ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БАЗИ ДАНИХ ДЛЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

першого рівня вищої освіти

м. Кропивницький

1. Загальна інформація

Назва дисципліни	**Бази даних для мережевої інфраструктури**
Викладач	Лектор – Петренюк Володимир Ілліч, кандидат фізико-математичних наук, доцент, доцент кафедри кібербезпеки та програмного забезпечення
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8^{30} до 14^{20}
E-mail:	petrenjukvi@i.ua
Консультації	*Очні консультації* відповідно до затвердженого графіку консультацій *Онлайн консультації* засобами електронної пошти, мессенджерів (Facebook-Messenger / Viber / Telegram) у робочі дні

2. Анотація дисципліни

Курс «Бази даних для мережевої інфраструктури» спрямована на формування у здобувачів вищої освіти практичних компетентностей у сфері системного та мережевого адміністрування, необхідних для підтримки працездатності ключових інфраструктурних сервісів комп'ютерних мереж. Основна ідея курсу полягає у вивченні мережевих сервісів як систем, що оперують структурованими даними у вигляді спеціалізованих баз даних або розподілених сховищ, а також у набутті вмінь діагностувати та усувати типові збої у їх роботі. У курсі розглядаються інфраструктурні сервіси, що забезпечують функціонування корпоративних мереж: DNS як розподілена ієрархічна база доменних записів, DHCP як система обліку адресних параметрів, веб-проксі як кеш-сховище контенту, SNMP як механізм доступу до параметрів і станів мережевого обладнання, протокол RADIUS як основа AAA (автентифікація, авторизація, облік), LDAP як централізована служба каталогів користувачів і груп, а також Kerberos як реалізація єдиного входу в доменних середовищах. Додатково вивчаються технології VPN і засоби автоматизованого мережевого розгортання операційних систем. Практичний компонент дисципліни побудований на лабораторних роботах з використанням типових інструментів Windows та Linux.

3. Мета і завдання дисципліни

Метою викладання дисципліни «Бази даних для мережевої інфраструктури» є забезпечення здобувачів вищої освіти знаннями та практичними навичками з адміністрування мережевих сервісів, що використовують бази даних і сховища для зберігання службової інформації, а також підготовка до розгортання, супроводу та відновлення працездатності інфраструктурних компонентів IT-середовища підприємства.

Основними **завданнями** вивчення дисципліни є формування у здобувачів здатності проєктувати та обслуговувати сервіси мережевої інфраструктури, які забезпечують адресацію, іменування, доступ до ресурсів і централізоване керування обліковими даними користувачів. Дисципліна передбачає засвоєння принципів функціонування мережевих протоколів і механізмів інтеграції робочих станцій та мережевих пристроїв у корпоративне середовище. Окремим завданням курсу є розвиток навичок моніторингу, пошуку несправностей та усунення збоїв у роботі ОС і сервісів (DNS, DHCP, LDAP, RADIUS, Kerberos тощо) із використанням сучасних адміністративних інструментів. Також дисципліна формує практичну підготовку, необхідну для подальших професійних курсів і застосування отриманих знань у реальних умовах експлуатації мережевої інфраструктури.

4. Результати навчання

У результаті вивчення дисципліни здобувач вищої освіти повинен:

Знати:

– принципи функціонування базових інфраструктурних мережевих сервісів і протоколів, зокрема DNS та DHCP, їх роль у забезпеченні адресації та іменування в корпоративній мережі;

– призначення та механізми реалізації AAA (автентифікації, авторизації та обліку доступу) у корпоративному середовищі;

– принципи роботи прикладних протоколів і сервісів SNMP, RADIUS, LDAP, Kerberos, а також типові підходи до діагностики й відновлення працездатності мережевих служб.

Вміти:

– встановлювати та адмініструвати інфраструктурні сервіси й супутнє програмне забезпечення в середовищах ОС Linux та Windows;

– налаштовувати конфігурації мережевих сервісів відповідно до заданих вимог, формувати політики доступу та параметри роботи служб;

– виконувати перевірку коректності роботи сервісів локально та з інших пристроїв мережі, виявляти помилки конфігурації та усувати несправності у функціонуванні мережевих служб.

5. Обсяг дисципліни

Ознака дисципліни	
Кількість кредитів / годин	4/120
Нормативна / вибіркова	вибіркова
Вид підсумкового контролю	залік

6. Політика дисципліни

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення. Детальніше за посиланням URL : http://www.kntu.kr.ua/doc/dobro.pdf

Відвідування занять

Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і лабораторні заняття курсу.

Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Поведінка на заняттях

Недопустимість: запізнень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення навчальних дисциплін вільного вибору; Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ, Кодексу академічної доброчесності ЦНТУ.

7. Програма навчальної дисципліни

Тема 1. Інфраструктурні мережеві сервіси та їх роль у корпоративній мережі
Призначення базових сервісів. Поняття службових баз даних/сховищ у мережевій інфраструктурі. Типові сценарії використання.
Тема 2. Система доменних імен DNS як розподілена база даних
Архітектура DNS. Зони, записи, кешування. Налаштування та діагностика DNS-сервісу.
Тема 3. DHCP та керування адресним простором мережі
Призначення DHCP, моделі видачі адрес, резервування. DHCP-сервер і клієнт. Перевірка та усунення типових проблем.
Тема 4. Проксі-сервіси та веб-кешування (HTTP/Proxy)
Огляд HTTP та принцип роботи веб-проксі. Кешування запитів, політики доступу, контроль трафіку. Практичні сценарії.
Тема 5. Моніторинг мережевих пристроїв і сервісів: SNMP
Архітектура SNMP. MIB, OID, агенти. Збір і аналіз параметрів стану обладнання та сервісів.
Тема 6. Централізована автентифікація та облік доступу: RADIUS, PAM, NSS
AAA-модель. Роль RADIUS у мережевій автентифікації. Інтеграція з системними механізмами PAM/NSS.
Тема 7. Служба каталогів LDAP та керування обліковими записами
Поняття каталогу. Структура LDAP, об’єкти, атрибути. Централізоване зберігання даних користувачів і груп.
Тема 8. Безпечна інфраструктура: Kerberos, PKI, VPN та мережеве розгортання
Єдиний вхід і Kerberos. Основи криптографії та інфраструктура відкритих ключів. VPN (IPsec), конфіденційність (Tor). Автоматизована інсталяція ОС у мережі (PXE).

8. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.
Методи контролю: спостереження за навчальною діяльністю, усне опитування, письмовий контроль, тестовий контроль.
Форма підсумкового контролю: залік.

Поточний контроль передбачає оцінювання кожної лабораторної роботи. Основними критеріями є правильність виконання завдання, якість захисту роботи та дотримання встановлених термінів. У процесі оцінювання враховується рівень розуміння теоретичного матеріалу та сформованість практичних навичок.

Підсумковий контроль здійснюється у формі заліку, який оцінює ступінь засвоєння теоретичних положень дисципліни та здатність студента застосовувати отримані знання на практиці. Однак, в процесі вивчення дисципліни передбачено виконання комплексу робіт під час лекційних та лабораторних занять, а також індивідуальних завдань. У зв’язку з цим здобувачам вищої освіти може бути виставлена оцінка понад 60 балів без обов’язкового виконання підсумкової залікової роботи.

9. Рекомендована література

Базова

1. Michael W Lucas. SNMP Mastery. — Tilted Windmill Press, 2020 – 260 pp.
2. Jon C. Snader. VPNs Illustrated: Tunnels, VPNs, and IPsec — Addison-Wesley, 2015. — 711 pp.
3. Ron Aitchison. Pro DNS and BIND 10. — Apress, 2011. — 692 pp.
4. Raphaël Hertzog, Roland Mas. The Debian Administrator's Handbook, Debian Buster from Discovery to Mastery. — Lulu.com, 2020. — 542 pp.

Допоміжна

5. James S. Tiller. A Technical Guide to IPSec Virtual Private Networks. — CRC Press, 2017. — 376 pp.
6. Evi Nemeth, Garth Snyder, Trent R. Hein et al. UNIX and Linux System Administration Handbook. — Addison Wesley, 2018. — 1179 pp.
7. Sam R. Alapati. Modern Linux Administration: How to Become a Cutting-edge Linux Administrator. — O'Reilly Media, 2017. — 500 pp.

Інформаційні ресурси

8. Онлайн-курси Prometheus. – URL: https://prometheus.org.ua/
9. Онлайн-курси Coursera. – URL: https://www.coursera.org
10. Академія Cisco. – URL: https://www.netacad.com
11. Он-лайн ресурс з інформаційних технологій. – URL:https://habr.com
12. Он-лайн ресурс з інформаційних технологій. – URL:https://dou.ua/
13. Пошукова система. – URL:https://www.google.com/
14. Он-лайн ресурс перегляду відеоуроків.– URL:https://www.youtube.com