як порушення безпеки. Крім того, синхронізація часу має вирішальне значення для правильної інтерпретації подій в файлах системного журналу syslog, а також для цифрових сертифікатів.

Мережний протокол часу (Network Time Protocol, NTP) - це протокол, який синхронізує час комп'ютерних систем по мережі. NTP дозволяє мережним пристроям синхронізувати свої налаштування часу за допомогою NTP-сервера. На рисунку 5 перераховані різні методи, що використовуються для безпечної синхронізації в мережі. Кіберзлочинці атакують сервери часу, щоб порушити безпечний обмін даними на основі цифрових сертифікатів і приховати інформацію про атаку, наприклад її точний час.

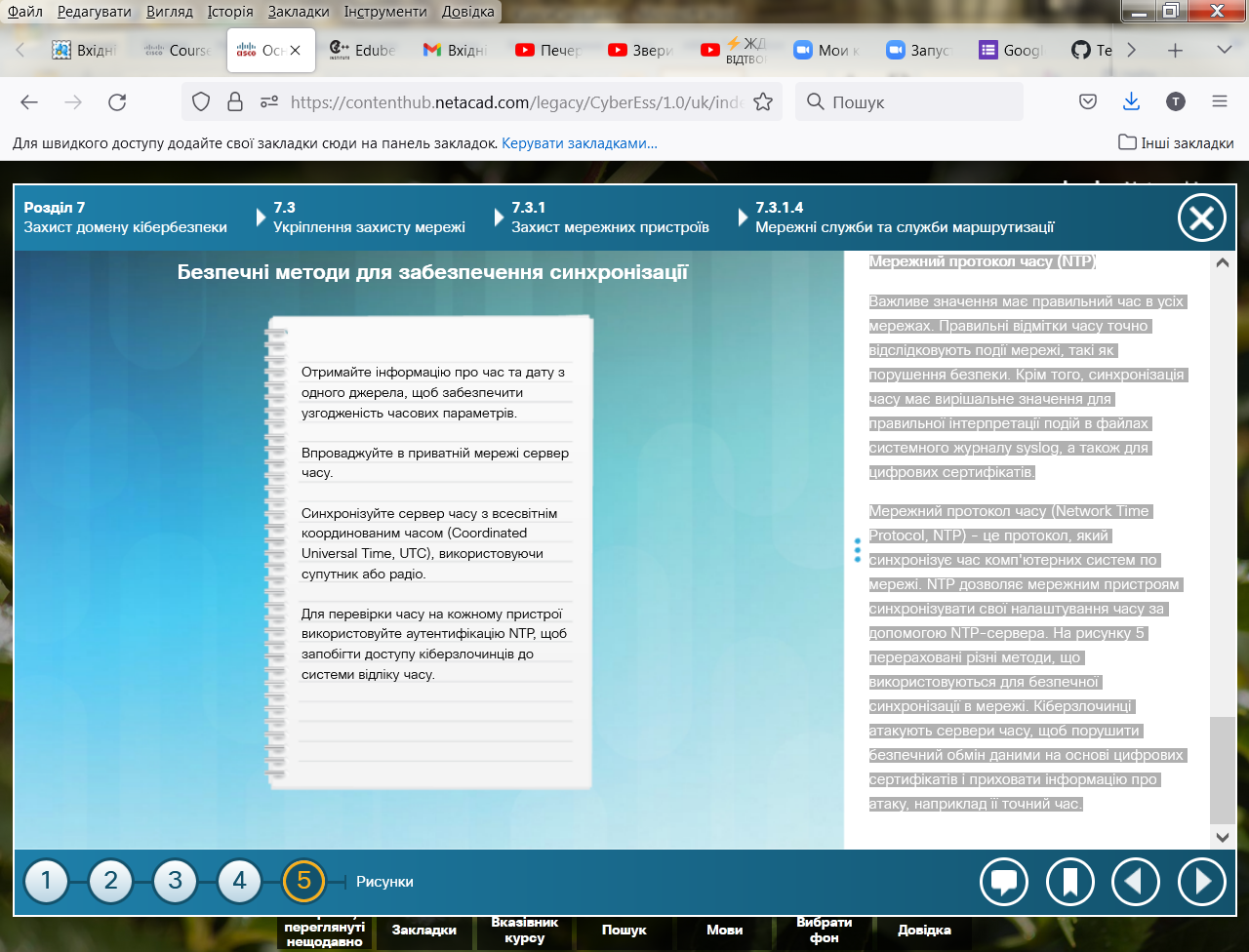
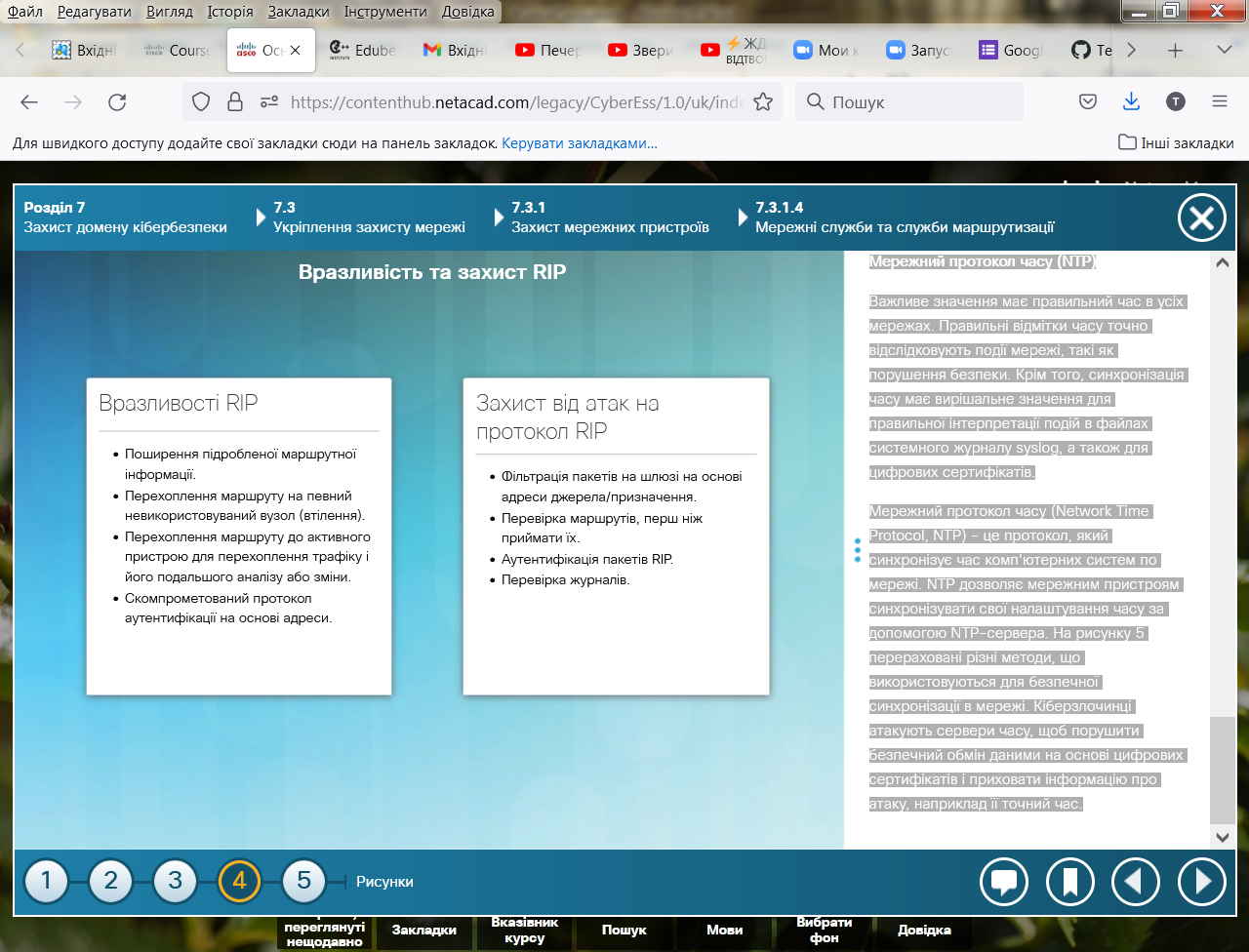
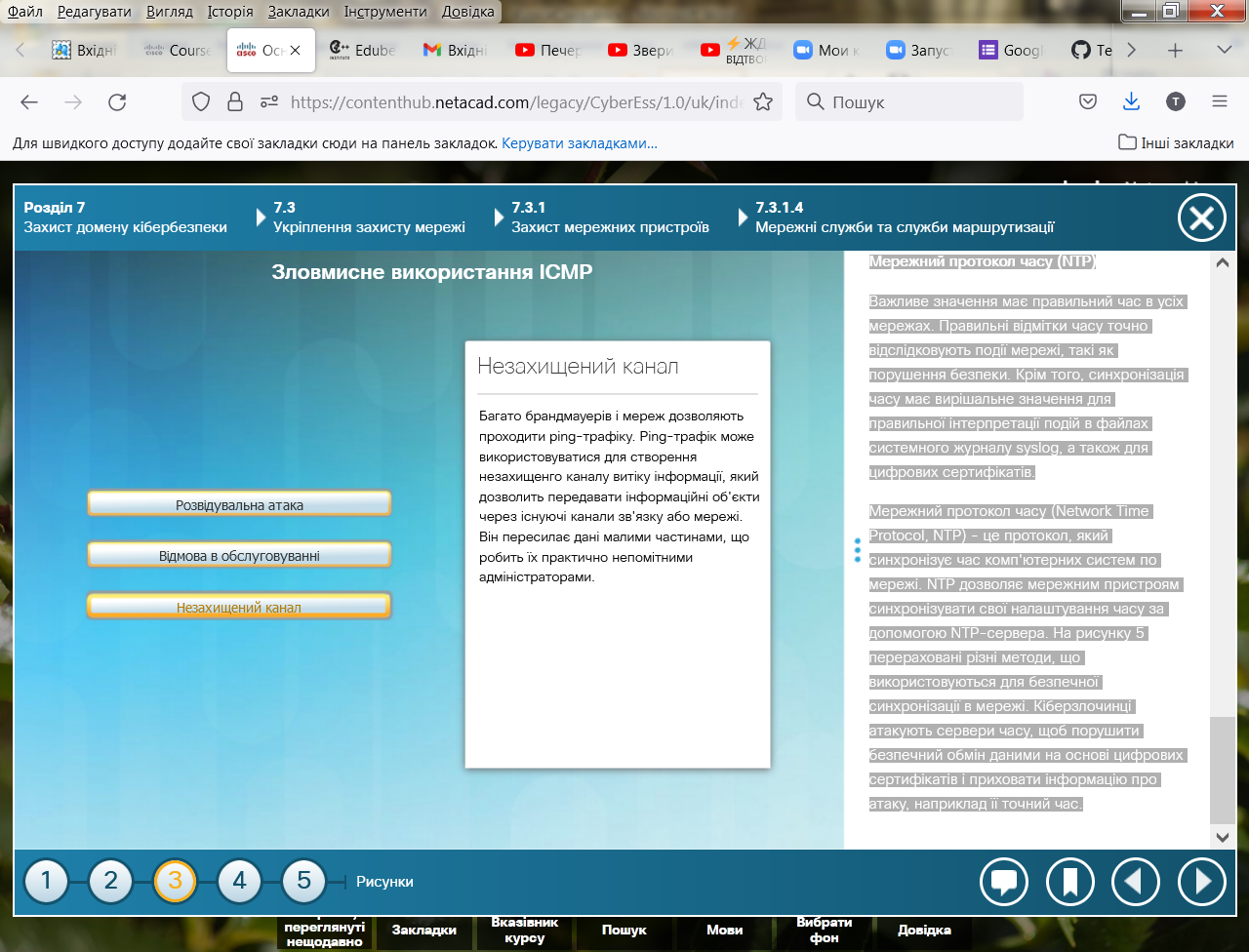


