

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Харківський національний університет внутрішніх справ

Кафедра кібербезпеки та DATA-технологій, факультет №6

ПРОГРАМА

навчальної дисципліни «Телекомунікаційні системи та мережі нового
покоління»

вибіркових компонент освітньої програми
другого (магістерського) рівня вищої освіти

Спеціальність: 125 "Кібербезпека"(«Безпека інформаційних
та комунікаційних систем»)

Харків 2022

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30 .01.23 № 1

СХВАЛЕНО

Вченою радою факультету № 6
Протокол від 13 .01.23 № 1

ПОГОДЖЕНО

Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 27 .01.23 № 1

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій
(протокол від 13 .01.23 № 1)

Розробники:

1. Професор кафедри, д.т.н., професор Семенов С.Г.
2. Професор кафедри, д.т.н., проф. Можжаєв О.О.
3. Завідувач кафедри, к.т.н., Гнусов Ю.В.

Рецензенти:

1. Доцент кафедри боротьби з кіберзлочинністю ХНУВС, к.т.н., доцент Клімушин П.С.;
2. Завідувач кафедри ЕОМ ХНУРЕ д.т.н., професор, Коваленко А.А.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Метою викладання навчальної дисципліни «Телекомунікаційні системи та мережі нового покоління» є ознайомлення студентів з сучасними технологіями розробки та впровадження телекомунікаційних технологій, систем та засобів, формування у них компетенцій, що необхідні для вирішення задач проектування телекомунікаційних систем нового покоління.

Основними завданнями вивчення дисципліни „Телекомунікаційні системи та мережі нового покоління” є розвиток у студентів практичних навичок щодо розуміння проблем, які виникають при практичному застосуванні телекомунікаційних систем та засобів; ознайомити студентів з сучасними методами передачі даних в телекомунікаційних системах.

Міждисциплінарні зв’язки: викладання дисципліни «Телекомунікаційні системи та мережі нового покоління» базується на знаннях дисциплін «Вища математика», «Теорія інформації і кодування», «Електроніка та схемотехніка», «Мережеві технології».

Очікувані результати навчання: у результаті вивчення навчальної дисципліни здобувач вищої освіти повинен отримати наступні компетенції та результати навчання:

Програма навчальної дисципліни складається з таких тем:

ТЕМА № 1. ПРИНЦИПИ ПОБУДОВИ СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

ТЕМА № 2. ФУНКЦІОНАЛЬНА АРХІТЕКТУРА ТРАНСПОРТНИХ МЕРЕЖ

ТЕМА № 3 ТЕХНОЛОГІЯ NG-SDN

ТЕМА №4. СИСТЕМИ ПЕРЕДАЧІ ОПТИЧНОЇ ТРАНСПОРТНОЇ ІЄРАРХІЇ ОТН. БЛОК НАВАНТАЖЕННЯ ОПТИЧНОГО КАНАЛУ OPU.

ТЕМА №5. БЛОК ДАНИХ ОПТИЧНОГО КАНАЛУ ODU

ТЕМА №6. ЗАГОЛОВКИ ІНФОРМАЦІЙНИХ СТРУКТУР КАНАЛУ OSC

ТЕМА №7. ЗАГАЛЬНІ ТА СПЕЦІАЛЬНІ ВИМОГИ ДО КІБЕРБЕЗПЕКИ МЕРЕЖ НАСТУПНИХ ПОКОЛІНЬ

ТЕМА №8. КІБЕРБЕЗПЕКА МЕРЕЖ НАСТУПНИХ ПОКОЛІНЬ У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

1. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни «Телекомунікаційні системи та мережі нового покоління» є ознайомлення студентів з сучасними технологіями розробки та впровадження телекомунікаційних технологій, систем та засобів, формування у них компетенцій, що необхідні для вирішення

задач проектування телекомунікаційних систем нового покоління.

Основними завданнями вивчення дисципліни „Телекомунікаційні системи та мережі нового покоління” є розвиток у студентів практичних навичок щодо розуміння проблем, які виникають при практичному застосуванні телекомунікаційних систем та засобів; ознайомити студентів з сучасними методами передачі даних в телекомунікаційних системах. 1.3. Форма підсумкового контролю залік.

На вивчення навчальної дисципліни відводиться 120 годин/3 кредитів ECTS.

