СИЛАБУС ДИСЦИПЛІНИ «ОСНОВИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

Ступінь вищої освіти – Бакалавр
Спеціальність 125 – КІБЕРБЕЗПЕКА
Освітня програма «Кібербезпека»
Рік навчання 2, семестр 4
Форма навчання денна
Кількість кредитів ЄКТС 4
Мова викладання українська

Лектор курсу	 **Кулініч Олег Миколайович, к.т.н., доцент.**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки, корпус. 15, к. 207, тел. 0445278724** **e-mail o.kulinich@nubi.edu.ua**
Сторінка курсу в eLearn	**ЕНК (4 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=4162

ОПИС ДИСЦИПЛІНИ

Навчальна дисципліна передбачає засвоєння студентами сучасних методів захисту інформації, отримання студентами необхідних базових знань, щодо порядку створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. В рамках курсу передбачено проведення теоретичних та практичних завдань щодо класифікації, шляхів утворення технічних каналів витоку інформації, а також сучасних методів та засобів технічного захисту інформації..

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.

Спеціальні (фахові, предметні) компетентності (СК):

СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

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.).

СК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

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

ПРН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН17. 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.

ПРН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

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).

ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

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 систем відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

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

ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

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/ лабораторні,)	Результати навчання	Завдання	Оцінювання
1 семестр				
Модуль 1. Сутність технічного захисту інформації.				
Тема 1. Загальні аспекти технічного захисту інформації	**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. - Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).	1. Підготовка до лабораторної роботи. 2. Виконання лабораторної роботи. 3. Захист звітів з лабораторної роботи.	**5**
Тема 2. Загальні положення та вимоги щодо розміщення режимних приміщень.	**2/2**			
Тема 3. Технічні канали витоку інформації та їх класифікація (ч.1).	**2/-**			**5**
Тема 4. Технічні канали витоку інформації та їх класифікація (ч.2).	**2/2**			
Тема 5. Сутність та шляхи утворення технічних каналів витоку інформації – електромагнітні, електричні, параметричні	**2/2**			**5**
Тема 6. Сутність та шляхи утворення технічних каналів витоку інформації – акустичні, акусто-вібраційні, акусто-електричні, акусто-оптичні.	**2/2**			**5**
Тема 7. Сутність та шляхи утворення технічних каналів витоку інформації – матеріально-речовинні, канали зв'язку, візуальної інформації.	**2/-**			**5**
Тема 8. Сутність та класифікація засобів несанкціонованого перехоплення інформації.	**2/4**			
Модульна контрольна робота				**10**
Модуль 2. Механізми технічного захисту інформації на об'єктах інформаційної діяльності.				
Тема 1. Основні положення та сутність створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності.	**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	**5**

		використанням процедур резервування згідно встановленої політики безпеки. - Виявляти небезпечні сигнали технічних засобів. - 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. - Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. - Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. - Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). - Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. - Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.	лабораторної роботи.	
Тема 2. Передпроектні роботи при створенні комплексів технічного захисту інформації на об'єктах інформаційної діяльності.	**2/4**			**5**
Тема 3. Розроблення технічного проекту комплексу технічного захисту інформації	**2/4**			**5**
Тема 4. Сутність та оформлення моделі загроз при створенні комплексу технічного захисту інформації.	**2/-**			
Тема 5. Розробка та впровадження заходів з технічного захисту інформації на об'єктах інформаційної діяльності.	**2/2**			**5**
Тема 6. Порядок проведення атестації комплексів технічного захисту інформації.	**2/2**			**5**
Тема 7. Фізична безпека інформаційних систем та об'єктів інформаційної діяльності.	**2/-**			
Модульна контрольна робота				**10**
Всього за семестр				**10*5+2*10= = 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 «26» квітня 2023 р. протокол № 10):

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