2

1

3

4



7

6

5

**VoIP обладнання**

Голос через IP (Voice over IP, VoIP) використовує такі мережі, як Інтернет, для здійснення та отримання телефонних дзвінків. Обладнання, необхідне для VoIP, включає в себе підключення до Інтернету плюс телефон. Для телефону є кілька варіантів:

* Традиційний телефон з адаптером (адаптер виступає як апаратний інтерфейс між традиційним, аналоговим телефоном та цифровою VoIP-лінією)
* Телефон із підтримкою VoIP
* Програмне забезпечення VoIP, встановлене на комп'ютері

Більшість споживачів VoIP-послуг використовують Інтернет для телефонних дзвінків. Багато організацій, однак, використовують свої приватні мережі, оскільки вони забезпечують більшу якість безпеки та якість обслуговування. Безпека VoIP безпосередньо залежить від безпеки мережі. Кіберзлочинці атакують ці системи, щоб отримати доступ до безкоштовних телефонних послуг, підслуховувати телефонні дзвінки або впливати на продуктивність і доступність.

Впроваджуйте наступні заходи захисту для забезпечення безпеки VoIP:

* Шифруйте пакети голосових повідомлень для захисту від прослуховування.
* Використовуйте SSH для захисту шлюзів і комутаторів.
* Змінюйте всі стандартні паролі.
* Використовуйте систему виявлення вторгнення для виявлення таких атак, як отруєння ARP.
* Використовуйте сильну аутентифікацію для мінімізації ризику підміни реєстрації (кіберзлочинці перенаправляють на себе всі вхідні дзвінки жертв), імітації проксі (кіберзлочинці хитрістю змушують жертву звертатися до створеного ними проксі-сервера) і перехоплення дзвінка (дзвінок перехоплюється і перенаправляється, перш ніж досягне місця призначення).
* Впроваджувати брандмауери, які розпізнають VoIP, для моніторингу потоків та фільтрації аномальних сигналів.

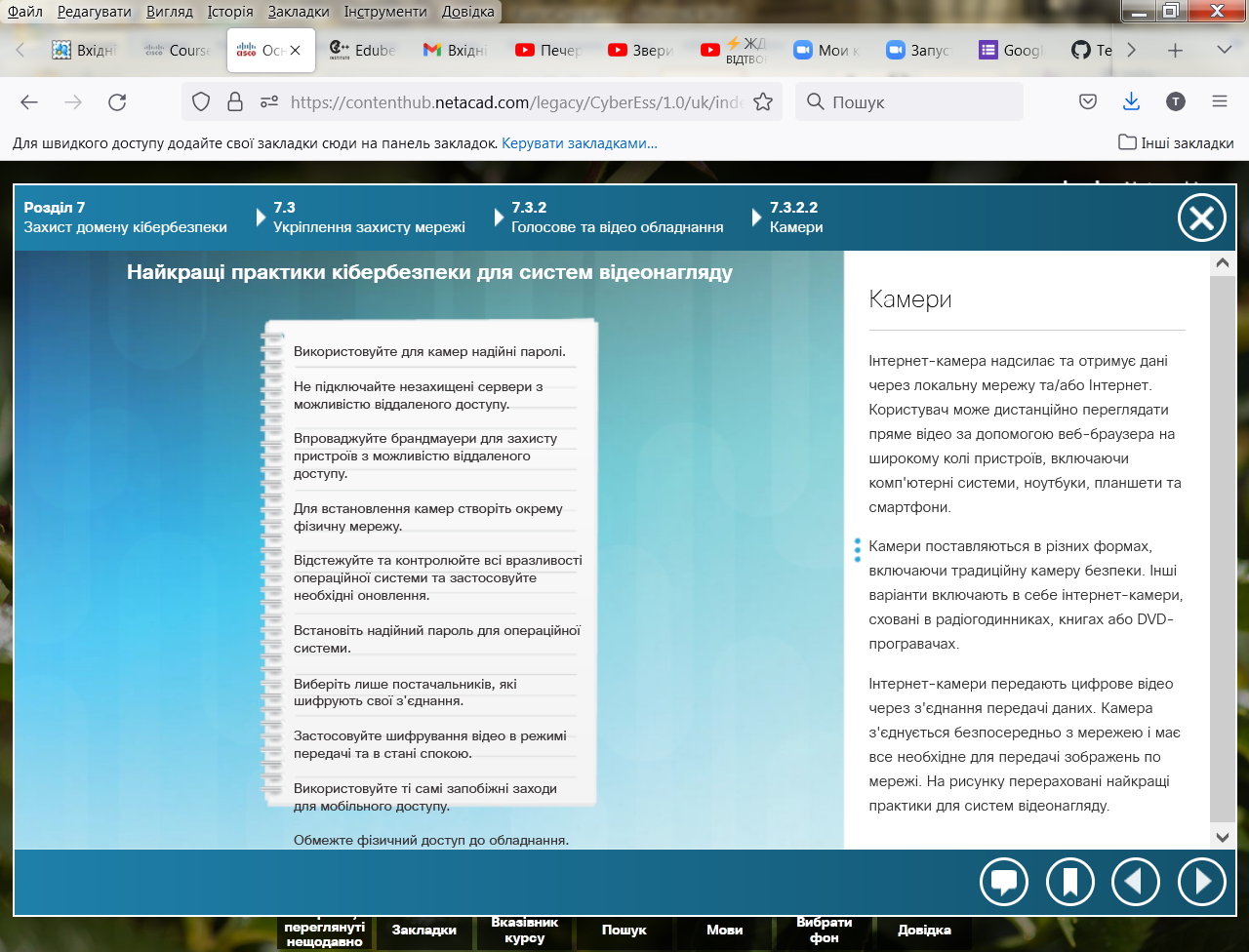
Порушення роботи мережі також веде до порушення голосового зв'язку.

**Камери**

Інтернет-камера надсилає та отримує дані через локальну мережу та/або Інтернет. Користувач може дистанційно переглядати пряме відео за допомогою веб-браузера на широкому колі пристроїв, включаючи комп'ютерні системи, ноутбуки, планшети та смартфони.

Камери поставляються в різних формах, включаючи традиційну камеру безпеки. Інші варіанти включають в себе інтернет-камери, сховані в радіогодинниках, книгах або DVD-програвачах.

Інтернет-камери передають цифрове відео через з'єднання передачі даних. Камера з'єднується безпосередньо з мережею і має все необхідне для передачі зображень по мережі. На рисунку перераховані найкращі практики для систем відеонагляду.



# Обладнання для відеоконференцзв'язку

Відеоконференції дозволяють двом або більше клієнтам у різних місцеположеннях спілкуватися одночасно за допомогою телекомунікаційних технологій. Ці технології використовують нові стандарти відео високої якості. Продукти, такі як Cisco TelePresence, дозволяють групі людей в одному місці зв'язатися з групою людей з інших регіонів у режимі реального часу. Відеоконференції є частиною звичайних щоденних операцій у таких галузях, як медична. Лікарі можуть оглядати пацієнта та проконсультуватися з експертами по виявленим симптомам з метою визначення можливих методів лікування.

