СИЛАБУС ДИСЦИПЛІНИ «КОМП'ЮТЕРНІ МЕРЕЖІ ТА КІБЕРБЕЗПЕКА»

ДЛЯ ВИБІРКОВОЇ СКЛАДОВОЇ ОСВІТНІХ ПРОГРАМ ПІДГОТОВКИ БАКАЛАВРІВ
ДЛЯ ВИБІРКОВОЇ СКЛАДОВОЇ ОСВІТНІХ ПРОГРАМ ПІДГОТОВКИ БАКАЛАВРІВ

Рік навчання 4, семестр 7
Форма навчання денна
Кількість кредитів ЄКТС 4
Мова викладання українська

Лектор курсу	**Комар Катерина Вячеславівна, ст. викладач**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки, корпус. 15, к. 207, тел. 0445278724**
Сторінка курсу в eLearn	**ЕНК (7 семестр)**

ОПИС ДИСЦИПЛІНИ

Навчальна дисципліна передбачає вивчення основних принципів побудови та функціонування комп'ютерних мереж, а також сучасних методів і засобів кібербезпеки. Отримання студентами необхідних базових знань і практичних навичок з проектування, розгортання та адміністрування мережевих інфраструктур. Зокрема, курс охоплює питання захисту даних, методів виявлення та реагування на кіберзагрози, а також організації комплексного захисту інформаційних систем.

Навчальна дисципліна забезпечує формування ряду фахових компетентностей:

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 8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові, предметні) компетентності (СК):

СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних мереж і моделей інформаційної безпеки та/або кібербезпеки.
СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) мережах.
СК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).
СК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
СК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
СК13. Здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем захисту інформації.

У результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме:
ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
ПРН10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних мереж.
ПРН11. Виконувати аналіз зв'язків між серверами на віддалених обчислювальних системах.
ПРН13. Аналізувати проекти інформаційно-телекомунікаційних мереж, базуючись на стандартизованих технологіях та протоколах передачі даних.
ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних мережах.
ПРН21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
ПРН25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
ПРН28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
ПРН35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН36. Виявляти небезпечні сигнали технічних засобів.
ПРН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних мереж відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

ПРН50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

Зробимо курс корисним для вас. Якщо ви будете наполегливо працювати і докладати особливих зусиль, щоб не відставати від матеріалу, ви отримаєте винагороду – як в короткостроковій перспективі, так і в набутті фахових компетентностей. Будь-ласка, широко використовуйте аудиторні заняття, відеоінструкції, вебінари, щоб переконатися, що рухаєтесь за графіком навчання.

СТРУКТУРА КУРСУ

Тема	**Години** (лекції/ лаборато -рні,)	Результати навчання	Завдання	Оціню-вання
7 семестр				
Змістовний модуль 1. Основи комп'ютерних мереж				
Тема 1. Вступ. Основи безпеки в комп'ютерних мережах.	**2/2**	Вміти: - Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. - Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних. - Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. - Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. - Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. - Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.	1. Підготовка до лабораторної роботи. 2. Виконання лабораторної роботи. 3. Захист звітів з лабораторної роботи.	**10**
Тема 2. Мережі та їх характеристики. Мережеве обладнання.	**2/2**			**10**
Тема 3. Мережеві стандарти	**2/2**			**10**
Тема 4. Апаратне забезпечення комп'ютерних мереж.	**2/2**			**10**
Тема 5. Організація мереж та еталонна модель OSI.	**2/2**			**15**
Тема 6. Принципи побудови глобальних комп'ютерних мереж.	**2/2**			**15**
Тема 7. Ієрархічний дизайн мережі. Хмара та віртуалізація.	**2/2**			**15**
Тема 8. Мережеві протоколи. Протокол TCP/IP.	**2/2**			**15**
Змістовний модуль 2. Основи кібербезпеки				
Тема 1. Актуальність та основи кібербезпеки	**2/2**	- Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. - Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з	1. Підготовка до лабораторної роботи. 2. Виконання лабораторної роботи. 3. Захист звітів з лабораторної роботи.	**15**
Тема 2. Захист даних і конфіденційність.	**2/2**			**15**
Тема 3. Типи загрози кібербезпеки. Вразливості та атаки.	**2/2**			**15**

Тема 4. Мережеві атаки та захист від них.	**2/2**	використанням процедур резервування згідно встановленої політики безпеки. - Виявляти небезпечні сигнали технічних засобів. - Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІС відповідно до вимог нормативних документів системи технічного захисту інформації. - Використовувати інструментарій для моніторингу процесів в інформаційних системах.		**15**
Тема 5. Інфраструктура безпеки. Пристрої безпеки	**2/2**			**15**
Тема 6. Політики безпеки, правила та стандарти кібербезпеки.	**2/2**			**15**
Тема 7. Системи захисту інформації	**2/2**			**10**
Всього за семестр				**0,7*(100+ 100)/2 = 70**
Екзамен			**Тест, теоретичні питання, задача**	**30**
Всього за курс				**100**

ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів та перескладання:	Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний, стажування або відрядження).
Політика щодо академічної доброчесності:	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).
Політика щодо відвідування:	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету).

ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл.1 «Положення про екзамени та заліки у НУБіП України» (наказ про уведення в дію від 27.12.2019 р. № 1371):

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзаменів	**Заліків**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано