СИЛАБУС ДИСЦИПЛІНИ
«Інформаційна безпека держави»

Ступінь вищої освіти - Бакалавр
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»
Рік навчання 1 семестр 2
Форма навчання денна
Кількість кредитів ЄКТС 4
Мова викладання українська

Лектор курсу	 **Касаткін Дмитро Юрійович, к.пед.н., доцент (Портфоліо НПП)**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки, корпус. 15, к. 207, тел. 5278199 e-mail d.kasatkin@nubip.edu.ua**
Сторінка курсу в eLearn	**ЕНК (2 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=2097

ОПИС ДИСЦИПЛІНИ

В курсі студенти знайомляться з поняттями інформаційна безпеки, як з однією із суттєвих складових частин національної безпеки країни. У сфері інформаційної безпеки знання (в будь-якій формі їх подання) виступають, з одного боку, як об'єкт безпосереднього захисту, а з другого – як фактор забезпечення інтересів людини, суспільства та країни у будь-якій сфері їх життєдіяльності на інформаційному рівні. Під методологічними засадами інформаційної безпеки розуміємо єдність концептуальних, теоретичних і технологічних основ забезпечення на інформаційному рівні безпеки всіх сфер державної і суспільної діяльності (політичної, економічної, соціальної, воєнної, екологічної, духовної та ін.), а також сфер формування, обігу, накопичення і використання інформації (інформаційний простір, інформаційні ресурси, інформаційно-аналітичне забезпечення органів державного управління у всіх різновидах діяльності тощо). Предметом методології інформаційної безпеки є дослідження способів, методів, засобів і каналів реалізації загроз національним інтересам на інформаційному рівні та їх своєчасного виявлення, запобігання і нейтралізації. Метою вивчення навчальної дисципліни «Інформаційна безпека держави» є формування знань про теоретичні основи інформаційної безпеки, особливості забезпечення інформаційної безпеки держави, правила відношення інформації до державної таємниці, конфіденційної інформації, що є власністю держави, недержавної конфіденційної і відкритої інформації що потребує захисту, шляхи побудови систем забезпечення інформаційної безпеки.

Навчальна дисципліна забезпечує формування ряду загальних 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 5. Здатність до пошуку, оброблення та аналізу інформації.

КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної

області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові) компетентності:

СК 1. 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.

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.

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
2 семестр				
Модуль 1. Основні поняття та визначення інформаційної безпеки держави				
Аналіз стану інформаційного простору та інформаційної безпеки держави.	2/1	Вміти 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. Вміти діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. Вміти готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.	Виконання та захист лабораторних робіт. Неформальна on-line освіта на основі Cisco.	**6**
Джерела загроз інформаційній безпеці.	1/2		Виконання та захист лабораторних робіт. Самостійне вивчення онлайн курсу Cisco-Cybersecurity.	**7**
Сутність інформаційної безпеки держави, суспільства та особи.	2/1		Виконання та захист лабораторних робіт. Самостійне вивчення онлайн курсу Cisco-Cybersecurity	**7**
Основи інформаційного протиборства.	2/2		Виконання та захист лабораторних робіт. Самостійне вивчення онлайн курсу Cisco-Cybersecurity.	**7**
Модуль 2. Загрози національній безпеці держави та боротьба з ними в інформаційній сфері				
Основні загрози національній безпеці держави в інформаційній сфері.	2/3	Вміти 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.	Виконання та захист лабораторних робіт	**6**
Стратегічні цілі та завдання інформаційної боротьби.	2/3		Виконання та захист лабораторних робіт.	**7**
Державне управління інформаційною безпекою.	2/3		Виконання та захист лабораторних робіт.	**7**

Національний інформаційний простір.	2/3	Вміти діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. Вміти готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.	Виконання та захист лабораторних робіт. Неформальна on-line освіта на основі Cisco.	**7**
Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності.	1/3		Виконання та захист лаб. робіт. Неформальна on-line освіта на основі Cisco.	**7**
Модульний контроль (1-2 модулі)			тест в системі E-Learn	**30**
Модуль 3. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності				
Свобода слова та інформаційна безпека	2/3	Вміти впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. Вміти застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.	Виконання та захист лабораторних робіт. Неформальна on-line освіта на основі Cisco.	**6**
Основи державної політики в сфері інформаційної безпеки України	2/3		Виконання та захист лабораторних робіт. Самостійне вивчення онлайн курсу Cisco-Cybersecurity.	**7**
Досвід забезпечення інформаційної безпеки в державах ЄС, США	2/3		Виконання та захист лабораторних робіт. Самостійне вивчення онлайн курсу Cisco-Cybersecurity.	**7**
Модель представлення системи інформаційної безпеки.	2/2		Виконання та захист лабораторних робіт. Самостійне вивчення онлайн курсу Cisco-Cybersecurity.	**7**
Види та властивості інформації як предмета захисту	2/3		Виконання та захист лабораторних робіт.	**6**
Модуль 4. Державна політика у сфері телекомунікацій				
Інформаційно-комунікаційні технології та проблеми їхньої безпеки.	1/3	Вміти впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. Вміти застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.	Виконання та захист лабораторних робіт.	**7**
Критерії безпеки інформаційних технологій	1/2		Виконання та захист лабораторних робіт. Неформальна on-line освіта на основі Cisco.	**7**
Державна політика у сфері телекомунікацій. Проблеми розвитку захищених телекому-нікацій в Україні та основні шляхи їх розв'язання.	1/3		Виконання та захист лабораторних робіт. Неформальна on-line освіта на основі Cisco.	**7**
Інформаційна безпека в умовах сучасного стану та перспектив розвитку державності.	1/2		Виконання та захист лабораторних робіт. Неформальна on-line освіта на основі Cisco.	**7** **10**
Модульний контроль (3-4 модулі)			тест в E-Learn	**30**
Всього за 1 семестр				**70**
Залік			тест в E-Learn	**30**
Всього за курс				**100**

ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів та перескладання:	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).
Політика щодо академічної доброчесності:	Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних гаджетів).
Політика щодо відвідування:	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в он-лайн 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