1.4. Програмні компетентності:

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.	
Спеціальні (фахові, предметні) компетентності (СК)	ФК1.	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

2. Короткий опис змісту навчальної дисципліни

ТЕМА № 1. ПРИНЦИПИ ПОБУДОВИ СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Глобальна інформаційна інфраструктура та еволюція мереж зв'язку.

Архітектура сучасних систем NGN.

Технології транспортного рівня NGN.

ТЕМА № 2. ФУНКЦІОНАЛЬНА АРХІТЕКТУРА ТРАНСПОРТНИХ МЕРЕЖ

Багаторівнева модель транспортної мережі.

Функції архітектурних елементів функціональної архітектури.

ТЕМА № 3 ТЕХНОЛОГІЯ NG-SDH

Організація транспортування пакетного трафіка у системах NG-SDH.

Узагальнена процедура формування кадрів GFP.

Типи і структура кадрів.

Формування кадрів GFP-F та GFP-T.

Організація широкосмугових каналів у системах NG-SDH.

ТЕМА №4. СИСТЕМИ ПЕРЕДАЧІ ОПТИЧНОЇ ТРАНСПОРТНОЇ

ІЄРАРХІЇ ОТН. БЛОК НАВАНТАЖЕННЯ ОПТИЧНОГО КАНАЛУ OPU.

Інтерфейси мережі OTN.

Секціонування траси оптичного каналу в OTN.

Структура блоків OPUk, ODUk і OTUk.

Призначення і формат.

Упакування сигналів CBR2G5, CBR10G і CBR40G в OPUk.

Упакування кадрів GFP в OPUk.

Віртуальна конкатенація OPUk.

ТЕМА №5. БЛОК ДАНИХ ОПТИЧНОГО КАНАЛУ ODU

Заголовок блока даних ODUk.

Структура ідентифікатора точки доступу.

Передача контрольного слова BIP-8 заголовка ODUk.

Інтерпретація статусу ODUk

ТЕМА №6. ЗАГОЛОВКИ ІНФОРМАЦІЙНИХ СТРУКТУР КАНАЛУ OSC

Структура заголовків OTS-O, OMS-O, OCh-O та OTSiG-O в каналі OSC.

ТЕМА №7. ЗАГАЛЬНІ ТА СПЕЦІАЛЬНІ ВИМОГИ ДО КІБЕРБЕЗПЕКИ МЕРЕЖ НАСТУПНИХ ПОКОЛІНЬ

Базові принципи системи кібербезпеки мереж наступних поколінь.

Розширені вимоги до ідентифікації та кібербезпеки в NGN

ТЕМА №8. КІБЕРБЕЗПЕКА МЕРЕЖ НАСТУПНИХ ПОКОЛІНЬ У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Механізми та функції забезпечення зв'язку в надзвичайних ситуаціях у NGN.

Задачі кібербезпеки та принципи приєднання служб зв'язку в надзвичайних ситуаціях.

3. Рекомендована література

Основна література

1.

Телекомунікаційні системи та мережі наступного покоління: конспект лекцій. Модуль 5.2 / Педяш В.В. – Одеса: ОНАЗ ім. О.С. Попова, 2017. – 76 с.

2. Кібербезпека мереж наступних поколінь : навч. посібник / О.О.

Вараксін, Є.В. Васіліу, С.М. Горохов, В.Й. Кільдішев, В.Г. Кононович; за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2012. – 240 с.

3. Заїка В.Ф., Варфоломеева О.Г., Домрачева К.О., Гринкевич Г.О.. «Телекомунікаційні системи та мережі наступного покоління». - 2019.

4. Гніденко М.П., Вишнівський В.В., Ільїн О.О. Побудова SDN мереж. – Навчальний посібник. – Київ: ДУТ, 2019. – 190 с..

5. Рекомендація МСЕ-Т Y.110. Global Information Infrastructure principles and framework architecture (Принципи та архітектура глобальної інформаційної інфраструктури).

6. Рекомендація МСЕ-Т Y.101. Global Information Infrastructure terminology: Terms and definitions (Глобальна інформаційна інфраструктура:

Терміни та визначення).