У багатьох місцевих аптеках працюють фельдшери, які можуть зв'язуватися з лікарями, використовуючи телеконференції, щоб запланувати візит або проконсультуватися при наданні надзвичайної допомоги. Багато виробничіх організацій використовують телеконференції, щоб допомогти інженерам та технікам виконувати складні операції або завдання з технічного обслуговування. Обладнання для відеоконференцій може бути надзвичайно дорогим та представляти інтерес для злодіїв та кіберзлочинців. Натисніть [тут](https://youtu.be/WlDkiwzzv3M) щоб переглянути відео про можливості систем відеоконференцзв'язку. Кіберзлочинці атакують ці системи, щоб підслухувати відеодзвінки або впливати їх продуктивність та доступність.

**Мережні датчики і датчики IoT**

Одним із найбільш швидкозростаючих напрямів інформаційних технологій є використання інтелектуальних пристроїв та датчиків. Комп'ютерна індустрія брендує цей сектор як Інтернет речей (Internet of Things, IoT). Підприємства та споживачі використовують пристрої IoT для автоматизації процесів, моніторингу стану навколишнього середовища та попередження користувачів про несприятливі умови. Більшість пристроїв IoT підключаються до мережі через бездротові технології. У число таких пристроїв входять камери, дверні замки, датчики близькості, світла та інші типи датчиків, які використовуються для збору інформації про навколишнє середовище або стан пристрою. Деякі виробники приладів використовують IoT, щоб інформувати користувачів про необхідність заміни компонентів, збої компонентів, або їх запаси вичерпуються.

Підприємства використовують ці пристрої для відстеження інвентарю, транспортних засобів та наявність персоналу. Пристрої IoT містять геопросторові датчики. Користувач може глобально відслідковувати та контролювати зміни навколишнього середовища, такі як температура, вологість та освітлення. ІоТ-індустрія становить величезну проблему для фахівців з інформаційної безпеки, оскільки багато пристроїв IoT збирають та передають конфіденційну інформацію. Кіберзлочинці атакують ці системи, щоб перехопити дані або впливати на продуктивність та доступність систем.

# Огородження та барикади

Фізичні бар'єри - це перше, що приходить на розум, коли мислимо про фізичну безпеку. Це зовнішній рівень безпеки і ці рішення є найбільш загальнодоступними. Система охорони периметра зазвичай складається з наступних компонентів:

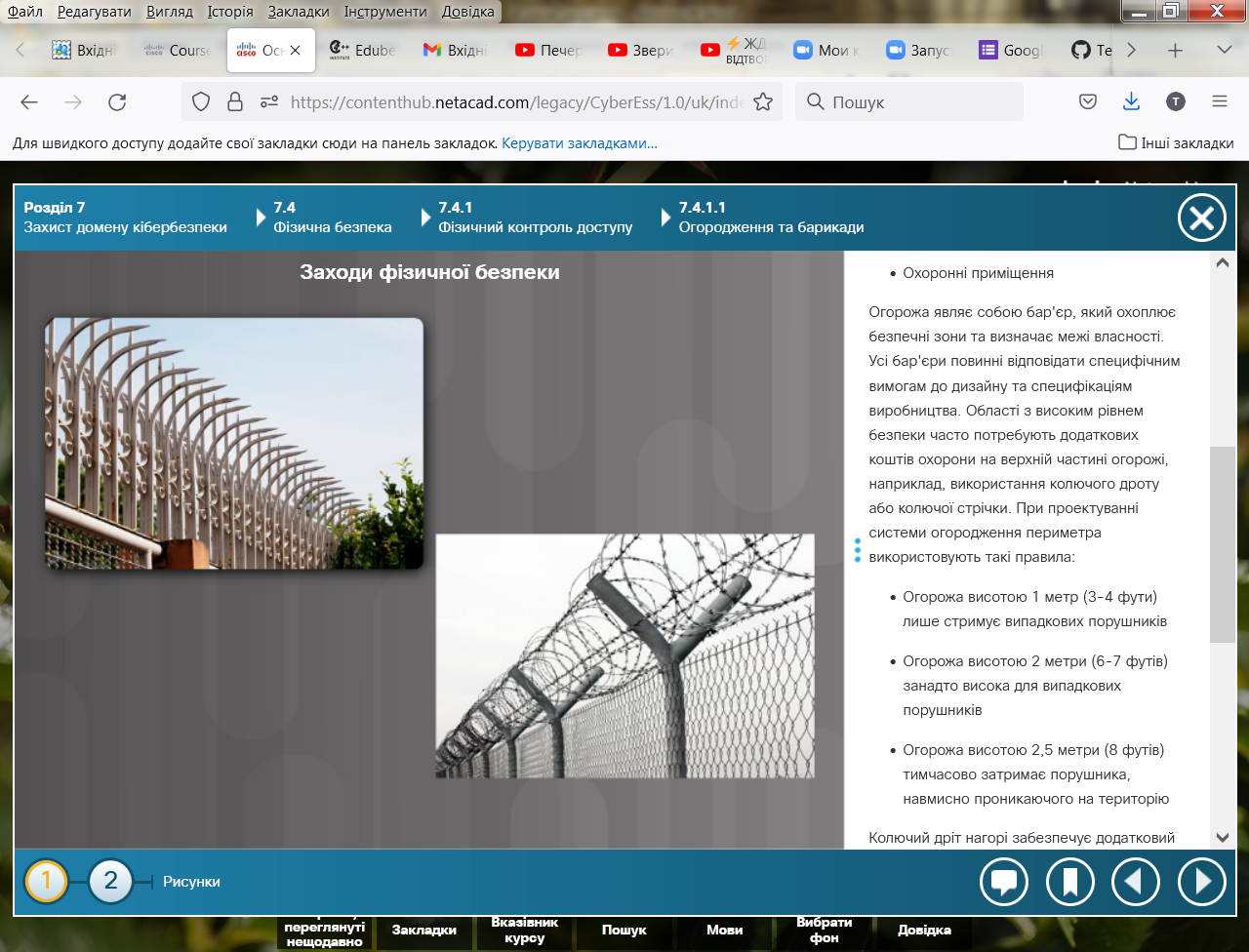
* Система огорожі периметра
* Система безпеки воріт
* Блокатори руху (короткий пост, який використовується для захисту від вторгнень автомобіля, як показано на рисунку 2)
* Перешкоди для в'їзду автомобіля
* Охоронні приміщення

