



Силабус освітнього компонента

Програма навчальної дисципліни



Комп'ютерні мережі

Шифр та назва спеціальності

257 – Управління інформаційною безпекою

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Освітня програма

Управління інформаційною безпекою

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Спеціальна (фахова), Обов'язкова

Семестр

3

Мова викладання

Українська

Викладачі, розробники



ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua

Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем», «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна "Комп'ютерні мережі" є обов'язковою навчальною дисципліною. Мережеві технології та інтернет впливають на людей по-різному в різних країнах світу. У майбутньому основні напрямки для розробників нових технологій будуть пов'язані з використанням інтернет в якості бази для створення нових продуктів і послуг, розроблених спеціально з урахуванням можливостей мережі. Оскільки розробники розширюють межі досяжного, можливості взаємно підключених мереж, що утворюють інтернет, гратимуть дедалі все більше значення в досягненні успіху цих проектів.

Мета та цілі дисципліни

Формування теоретичних знань основних принципів побудови сучасних мереж, до яких відносяться локальні, глобальні та регіональні мережі, за допомогою яких реалізуються нові

підходи управління сучасним інформаційним суспільством, а також формування практичних навичок із побудови та управління корпоративними системами та мережами.

Формат занять

Лекції, лабораторні роботи, самостійна робота, курсовий проект, консультації. Підсумковий контроль – іспит.

Компетентності

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-4. Здатність спілкуватися державною мовою як усно, так і письмово.

КЗ-5. Здатність спілкуватися іноземною мовою.

КЗ-6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.

ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.

ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.

ФК-6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.

ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.

ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

ФК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.

ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.

ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

ПРН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.

ПРН-4. Вільно спілкуватися державною мовою.

ПРН-5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.

ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки

ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.

ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

ПРН-11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.

ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.

ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

ПРН-17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отримання несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Законодавчі основи процесів інформатизації в Україні, вміння використовувати ОС Linux, знання механізмів роботи з Packet Tracer.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проекти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Основні положення теорії взаємодії відкритих систем.

Хронологічна наслідність важливих подій в історії розвитку комп'ютерних мереж. Хронологічна наслідність важливих подій в історії розвитку комп'ютерних мереж. Загальна структура системи зв'язку. Методи комутації. Протоколи глобальних мереж. Імовірно-тимчасові характеристики технологій ГВП. Стек протоколів мережі x.25. Теоретичні способи зменшення надмірності. Алгоритм стиснення повторюваних даних RLE. Алгоритми стиснення за ключовими словами KWE. Алгоритми кодування змінної довжини. Кодування інформації у локальних мережах.

Тема 2. Модель OSI.

Модель взаємодії відкритих систем. Багаторівнева система вкладання пакетів. Включення проміжних пристрій мережі. Функції різних рівнів iso/osi. Транспортний рівень. Методи взаємодії в мережі iso/osi. Функції різних рівнів iso/osi. Канальний рівень iso/osi. Фізичний рівень (physical layer - pl). Канальний рівень iso/osi. Апаратура локальних мереж. Основні функції адаптерів. Функції драйвера мережевого адаптера в моделі osi. Протоколи високих рівнів. Протоколи високих рівнів. Транспортні протоколи. Мережеві протоколи. Протоколи стеку apple talk і модель osi/iso. Класи мереж. Стандартні мережеві програмні засоби. Однорангові мережі. Мережі на основі серверу.

Тема 3. Якість обслуговування QoS.

Основні вимоги. Показник якості обслуговування мережі. Основні характеристики виробництва. Показники якості передачі даних. Допускні значення вимог до основних показників якості. Алгоритм розрахунку. Приклад розрахунку.

Тема 4. Методи повторної передачі.

Стек протоколів мережі x.25. Множина протоколів hdlc . Метод з зупинкою та очікуванням . ARQ з паралельним використанням віртуальних каналів. Повторна передача на n кроків назад. Ефективність роботи алгоритму ARQ на N кроків назад. Передача з виборчим повтором. Недоліки методу. Методика оцінки ефективності обміну даними у корпоративній мережі. Оцінки ефективності обміну даними у корпоративній мережі у каналах без пам'яті. Ефективність різних мереж без пам'яті.

Тема 5. Мережа Ethernet.

Мережі ethernet і fast ethernet . Стандарти категорії IEEE 802.X . Типи процедур LLC підрівнів . Адресації пакетів. Структура адреса. Метод доступу CSMA / CD . Виникнення конфлікту. Об'єднання кількох сегментів кабелю. Еволюція локальних мереж . Функціонування комутаторів локальної мережі. Передача кадру з порту на порт комутатора. Методи комутації . Управління потоком у напівдуплексному і дуплексному режимах. Технології комутації і модель osi. Трьохрівнева ієрархічна модель мережі.

Тема 6. Протокол мережевого рівня – IP протокол.

Типи адрес. Формати IP-адреси. IP-адресації версії 4. Формат заголовка IP . Угоди про особливості інтерпретації IP-адрес. Використання масок в IP адресації. Особливості IPV6. Заголовок IPV6 . Типи адрес в IPV6 . Форми представлення адреси . Модель адресації. Розподіл адресного простору. Протокол ARP . Структура заголовку ARP. Алгоритм використання ARP у ГВС . Маршрутизації в IP-мережах. Таблиці маршрутизації. Протокол DNS . Ієрархія імен в DNS . Типи записів DNS . Основні схеми дозволу DNS-імен.

