СИЛАБУС ДИСЦИПЛІНИ «ПРИКЛАДНІ АСПЕКТИ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ»

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	 **Мамченко Сергій Миколайович, д.пед.н., професор (**https://docs.google.com/document/d/11yav3OQ1-Fja6hRolTrFYXjGd6mzbL8S/edit?usp=share_link&ouid=117030542413268962483&rtpof=true&sd=true**)**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки корпус. 15, к. 207, тел. 0445278724 e-mail s.mamchenko@nubip.edu.ua**
Сторінка курсу в eLearn	**ЕНК (4 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=3403

ОПИС ДИСЦИПЛІНИ

Мета навчальної дисципліни “Прикладні аспекти побудови системи захисту інформації” є навчання студентів принципам побудови комплексних систем захисту інформації на основі синтезу організаційних і технічних заходів щодо забезпечення захисту інформації з обмеженим доступом, основ ведення електронного документообігу в умовах сучасних кіберзагроз та витоку технічними каналами, забезпечення захисту інформації від несанкціонованого доступу на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології 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.

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

Спеціальні (фахові, предметні) компетентності (СК):

СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

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.

СК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

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

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;

ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

ПРН 17. 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;

ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) 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
4 семестр				
Модуль 1. Порядок проведення робіт із створення комплексної системи захисту інформації підприємства АПК.				
Тема 1. Організаційні, технічні та програмно-апаратні засоби комплексної системи захисту корпоративної інформації.	**2/2**	- Вміти критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. - Вміти виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем підприємств АПК. - Вміти виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. - Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та	1. Підготовка до лабораторної роботи. 2. Виконання лабораторної роботи. 3. Захист звітів з лабораторної роботи.	**10**
Тема 2. Автоматизовані системи АПК.	**2/2**			**10**
Тема 3. Формування загальних вимог до	**2/2**			**15**

КСЗІ в ІТС АПК.		протоколах передачі даних.		
Тема 4. Оцінка загроз та джерел загроз безпеці інформації, що циркулює на об'єкті інформаційної діяльності в АПК .	**2/2**	- Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. - Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах підприємств АПК.. - 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 підприємств АПК. - 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). - 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. - Виявляти небезпечні сигнали технічних засобів. - Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.		**15**
Тема 5. Сутність моделі порушника інформаційної безпеки в ІТС підприємств АПК.	**2/2**			**15**
Тема 6. Вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій, які регламентують використання захищених технологій обробки інформації в ІТС.	**2/2**			**15**
Тема 7. Визначення вимог із захисту оброблюваної в ІТС інформації.	**2/2**			**10**
Тема 8. Обґрунтування і прийняття проектних рішень, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ.	**2/2**			**10**
Модуль 2. Визначення відповідності комплексної системи захисту інформації технічному завданню.				
Тема 1. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС	**2/2**	- 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. - Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. - Вирішувати задачі забезпечення та супроводу комплексних систем захисту	1. Підготовка до лабораторної роботи. 2. Виконання лабораторної роботи. 3. Захист звітів з лабораторної роботи.	**15**
Тема 2. Захист інформації WEB-сторінки від НСД.	**2/2**			**15**
Тема 3. Розробка програми та методики державної експертизи комплексної системи захисту інформації.	**2/2**			**15**
Тема 4. Етапи	**2/2**			**15**

проведення експертизи комплексної системи захисту інформації.		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. - 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. - Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). - Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.		
Тема 5. Декларація про відповідність, порядок розробки та відмінності в застосуванні.	**2/2**			**10**
Тема 6. Порядок створення та впровадження організаційно-технічного рішення на комплексну систему захисту інформації.	**2/2**			**15**
Тема 7. Організація служби захисту інформації (СЗІ) та організаційне проектування діяльності СЗІ.	**2/2**			**15**
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:	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

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