Огорожа являє собою бар'єр, який охоплює безпечні зони та визначає межі власності. Усі бар'єри повинні відповідати специфічним вимогам до дизайну та специфікаціям виробництва. Області з високим рівнем безпеки часто потребують додаткових коштів охорони на верхній частині огорожі, наприклад, використання колючого дроту або колючої стрічки. При проектуванні системи огородження периметра використовують такі правила:

* Огорожа висотою 1 метр (3-4 фути) лише стримує випадкових порушників
* Огорожа висотою 2 метри (6-7 футів) занадто висока для випадкових порушників
* Огорожа висотою 2,5 метри (8 футів) тимчасово затримає порушника, навмисно проникаючого на територію

Колючий дріт нагорі забезпечує додатковий стримуючий ефект і може затримати порушника, серйозно поранивши його. Однак зловмисники можуть використовувати ковдру або матрац для зменшення цієї загрози. Місцеві правила можуть обмежувати тип системи огородження, яку може використовувати організація.

Регулярно оглядайте системи огородження. Тварини можуть підкопувати під огорожею, або земля може вимиватися, залишаючи огородження нестійким, забезпечуючи легкий доступ для вторгнення. Регулярно оглядайте системи огородження. Забороняється паркування транспортних засобів поблизу огорожі. Припаркована машина біля огорожі може допомогти зловмисникові піднятися або пошкодити її. Натисніть [тут](http://www.chainlinkinfo.org/security-fencing-guidelines/) для додаткових рекомендацій щодо огородження.



