СИЛАБУС ДИСЦИПЛІНИ
«ОСНОВИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Ступінь вищої освіти – бакалавр
Спеціальність 125 – Кібербезпека
Освітня програма «Кібербезпека»
Рік навчання 4, семестр 7
Форма навчання денна
Кількість кредитів ЄКТС 4
Мова викладання українська

Лектор курсу	 **Мамченко Сергій Миколайович, д.пед.н., професор (портфоліо)**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки корпус. 15, к. 207, тел. 044-527-8724 e-mail s.mamchenko@nubip.edu.ua**
Сторінка курсу в eLearn	**ЕНК (8 семестр)**

ОПИС ДИСЦИПЛІНИ

Курс має навчити майбутніх спеціалістів навчитися відповідати вимогам інформаційної безпеки - це комплексний, циклічний процес, який складається з наступних етапів: - планування аудиту; - планування заходів по аудиту (розробка, узгодження і затвердження планів заходів); - перевірка на відповідність групі вимог (наприклад, на відповідність стандарту ISO/IEC 27001: 2013); - систематизація результатів обстеження і формування звітності.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

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

Спеціальні (фахові) компетентності:

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.

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

СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

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.

В 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 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/ Лабораторні,)	Результати навчання	Завдання	Оціню-вання
1 семестр				
Модуль 1. Моніторинг мережевої безпеки.				
Тема №1. Системи аудиту інформаційної безпеки.	**2/0**	ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.	Опитування.	**-**
Тема №2. Системи менеджменту інформаційної безпеки (СМІБ) за вимогами ISO/IEC 27001.	**2/4**		Захист лабораторної роботи.	**10**
Тема №3. Стандарт CobiT 4.1.	**2/4**		Захист лабораторної роботи.	**10**
Тема №4. Стандарт ISO/IEC 15408. Серія стандартів ISO/IEC 2700X.	**2/2**		Опитування.	**2**
Тема №5. Комплексний аудит інформаційної безпеки Компетентність особи, що здійснює управління програмою аудиту.	**2/2**		Опитування.	**2**
Тема №6. Оцінка діяльності з управління інформаційною безпекою організації.	**2/2**			
Модульний контроль			Підсумковий тест в ЕНК.	**30**
Модуль 2. Практичне застосування систем моніторингу загроз та атак.				
Тема № 7. Базові принципи, терміни та визначення системи менеджменту	**2/2**	ПРН 49. Забезпечувати належне функціонування системи моніторингу	Захист лабораторної роботи.	**10**

інцидентами інформаційної безпеки (СМІІБ).		інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.		
Тема №8. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035.	**2/0**		Опитування.	**-**
Тема № 9. Особливості менеджменту інцидентів відповідно до ITIL.	**2/6**		Опитування.	**2**
Тема № 10. Концепція та структура автоматизованої системи управління інцидентами ІБ.	**4/2**		Опитування.	**2**
Тема № 11. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.	**4/4**		Опитування.	**2**
Тема № 12. Обробка інцидентів інформаційної безпеки групами CERT/CSIRT. Документаційне забезпечення процесу управління інцидентами інформаційної безпеки.	**4/2**		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