СИЛАБУС ДИСЦИПЛІНИ «ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ»

Ступінь вищої освіти – бакалавр
Спеціальність 123 – Комп'ютерна інженерія
Освітня програма «Комп'ютерна інженерія»
Рік навчання 4, семестр 8
Форма навчання денна
Кількість кредитів ЄКТС 4
Мова викладання українська

Лектор курсу	 **Лахно Валерій Анатолійович, д.т.н., професор (портфоліо)**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки корпус. 15, к. 207, тел. 0445278724 e-mail lva964@nubip.edu.ua**
Сторінка курсу в eLearn	**ЕНК (8 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=2773

ОПИС ДИСЦИПЛІНИ

Завдання навчальної дисципліни «Захист інформації в комп'ютерних системах» - є теоретична та практична підготовка здобувачів до розробки та застосування сучасних програмно-апаратних систем захисту інформації в різних установах та на підприємствах, зокрема АПК.

Місце і роль дисципліни в системі підготовки фахівців відповідно до навчального плану. Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області комп'ютерної інженерії та захисту інформації.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 123 «Комп'ютерна інженерія» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

ЗК1. Здатність до абстрактного і системного мислення, аналізу та синтезу.

ЗК2. Здатність вчитися і оволодівати сучасними знаннями.

ЗК3. Здатність застосовувати знання у практичних ситуаціях.

ЗК6. Навички міжособистісної взаємодії.

Фахові компетентності:

СК4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

СК5. Здатність використовувати засоби і системи автоматизації проектування до розроблення компонентів комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем тощо.

СК13. Здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій.

СК10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

СК14. Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію.

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

ПРН1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

ПРН2. Мати навички проведення експериментів, збирання даних та моделювання в комп'ютерних системах.

ПРН7. Вміти застосовувати знання для розв'язування задач аналізу та синтезу засобів, характерних для спеціальності.

ПРН13. Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.

ПРН 15. Вміти виконувати експериментальні дослідження за професійною тематикою.

ПРН 16. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.

ПРН 21. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

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/ Лабо-рато-рні,)	Результати навчання	Завдання	Оціню-вання
8 семестр				
Модуль 1. Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки. Основні поняття політики інформаційної безпеки та захисту інформації.				
Властивості інформації з точки зору проблематики її захисту.	**2/0**	Вміти застосовувати теорії, методи та засоби захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.	Опитування.	-
Ризики порушення політики інформаційної безпеки об'єкту інформатизації.	**2/4**	Вміти здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.	Захист лабораторної роботи.	**10**
Вимоги щодо безпеки системи, ризики безпеки.	**2/4**	Вміти вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.	Захист лабораторної роботи.	**10**
Механізми реалізації послуг безпеки.	**2/0**	Вміти застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.	Опитування.	**2**
Поняття загрози інформації.	**2/0**	Вміти здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.	Опитування.	**2**
Політика інформаційної безпеки	**2/0**	Вміти вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).	Опитування.	**2**
Аналіз моделей безпеки ІКС.	**2/4**	Вміти забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних)	Захист лабораторної роботи.	**10**

		схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.		
Загальні моделі ІБ.	**2/0**	Вміти 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.	Опитування.	**2**
Аналіз безпеки програмного забезпечення.	**2/4**	Вміти вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень	Захист лабораторної роботи.	**10**
Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	**2/4**	Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.	Захист лабораторної роботи.	**10**
Політики резервного копіювання даних.	**2/4**	Вміти вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.	Захист лабораторної роботи.	**10**
Механізми безпеки комп'ютерних мереж.	**2/0**	Вміти 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.	Опитування.	**2**
Модульний контроль			Підсумковий тест в ЕНК.	**30**
Модуль 2. Моделювання та аналіз безпеки об'єктів захисту інформації.				
Модель архітектури безпеки ІКС.	**2/4**	Вміти 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.	Захист лабораторної роботи.	**10**
Методи захисту інформації в ІКС.	**2/0**	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.	Опитування.	**-**
Джерела інформації про події та типи	**2/0**	Вміти забезпечувати введення підзвітності системи управління доступом до	Опитування.	**2**

подій, що аналізуються в системах моніторінгу. Система візуалізації та управління подіями (SIEM).		електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.		
Концептуальна схема оцінки ІБ. Кількісна та якісна оцінки ІБ.	**2/0**	Вміти 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.	Опитування.	**2**
Виявлення технічних каналів витоку інформації.	**2/4**	Вміти 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.	Захист лабораторної роботи.	**10**
Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами.	**2/4**	Вміти 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.	Захист лабораторної роботи.	**10**
Управління кіберінцидентами (зокрема, на прикладі підприємств АПК).	**2/4**	Вміти впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.	Захист лабораторної роботи.	**10**
Розслідування кіберінцидентів / кібератак (зокрема, на прикладі підприємств АПК).	**2/4**	Вміти забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.	Захист лабораторної роботи.	**10**
Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ.	**2/0**	Вміти впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної, і/або кібербезпеки, застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.	Опитування.	**2**
Вибір методів та засобів забезпечення необхідного рівня ІБ (зокрема, на прикладі підприємств АПК).	**2/4**	Вміти 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.	Захист лабораторної роботи.	**10**
IDS.	**2/0**	Вміти впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної, і/або кібербезпеки.	Опитування.	**2**
IPS.	**2/0**	Вміти впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної, і/або кібербезпеки.	Опитування.	**2**
Модульний контроль			Підсумковий тест в ЕНК.	**30**

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