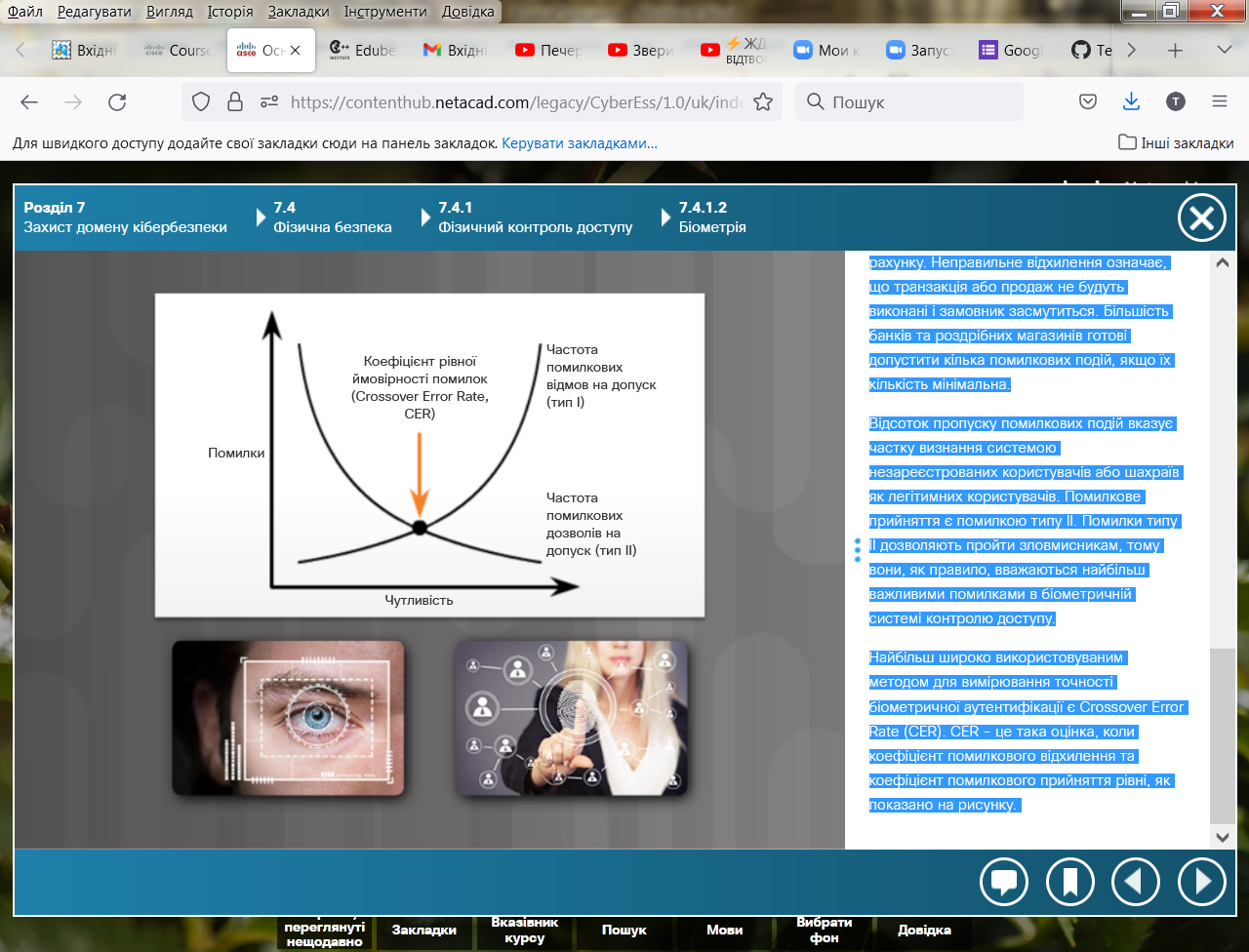
1

# 

2

# Біометрія

Біометрія описує автоматизовані методи розпізнавання особи на основі фізіологічних або поведінкових характеристик. Біометричні системи аутентифікації включають вимірювання обличчя, відбитків пальців, геометрії рук, райдужній оболонці і сітківці ока, рукописному почерку та голосу. Біометричні технології можуть стати основою для добре захищених рішень ідентифікації та посвідчення особи. Збільшення кількості порушень безпеки і шахрайства з транзакціями призвело до зростання популярності використання біометричних систем. Біометрія забезпечує конфіденційність фінансових операцій та особистих даних Наприклад, Apple використовує технологію відбитків пальців у смартфонах. Відбиток пальця користувача розблоковує пристрій і отримується доступ до різних застосунків, таких як онлайн-банкінг або платні додатки.

При порівнянні біометричних систем слід врахувати кілька важливих факторів: точність, швидкість або пропускну здатність, прийнятність для користувачів, унікальність біометричного органу або дії, стійкість до фальсифікації, надійність, вимоги щодо зберігання даних, час реєстрації та зручність процедури сканування. Найважливішим фактором є точність. Точність виражена за типом помилок і її показниками.

Перший клас - це помилки типу I або помилкові відхилення. Вони відбуваються, коли відмовлено в доступі зареєстрованому авторизованому користувачеві. З точки зору розмежування доступу, якщо потрібно перешкодити доступ зловмисникам, помилкове відхилення є найменш важливою помилкою. Однак у багатьох біометричних застосунках помилкові відмови можуть мати дуже негативний вплив на бізнес. Наприклад, банківський або роздрібний магазин повинен ідентифікувати клієнта та залишок на рахунку. Неправильне відхилення означає, що транзакція або продаж не будуть виконані і замовник засмутиться. Більшість банків та роздрібних магазинів готові допустити кілька помилкових подій, якщо їх кількість мінімальна.

Відсоток пропуску помилкових подій вказує частку визнання системою незареєстрованих користувачів або шахраїв як легітимних користувачів. Помилкове прийняття є помилкою типу II. Помилки типу II дозволяють пройти зловмисникам, тому вони, як правило, вважаються найбільш важливими помилками в біометричній системі контролю доступу.

Найбільш широко використовуваним методом для вимірювання точності біометричної аутентифікації є Crossover Error Rate (CER). CER - це така оцінка, коли коефіцієнт помилкового відхилення та коефіцієнт помилкового прийняття рівні, як показано на рисунку.

