СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	Управління мережевою безпекою
Мова викладання	українська
Викладач	Петренко Тарас Анатолійович, доцент
Профайл викладача	Сайт кафедри: https://mmi.stu.cn.ua/personal-kafedry/ Google академія: https://scholar.google.com/citations?user=2bJE-4IAAAAJ&hl=ru
Контакти викладача	тел.: 0636419136, e-mail: mail_taras@ukr.net

1. Анотація курсу – сьогодні передача інформації на відстань практично неможлива без використання різного роду інформаційно-комунікаційних мереж. При цьому виникає багато загроз втрати конфіденційності, цілісності та доступності інформації. Для забезпечення безпечного функціонування сучасних інформаційних систем необхідно надійне і ефективне управління не тільки самими мережами, але і засобами мережевої безпеки. Саме тому управління мережевою безпекою є актуальною, технічною, теоретичною та практичною проблемою. Необхідність управління захистом інформаційно-комунікаційних мереж виникає в самих різних областях – в сфері зв'язку, військової справі й системах безпеки країни, корпоративних інформаційних системах, системах моніторингу та управління, повсякденній діяльності людини.

Висококваліфіковані фахівці в сфері кібербезпеки повинні вміти захистити інформаційні ресурси мережі від найбільш поширених зовнішніх і внутрішніх атак, спрямованих на виведення з ладу серверів і знищення даних, від небажаного проникнення в локальні обчислювальні мережі через «діри» в ОС, від цілеспрямованого вторгнення в систему через інформаційно-комунікаційні мережі для отримання конфіденційної інформації тощо.

На заняттях курсу «Управління мережевою безпекою» студенти отримують теоретичні знання та практичні вміння в сфері управління мережевою безпекою, проектування, впровадження, безпечної експлуатації та супроводження інформаційно-комунікаційних мереж.

2. Мета та цілі курсу - формування комплексу знань щодо основ менеджменту інформаційної безпеки, набуття ЗВО теоретичних знань та практичних навичок щодо управління інформаційною безпекою в інформаційно-телекомунікаційних системах для реалізації встановленої політики безпеки, формування науково-професійного світогляду магістра спеціальності 125 – Кібербезпека в області використання цих технологій для захисту інформації під час її передачі інформаційно-комунікаційними мережами та в повсякденній професійній діяльності. Розкриття сучасних методів захисту інформації в комп'ютерних мережах і ознайомлення з особливостями їх апаратної та програмної реалізацій.

Під час вивчення дисципліни здобувач вищої освіти має набути або розширити наступні загальні та фахові компетентності, передбачені освітньою програмою:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 2. Здатність розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах (автоматизованих систем та їх додатків) та у інфраструктурі організації в цілому.

КФ 3. Здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, інфраструктури установи, архітектури використання інформаційних технологій (хмарних), а також бізнес/операційних процесів з метою якісного функціонування інформаційно-комунікаційних систем (комутативних або без комутативних), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

КФ 5. Здатність розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, а також систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

КФ 6. Здатність розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії.

Основними завданнями вивчення дисципліни “Управління мережевою безпекою” є:

– ознайомлення з вимогами до забезпечення інформаційної безпеки ІКМ, відповідними стандартами, технічними специфікаціями, протоколами і технологіями;

– формування умінь по створенню, налаштування і експлуатації захищених ІКМ;

– оволодіння навичками по використанню компонентів ІКМ, здатністю розробляти моделі загроз і моделі порушників ІБ ІКМ на основі вихідних даних про мережу;

– формування навичок забезпечення безпеки ІКМ, їх безпечного використання і протидію правопорушенням, пов’язаними із використанням ІКМ.

3. Результати навчання:

ПРН 2. Планувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН 6. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі у напрямах найкращих практик, технічних вимог та рекомендацій з управління інформаційною безпекою та /або кібербезпекою;

ПРН 7. Проектувати, впроваджувати, та супроводжувати інформаційно-комунікаційні системи, а також забезпечувати захист інформаційних ресурсів мереж (мережева безпека) та всієї інфраструктури установи на базі сучасних моделей, методів і засобів передачі даних в комутативних або без комутативних каналах зв’язку, хмарного простору, протоколів обміну даними, мережного устаткування, тощо;

ПРН 8. Проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту додатків (веб - додатків) з метою забезпечення

якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації;

ПРН 10. Розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно - апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації;

ПРН 12. Розробляти, впроваджувати та супроводжувати процеси належного функціонування системи моніторингу інформаційних ресурсів і бізнес процесів в інфраструктурі організації;

Після вивчення дисципліни «Управління мережевою безпекою» ЗВО повинні:

знати :

- існуючі мережеві протоколи, що необхідні для функціонування мережі;
- існуючи мережні стандарти та протоколи захищеної передачі даних;
- перспективи розвитку обчислювальних мереж;
- принципи організації безпечної взаємодії між прикладними програмами на різних комп'ютерах в локальних та глобальних мережах;
- планування адресного простору IP мереж та налаштування динамічної маршрутизації;
- організація системних мережних сервісів (DNS, XNTP, DHCP та ін.);
- організація та підтримка базових мережних сервісів (SMTP, HTTP, FTP та ін.);
- особливості сучасних комп'ютерних систем передачі даних.