Тема 7. Протоколи транспортного рівня.

Транспортний рівень. Transmission Control Protocol. Заголовок TCP. Структура заголовка TCP. TCP порти. Встановлення з'єднання TCP . Протокол UDP . UDP заголовок. Протокол TCP/IP . Функції рівнів. протокол RTP . Заголовок пакета RTP . Мережі на основі RTP. Послідовне включення змішувачів . Протокол RTCP . Пакети звіту RTCP. Формат пакета SDES (опис джерела). Характеристики джерела . Перевірка коректності заголовка RTCP .

Тема 8. Протоколи маршрутизації.

Протоколи маршрутизації. Фіксована маршрутизація. Адаптивна маршрутизація. Показники алгоритмів(метрики). Алгоритми маршрутизації. Динамічна маршрутизація. До маршрутизація. IGP: DISTANCE-VECTOR . IGP: LINK STATE. RIP:Освіта петель. OSPF (OPEN SHORTEST PATH FIRST).

Тема 9. Сучасні мережеві технології.

Компоненти мережі. Подання та топології мереж. Основні типи мереж. Інтернет-підключення. Надійні мережі. Безпека мережі.

Тема 10. Базова конфігурація комутатора та кінцевого пристрою.

Навігація по IOS. Структура команд. Базове налаштування пристроїв. Збереження змін. Порти та адреси. Налаштування IP-адресації.

Тема 11. Протоколи та моделі.

Правила. Протоколи. Набір протоколів. Організації зі стандартизації. Еталонні моделі. Інкапсуляція даних. Доступ до даних.

Тема 12. Фізичний рівень.

Призначення фізичного рівня. Характеристики фізичного рівня. Мідні кабелі. Кабелі UTP. Оптичолоконні кабелі. Бездротове середовище передачі даних.

Тема 13. Транспортний рівень.

Двійкова система числення. Шістнадцяткова система числення. Передача даних. Огляд протоколу TCP. Огляд UDP. Номери портів. Процес обміну даними за протоколом TCP. Надійність та керування потоком. Обмін даними за протоколом UDP. Прикладний рівень, рівень вистави, сеансовий рівень. Однорангові мережі. Протоколи веб-трафіку та електронної пошти. Сервіси IP-адресації. Сервіси обміну файлами.

Тема 14. Принципи забезпечення безпеки мереж.

Загрози та вразливість безпеки. Мережеві атаки. Захист від мережевих атак. Безпека пристроїв. Пристрої в мережі невеликого розміру. Програми та протоколи в мережі невеликого розміру. Масштабування до більших мереж. Перевірка підключення. Команди хоста та IOS. Методи пошуку та усунення несправностей. Сценарії пошуку та усунення несправностей.

Тема 15. Базова конфігурація маршрутизатора.

Початкове налаштування маршрутизатора. Налаштування інтерфейсів. Налаштування стандартного шлюзу.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Вивчення мережевих інструментів спільної роботи.

Тема 2. Вивчення вакансій в сфері інформаційних і мережевих технологій.

Тема 3. Вивчення сервісів конвергентних мереж.

Тема 4. Packet Tracer. Навігація по IOS.

Тема 5. Packet Tracer. Налаштування початкових параметрів комутатора.

Тема 6. Початок роботи консолі за допомогою програми Tera Term.

Тема 7. Packet Tracer. Створення основних підключень.

Тема 8. Створення простої мережі.

Тема 9. Налаштування адреси управління комутатором.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (<http://surl.li/pxssv>), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:

CCNA1

<https://www.netacad.com/catalogs/learn?category=course>.

Література та навчальні матеріали

Основна література:

1. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.

<http://kist.ntu.edu.ua/textPhD/tzi.pdf>.

2. Волосюк Ю.В. Комп'ютерні мережі: курс лекцій / Ю. В. Волосюк. - Миколаїв: МНАУ, 2019. - 203 с.

https://dspace.mnau.edu.ua/jspui/bitstream/123456789/6377/1/Kompiuterni_merezhi_kurs_lektsii.pdf

3. Kurose James F., Ross Keith W. Computer Networking: A Top-Down Approach. 6th Edition / James F. Kurose, Keith W. Ross. - TX: Pearson, 2012. - 864 p.

<https://broman.dev/download/Computer%20Networking:%20A%20Top-Down%20Approach%206th%20Edition.pdf>

4. CCNAv7: Введення в ресурси курсу Networks [Електронний ресурс]. – Режим доступу:

<https://www.netacad.com/portal/resources/course-resources/ccna-itn>.

5. Bonaventure O. Computer Networking: Principles, Protocols and Practice. - Louvain-la-Neuve: Universite catholique de Louvain (Belgium), 2019. - 272 p.

<https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf>

6. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

<https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnologii-zakhystu.pdf>.

Додаткова література :

7. Технологія Ethernet: лабораторний практикум / М. О. Білова, С. П. Євсєєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко. - Львів: "Новий Світ - 2000", 2020. - 196 с.

<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 30% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- курсовий проєкт: 20% семестрової оцінки;
- іспит: 40% семестрової оцінки

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: <http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/>

Погодження

Силабус погоджено

28.08.2024



Завідувач кафедри

Сергій ЄВСЕЄВ

28.08.2024



Гарант ОП

Роман КОРОЛЬОВ