СИЛАБУС ДИСЦИПЛІНИ «СТАНДАРТИ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ»

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	**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 (6 семестр)** https://elearn.nubip.edu.ua/course/

ОПИС ДИСЦИПЛІНИ

Мета дисципліни “Стандарти інформаційної та кібернетичної безпеки” полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для визначення місця і ролі кібербезпеки в загальній системі національної безпеки, стану та принципів забезпечення інформаційної безпеки особистості, суспільства та держави, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів ефективного та безпекового поводження з інформацією незалежно від її походження та виду в умовах широкого використання сучасних інформаційних технологій.

Дисципліна «Стандарти інформаційної та кібернетичної безпеки» взаємопов’язана з такими дисциплінами, як «Комплексні системи захисту інформації» та «Організаційне забезпечення захисту інформації».

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;	Захист практичної роботи.	**15**
Тема 2. Міжнародний стандарт з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).	**4/4**	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 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	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**	міжнародних в галузі інформаційної та /або кібербезпеки; ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;	Захист практичної роботи.	**15**
Тема 8. Основна правова база забезпечення інформаційної та кібернетичної безпеки в Україні.	**4/4**	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**
			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

Рекомендовані джерела інформації

Базові

1. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017 // Офіційний вісник Президента України. – 2017. – № 5. – С. 15. – Ст. 102.

2. Довгань О.Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: монографія; НАПрН України, НДІІП, НАН України, Нац. б-ка ім. В.І. Вернадського. – Київ, 2015. – 388 с.

3. Інформаційна безпека держави : підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.] ; в 2 т. – Т.1. / за аг. ред.. В.В. Остроухова. – К. : ДНУ «Книжкова палата Україна», 2016. – 264 с.

4. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 р. № 96/2016// Офіційний вісник України. – 2016. – № 23. – С. 69. – Ст. 899.

5. Стратегія національної безпеки України : Указ Президента України від 06.05.2015 р. № 287/2015// Офіційний вісник України. – 2015. – № 43. – С. 14. – Ст. 1353.

6. Воєнна доктрина України: Указ Президента України від 24.09.2015 р. №555/2015 // Офіційний вісник України. – 2015. – № 78. – С. 38. – Ст. 2592.

7. Законодавчі основи забезпечення інформаційної безпеки України: наукова доповідь / Пилипчук В.Г., Корж І.Ф., Петришин О.В., Савінова Н.А., Фурашев В.М. (За заг. ред. Пилипчука В.Г.) – К: НДІІП НАПрН України, 2014. – 60 с.

8. Конституція України : Закон України від 28.06.96 р. № 254к/96-ВР // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – Ст. 141.

9. Концепція розвитку сектору безпеки і оборони України : Указ Президента України від 14.03.2016 р. № 92/2016 // Офіційний вісник України. – 2016. – № 23. – С. 12. – Ст. 898.

10. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори:проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. – 449 с.

11. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. – Житомир: ЖНАЕУ, 2016. – 636 с.

12. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л.Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка.— К.: ДУТ, 2015.— 288 с.

Допоміжні

1. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ЦП «Компринт» О.В., 2020. – 444 с.

2. Параметри оцінки ефективності інформаційного права / П.В. Кіндрат // Право і суспільство. – 2016. – № 5. – С. 102–107. ISSN 2078–3736

3. Правові засади та пріоритети розвитку протидії негативним інформаційним впливам на дітей / О. Г. Радзієвська // Інформація і право. – 2017. – № 2(21)/2017. – С. 88-98.

4. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

5. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. (ISO/IEC 27002:2013; Cor 1:2014, IDT).

Інформаційні ресурси

1. АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=81998&cat_id=38835

Нормативна література

1. ДСТУ ISO/IEC 11770-3:2002 «Інформаційні технології. Методи захисту».

2. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

3. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.