вміти :

- робити вибір протоколів та мережевого обладнання, необхідного для забезпечення інформаційної безпеки;
- робити вибір методу доступу до каналу передачі даних;
- забезпечувати взаємодію комп'ютерів у мережному середовищі з врахуванням вимог безпеки;
- реалізувати управління мережевою безпекою засобами транспортного протоколу, протоколів автентифікації та конфіденційної передачі даних;
- аналізувати ефективність функціонування обчислювальної мережі;
- створювати віртуальні приватні мережі;
- створювати мережні сервіси автентифікації, авторизації та обліку.

4. Обсяг курсу. 4 кредити ECTS, що становить 120 годин роботи студентів, з них 80 годин самостійної роботи та 40 годин аудиторної роботи з викладачем.

Вид заняття	Загальна кількість годин
Лекції	22
Лабораторні заняття	18
Самостійна робота (РГР, наукові дослідження)	80

Тематика курсу

Змістовий модуль 1. Теоретичні основи управління мережевою безпекою

Тема 1. Основні поняття та базові принципи управління мережевою безпекою

Тема 2. Проблеми інформаційної безпеки мереж

Тема 3. Методи та засоби забезпечення мережевої безпеки

Тема 4. Управління мережевою безпекою на основі стеку протоколів

Тема 5. Методи управління засобами мережевої безпеки

Тема 6. Проблеми безпеки під час використання Інтернет

Змістовий модуль 2. Прикладні аспекти управління мережевою безпекою

Тема 7. Інструменти забезпечення мережевої безпеки сучасних операційних систем
Тема 8. Управління безпекою бездротових мереж
Тема 9. Особливості міжмережевого екранування
Тема 10. Побудова захищених віртуальних мереж VPN
Тема 11. Безпека віддаленого доступу до комп`ютерної мережі
Тема 12. Мережеві протоколи ідентифікації та автентифікації

5. Пререквізити. Передумовою для вивчення курсу «Управління мережевою безпекою» є успішне засвоєння дисциплін: інформатика, архітектура комп'ютерних систем, комп'ютерна схемотехніка, технології програмування, комп'ютерні мережі, основи криптографічного захисту інформації, методи побудови та аналізу криптосистем та ін. Дисципліна «Управління мережевою безпекою» є базовою для подальшої успішної професійної діяльності за спеціальністю, а також може використовуватися під час підготовки випускної кваліфікаційної роботи магістра.

6. Система оцінювання та вимоги

Загальна система оцінювання курсу	ECTS
Вимоги розрахунково-графічної роботи	При перевірці та оцінюванні розрахунково-графічної роботи враховується правильність виконання теоретичних та практичних завдань, самостійність виконання, вчасність здачі роботи та відповідність оформлення результатів діючим вимогам
Лабораторні заняття	Кожна виконана лабораторна робота оцінюється від 0 до 3-х балів. Кількість балів залежить від рівня теоретичних знань та практичних навичок студента за темою, самостійності виконання роботи та вчасності її захисту
Умови допуску до підсумкового контролю	Умовою допуску до екзамену є виконання та отримання хоча б мінімальної кількості балів з усіх обов'язкових видів навчальної роботи передбачених робочою програмою (лабораторних, модульного контролю та розрахунково-графічної роботи). Мінімальна кількість балів необхідна для допуску до екзамену – 20.