**Перепустки та журнали доступу**

Перепустка дозволяє людині отримати доступ до області з автоматизованими точками входу. Точка входу може бути: двері, турнікет, ворота або інший бар'єр. В перепустках використовуються різні технології, такі як магнітна смуга, штрихкод або біометрія.

Картрідер зчитує номер, що міститься на перепустці. Система надсилає номер на комп'ютер, який приймає рішення щодо доступу на основі наданих облікових даних. Система реєструє транзакцію і згодом можна звернутися до цієї інформації. У звітах вказуються, хто увійшов, час і точка входу.

**Охорона і супровід**

Всі фізичні засоби контролю доступу, включаючи системи стримування та виявлення, в кінцевому підсумку залежать від персоналу, який повинен втручитися та припинити фактичний напад або вторгнення. На об'єктах з системою інформаційної охорони високого рівня доступ до особливо важливих зон організації контролюється охоронцями. Перевага використання охоронців полягає в тому, що вони можуть адаптуватися краще, ніж автоматизовані системи. Охорона може дослідити і розрізнити різні умови та ситуації і прийняти рішення на місці. Це є кращим рішенням для контролю доступу, коли ситуація вимагає миттєвої і адекватної реакції. Однак охоронці не завжди є найкращим рішенням. Існують численні недоліки використання охоронців, включаючи витрати і неможливість контролювати і реєструвати великий обсяг трафіку. Використання охоронців також вносить фактор людської помилки.

**Відеоспостереження і спостереження з використанням електронних засобів**

Відеоспостереження і спостереження з використанням електронних засобів може доповнити, а в деяких випадках і замінити охоронців. Переваги відеоспостереження або спостереження з використанням електронних засобів - це можливість відслідковувати зони навіть за відсутності охоронців або персоналу, здатність записувати та реєструвати відео та дані спостереження протягом тривалого періоду часу, а також можливість використання детекторів руху та сповіщення.

Крім того, можна забезпечити більш високу точність фіксації подій навіть після того, як вони відбулися. Іншою важливою перевагою цього типу забезпечення безпеки є можливість вести спостереження з точок, важкодоступних для охоронців. Також може бути набагато економічніше використовувати камери для моніторингу всього периметру об'єкта. В добре захищеній організації відеоспостереження або спостереження з використанням електронних засобів повинні бути розміщені на всіх входах, виходах, вантажних відсіках, сходах та місцях збирання сміття. У більшості випадків ці системи доповнюють охоронців.

**RFID та бездротовий нагляд**

Відстеження розташування важливих ресурсів інформаційної системи та керування ними є ключовим завданням для більшості організацій. Зростання кількості мобільних пристроїв та пристроїв IoT зробило цю роботу ще більш складнішою. Час, витрачений на пошук критичного обладнання, може призвести до дорогих затримок або простоїв. Використання пристроїв радіочастотної ідентифікації (Radio Frequency Identification, RFID) дозволяє істотно полегшити роботу персоналу служби безпеки. Організація може помістити зчитувачі RFID в дверних рамах захищених приміщень так, щоб вони не були непомітні для людей.

Перевага інвентаризаційних RFID-міток полягає в можливості відстежувати будь-який актив, який фізично залишає захищену зону. Нові системи інвентаризаційних RFID-міток можуть одночасно зчитувати кілька міток. RFID-система не вимагає прямої видимості для сканування міток. Ще однією перевагою RFID є можливість читати пристрої, які не видно. На відміну від штрих-кодів та міток, зчитувальних за допомогою людини, які повинні бути фізично розташовані в легкодоступних місцях, при скануванні RFID-мітки не обов'язково повинні бути видимими. Наприклад, щоб фізично виявити і переглянути штрих-код або візуальну мітку на корпусі ПК під столом, співробітник повинен буде забратися під стіл. Використання RFID-мітки дозволить персоналу сканувати його, навіть не бачачи його.

**Глава. Захист домену кібербезпеки**

У цьому розділі обговорювалися технології, процеси та процедури, які спеціалісти з кібербезпеки використовують для захисту систем, пристроїв та даних, які складають мережну інфраструктуру.

Забезпечення безпеки хостів включає в себе захист операційної системи, впровадження антивірусних рішень і використання рішень на основі хоста, таких як брандмауери і системи виявлення вторгнень.

Забезпечення безпеки сервера включає в себе керування віддаленим доступом, захист привілейованих облікових записів та послуги моніторингу.

Захист даних включає контроль доступу до файлів та здійснення заходів безпеки для забезпечення конфіденційності, цілісності та доступності даних.

Забезпечення безпеки пристрою також передбачає впровадження перевірених методів фізичного захисту мережних пристроїв. Захист вашого домену кібербезпеки - це безперервний процес захисту мережної інфраструктури організації, який вимагає постійної пильності щодо загроз.