СИЛАБУС ДИСЦИПЛІНИ
«БЕЗПЕКА ТА АУДИТ БЕЗПРОВОДОВИХ ТА РУХОМИХ МЕРЕЖ»

Ступінь вищої освіти – Бакалавр
Спеціальність 125 – КІБЕРБЕЗПЕКА
Освітня програма «Кібербезпека»
Рік навчання 3, семестр 5
Форма навчання денна
Кількість кредитів ЄКТС 5
Мова викладання українська

Лектор курсу	 **Нікітенко Євгеній Васильович, к.ф.-м.н., доцент (портфоліо)**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки корпус. 15, к. 207, тел. 5278724 e-mail ev.nikitenko@nubip.edu.ua**
Сторінка курсу в eLearn	**ЕНК (5 семестр)**

ОПИС ДИСЦИПЛІНИ

Мета навчальної дисципліни «Безпека та аудит безпроводових та рухомих мереж» – формування у здобувачів уміння розв'язувати задачі адміністрування безпроводових і мобільних мереж і систем, застосовувати нормативно-правові, організаційні та технічні процедури при роботі безпроводових і мобільних технологій.

Навчальна дисципліна забезпечує формування ряду загальних компетентностей:

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.

У результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме

ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

ПРН 28. 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.

ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

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/ практичні)	Результати навчання	Завдання	Оцінювання
Модуль 1. Загрози для безпроводових технологій і їх аналіз.				
Кіберпростір і кібербезпека — головні ознаки нової інформаційної цивілізації. Заходи України із забезпечення кібербезпеки національної інфосфери та протидії проявам кіберзлочинності.	**3/3**	Вміти відшукувати, збирати або добувати інформацію про IT-системи й мережі протиборчих сторін, а також про технології та засоби їхнього впливу на власну інфосферу. Вміти виявляти ознаки стороннього кібервпливу й моделювати можливі ситуації такого впливу, прогнозуючи відповідні наслідки. Вміти протидіяти несанкціонованому проникненню протиборчих сторін у власні IT-системи й мережі, забезпечуючи стійкість їхньої роботи, а також відновлення нормального функціонування після здійснення кібернападів тощо.	Теоретичне опитування.	**20**
Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози.	**3/3**		Здача лабораторної роботи.	**20**
Кібератаки та кібертероризм: поняття і визначення. Особливості реалізації атак і заходи з послаблення їхнього деструктивного впливу. Тип атак: зовнішні, апаратні, маскувальні. Злоякісні програмні коди.	**4/4**		Здача лабораторної роботи. Неформальна on-line освіта на основі МВОК.	**20** **20**
Модульний контроль			Підсумковий тест в ЕНК	**20**
Модуль 2. Атаки на комерційні безпроводові протоколи.				
Бездротові мережі загрози моделей. Бездротовий збір даних та WiFi. MAC-аналіз. Бездротові засоби інформаційного аналізу	**4/4**	Вміти відшукувати, збирати або добувати інформацію про IT-системи й мережі протиборчих сторін, а також про технології та засоби їхнього впливу на власну інфосферу. Вміти виявляти ознаки стороннього кібервпливу й моделювати можливі ситуації такого впливу,	Здача лабораторної роботи. Опитування	**10** **10**
Атаки на Bluetooth, DECT і ZigBee.	**3/3**		Здача лабораторної роботи. Опитування	**20** **15**

Розширені методики атак WiFi.	**3/3**	прогнозуючи відповідні наслідки. Вміти протидіяти несанкціонованому проникненню протиборчих сторін у власні ІТ-системи й мережі, забезпечуючи стійкість їхньої роботи, а також відновлення нормального функціонування після здійснення кібернападів тощо.	Здача лабораторної роботи. Неформальна on-line освіта на основі МВОК.	**15** **10**
Модульний контроль			Підсумковий тест в ЕНК	**20**
Модуль 3. Захист інформації в системах мобільного зв'язку.				
Засоби захисту в сучасних системах мобільного зв'язку. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки. Загрози соціального інжинірингу. Загрози з використанням електронної пошти (e-mail). Загрози при використанні телефонного зв'язку.	**4/4**	Вміти відшукувати, збирати або добувати інформацію про ІТ-системи й мережі протиборчих сторін, а також про технології та засоби їхнього впливу на власну інфосферу. Вміти виявляти ознаки стороннього кібервпливу й моделювати можливі ситуації такого впливу, прогнозуючи відповідні наслідки.	Здача лабораторної роботи.	**10**
Соціальні мережі: особливості, основні поняття та визначення. Моніторинг соціальних мереж — цілі та способи реалізації.	**3/3**		Здача лабораторної роботи. Опитування	**10** **15**
Поняття соціотехнічної системи та її властивостей. Системний підхід як загальнометодологічний принцип створення складних соціотехнічних систем.	**3/3**	Вміти протидіяти несанкціонованому проникненню протиборчих сторін у власні ІТ-системи й мережі, забезпечуючи стійкість їхньої роботи, а також відновлення нормального функціонування після здійснення кібернападів тощо.	Здача лабораторної роботи. Неформальна on-line освіта на основі МВОК. Опитування	**20** **15** **10**
Модульний контроль			Підсумковий тест в ЕНК	**20**
Всього за семестр				**70**
Екзамен			**Тест, теоретичні питання, задача**	**30**
Всього за курс				**100**

ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів та перескладання:	Дедлайни визначені в ЕНК. 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

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