Діяльність ЗВО та форма контролю	**Кількість балів**	
Повнота ведення конспектів занять (присутність на лекції+конспект – 0,5 бала за кожну лекцію)	0	5
Якість виконання завдань до самостійної роботи. Рівень знань студента за темою самостійної роботи (максимум - 2 бали за кожне завдання)	0	8
Самостійність виконання завдання до самостійної роботи (максимум 0,5 бала)	0	2
Своєчасність виконання завдання до самостійної роботи (максимум 0,5 бала)	0	2
Підготовленість до лабораторних робіт. Рівень знань студента за темою	0	14

Діяльність ЗВО та форма контролю	Кількість балів	
лабораторної роботи (максимум - 1 бал за кожну лаб. роботу)		
Самостійність виконання лабораторних робіт (максимум 0,5 бала)	0	3,5
Своєчасність виконання лабораторних робіт (максимум 0,5 бала)	0	3,5
Модульний контроль	0	10
Оцінка за РГР	**0**	**12**
Семестрова оцінка поточного контролю	**0**	**60**
Екзамен	**0**	**40**

Шкала оцінювання: національна та ECTS

Критерії оцінювання	Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
			для екзамену, КСР, КП, ДР	для заліку
Студент виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили, проводить наукові дослідження	90 – 100	**A**	відмінно	зараховано
Студент вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв’язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна	82-89	**B**	добре	
Студент вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок	75-81	**C**		
Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал,	66-74	**D**	задовільно	

Критерії оцінювання	Сума балів за всі види	інка а ЄС	Оцінка за національною шкалою	
виправляти помилки, серед яких є значна кількість суттєвих				
Студент володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні	60-65	**E**		
Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу	0-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання

7. Політики курсу.

7.1 Академічна доброчесність – самостійність виконання навчальних завдань та посилання на джерела у випадку використання напрацювань інших авторів. Види порушень академічної доброчесності – академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво.

Відповідно до Положення про академічну доброчесність студентів та науково-педагогічних працівників Національного університету «Чернігівська політехніка» за порушення академічної доброчесності здобувачі освіти можуть мати наслідком: повторне проходження оцінювання (контрольна робота, іспит, залік тощо); повторне проходження відповідного освітнього компонента освітньої програми; відрахування із закладу освіти (крім осіб, які здобувають загальну середню освіту); позбавлення академічної стипендії; позбавлення наданих закладом освіти пільг з оплати навчання.

7.2 Політика дедлайнів – своєчасність здачі лабораторної роботи оцінюється в 0,5 бала за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 2 бали. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом).

7.3 Політика перезарахування кредитів у випадку мобільності – перезарахування відбувається якщо назви навчальних дисциплін ідентичні або мають незначну стилістичну відмінність, але обсяги та змістова частина навчальних програм не відрізняються; кількість кредитів, відведена на вивчення навчальної дисципліни відрізняється менше, ніж на 25 %; форми підсумкового контролю з дисциплін однакові. При перезарахуванні дисципліни зберігається раніше здобута позитивна оцінка. Перескладання іспиту з дисципліни з метою підвищення оцінки, визначеної в документах виданих здобувачу вищої освіти за попереднім місцем навчання, не дозволяється. Перезарахування кредитів проводиться відповідно Порядку визначення академічної різниці та перезарахування навчальних дисциплін при переведенні, поновлені, зарахуванні або академічній мобільності здобувача вищої освіти Національного університету «Чернігівська політехніка».

7.4 Політика щодо відвідування – відвідування занять є обов’язковим. При наявності поважних причин (хвороба, участь в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом) студенти можуть узгодити з викладачем індивідуальний графік навчання та здачі всіх видів навчальної роботи.

Студенти можуть перескладати або відпрацьовувати пропущені заняття на консультаціях викладача чи у спеціально відведений викладачем для цього час.

7.5 Політика щодо правил поведінки на заняттях – активна участь у навчальному процесі, виконання необхідного мінімуму навчальної роботи, коректна поведінка щодо інших учасників навчального процесу, взаємоповага, використання мобільних пристроїв тільки для навчання.

7.6 Політика заохочень та стягнень. Результати навчальної, наукової та організаційної діяльності студентів за напрямами курсу їм можуть нараховуватися додаткові бали - до 10 балів, в залежності від вагомості досягнень студента. Види позанавчальної діяльності, за які студенти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, статті на науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

8. Рекомендована література та інформаційні джерела

1. Cisco академія. [Електронний ресурс]. – Режим доступу: http://edu-cisco.org
2. Prometheus: Платформа масових відкритих онлайн-курсів [Електронний ресурс]. – Режим доступу: https://prometheus.org.ua
3. Рибальський О.В. Захист інформації в інформаційно-комунікаційних системах. Навчальний посібник для курсантів ВНЗ МВС України / О.В. Рибальський, В.Г. Хахановський, В.А. Кудінов, В.М. Смаглюк. – К.: Вид. Національної академії внутріш. справ, 2013. – 118 с.
4. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
5. Курило А.П. Аудит информационной безопасности / А.П.Курило, С.Л.Зефиров, В.Б.Голованов - М.: Издательская группа «БДЦ-пресс", 2006 — 304с.