СИЛАБУС ДИСЦИПЛІНИ
«Державні та міжнародні вимоги з кібербезпеки»

Ступінь вищої освіти – бакалавр
Спеціальність 125 – Кібербезпека
Освітня програма «Кібербезпека»
Рік навчання 3, семестр 6
Форма навчання денна
Кількість кредитів ЄКТС 5
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 (6 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=5418

ОПИС ДИСЦИПЛІНИ

Мета дисципліни “Державні та міжнародні вимоги з кібербезпеки” полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для: визначення місця і ролі кібербезпеки в загальній системі національної безпеки; стану та принципів її забезпечення, необхідних для подальшої професійної діяльності; застосування політик, методів та засобів ефективного й безпекового поводження у кіберпросторі в умовах широкого використання сучасних інформаційних технологій.

Дисципліна «Державні та міжнародні вимоги з кібербезпеки**»** взаємопов’язана з такими дисциплінами, як «Комплексні системи захисту інформації», «Організаційне забезпечення захисту інформації» та «Безпека інформації в інформаційно-комунікаційних системах»**.**

Набуття компетентностей:

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

Загальні компетентності:

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Знання та розуміння предметної області та розуміння професії.

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.

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

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

ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

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 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

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**
6 семестр				
Модуль 1. Стандарти кібербезпеки.				
Тема 1. Характеристика стандартів із забезпечення кібербезпеки.	**2/2**	ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; 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 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.	Захист практичної роботи.	**15**
Тема 2. Міжнародний стандарт з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).	**4/4**		Захист практичної роботи.	**15**
Тема 3. Стандарт ISO/IEC 27002 «Інформаційні технології - Методики безпеки - Практичні правила управління безпекою інформації».	**4/4**		Захист практичної роботи.	**15**
Тема 4. Міжнародний стандарт безпеки ISO/IEC 17799.	**4/4**		Захист практичної роботи. Опитування.	**15** **10**
Модульний контроль			Підсумковий тест в ЕНК.	**30**

Модуль 2. Нормативно-правове забезпечення кібербезпеки в зарубіжних країнах та Україні.				
Тема 5. Порівняння підходів за ISO 17799 і BSI.	**4/4**	ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; 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 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.	Захист практичної роботи.	**15**
Тема 6. Інформаційна безпека як об'єкт правовідносин.	**4/4**		Захист практичної роботи.	**15**
Тема 7. Поняття кібербезпеки, кіберзлочинності та кібертероризму в різних країнах.	**4/4**		Захист практичної роботи.	**15**
Тема 8. Основна правова база забезпечення інформаційної та кібернетичної безпеки в Україні.	**4/4**		Захист практичної роботи.	**15**
			Опитування.	**10**
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