7. Битнер В.И. Лекции по дисциплине "Сети следующего поколения" /Битнер В.И. □ Новосибирск: СибГУТИ, 2008. – 252 с.
8. Рекомендація МСЕ-Т Y.2001. Общий обзор СПП.
9. Рекомендація МСЕ-Т Y.2091. Terms and definitions for Next Generation Networks (Терміни та визначення для Мереж Наступного Покоління).
10. Рекомендація МСЕ-Т Y.2011. General principles and general reference model for Next Generation Networks (Основні принципи та опорна модель для Мереж Наступного Покоління)
11. Рекомендація МСЕ-Т Y.2012. Functional requirements and architecture of next generation networks (Функціональні вимоги та архітектура для Мереж Наступного Покоління).
12. Рекомендація МСЕ-Т Y.2031. Архитектура эмуляции сетей КТСОП/ЦСИС.
13. Рекомендація МСЕ-Т G.707/Y.1322. Network node interface for the synchronous digital hierarchy (SDH) (Інтерфейси вузлів мережі для синхронної цифрової ієрархії SDH).
14. Рекомендація МСЕ-Т G.7042/Y.1305. Схема регулировки пропускной способности линии (LCAS) для виртуальных сцепленных сигналов.
15. Рекомендація МСЕ-Т X.85/Y.1321. IP over SDH using LAPS (IP поверх SDH з використанням LAPS).
16. Рекомендація МСЕ-Т X.86/Y.1323. Ethernet over LAPS (Ethernet через LAPS).
17. Рекомендація МСЕ-Т G.7041/Y.1303. Generic framing procedure (GFP) (Основна процедура фреймування (GFP)).
18. Рекомендація МСЕ-Т G.872. Architecture of optical transport networks (Архітектура оптичних транспортних мереж).
19. Рекомендація МСЕ-Т G.870/Y.1352. Terms and definitions for optical transport networks (OTN) (Терміни та визначення для оптичних транспортних мереж (OTN)).

4. Засоби оцінювання здобувачів вищої освіти

1. Які повинні бути використані вимоги до інфокомунікаційних систем для їхнього застосування одночасно в локальних і глобальних мережах?
2. Яким чином підтримуються функції взаємодії між існуючою телефонною мережею та мультимедійною мережею криз міст?
3. Сформулювати спеціальні вимоги до інфокомунікаційної структури.
4. Які рівні охоплює структура інфокомунікаційної системи?
5. Охарактеризувати варіанти складу програмних комутаторів.
6. Якими протоколами декларується мета створення мереж NGN?
7. Охарактеризувати особливості та можливості NGN.
8. Які проблеми при мінімальних витратах вирішує впровадження NGN?
9. Яка технологія маршрутизації впроваджується в мережах NGN?
10. Охарактеризувати архітектуру мережі NGN.
11. Яким механізмом безпеки повинна бути відповідна мережа NGN?

12. Розподіл функцій страт між обслуговуванням і транспортом.
13. Що таке страта послуг? Які площини виділяються в кожній страті?
14. Що таке страта транспорту?
15. Функції управління загальної функціональної моделі NGN з точки зору захисту. Питання забезпечення безпеки функцій транспорту.
16. Охарактеризувати страти з точки зору менеджменту.
17. Охарактеризувати архітектуру широкосмугової конвергентної мережі. Поясніть визначення кібербезпеки та кіберсередовища.
18. Яка природа середовища кібербезпеки?
19. Охарактеризуйте структурну модель NGN з позицій кібербезпеки.
20. Дайте перелік цілей проектування мереж майбутнього.
21. Яка модель довіри щодо кібербезпеки NGN?
22. Яка функціональна гнучкість проектується реалізувати в мережах майбутнього?
23. Поясніть головні інтерфейси взаємодії телекомунікаційних мереж.
24. Яка функціональна архітектура NGN з позицій кібербезпеки?
25. Які ресурси підлягають захисту та цілі захисту в мережах майбутнього?
26. Цілі та задачі захисту цінностей, ресурсів та інтерфейсів NGN, пов'язаних з UNI.
27. Цілі та задачі захисту цінностей, ресурсів, інформації та інтерфейсів, пов'язаних із транспортним рівнем.
28. Цілі та задачі захисту цінностей, ресурсів, інформації та інтерфейсів, пов'язаних з рівнем послуг у частині менеджменту послугами.
29. Цілі та задачі захисту цінностей, ресурсів, інформації та інтерфейсів, пов'язаних з рівнем послуг у частині підтримки застосувань і послуг.
30. Цілі та задачі захисту цінностей, ресурсів, інформації та інтерфейсів, пов'язаних з адмініструванням.
31. Якими методами й засобами буде розвинена ідентифікація в мережах майбутнього?