СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Нормативно-правове забезпечення інформаційної бехпеки»

Лектор курсу			**Щавінський Юрій Віталійович,** кандидат технічних наук, .		**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:** yushchavinsky@ukr.net; **сторінка курсу в Moodle –** Курс: Нормативно-правове забезпечення інформаційної безпеки (dut.edu.ua)	
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	перший (бакалаврський)	
Спеціальність			125 Кібербезпека та захист інформації		**Семестр**	1	
Освітня програма			УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ		**Тип дисципліни**	основна	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	4	120	18	-	18	-	84

АНОТАЦІЯ КУРСУ

Мета курсу:	формування у студентів необхідної системи знань з основ національного та міжнародного законодавства, яке регулює правові відносини в інформаційній сфері, визначає сутність та зміст механізмів забезпечення інформаційної безпеки, світогляду щодо сфери забезпечення інформаційної безпеки, різновидів завдань інформаційної безпеки та способів їх вирішення; здобуття теоретичних знань, умінь, навичок та інших компетентностей щодо використання правових механізмів захисту інформації та вирішення інших завдань інформаційної безпеки

Компетентності відповідно до освітньої програми

Загальні компетентності (КЗ)	Фахові компетентності (КФ)
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. **КЗ 3**. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **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.	**КФ 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. **КФ 4.** Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. **КФ 7.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

Програмні результати навчання (ПРН)

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.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
ЗМІСТОВИЙ МОДУЛЬ **1 «ОСНОВИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ»**			
Тема №1. Теоретичні основи правового забезпечення інформаційної безпеки ***Знати***: сутність та основні поняття нормативно-правового забезпечення інформаційної безпеки, характеристику діяльності міжнародних організацій щодо правого забезпечення міжнародної інформаційної безпеки ***Вміти:*** характеризувати діяльність організацій щодо правого забезпечення інформаційної безпеки з урахуванням міжнародного досвіду . ***Формування компетенцій:*** КЗ 1, КЗ 3, КФ 1 ***Результати навчання:*** ПРН 7, ПРН 9 ***Рекомендовані джерела:*** 1-12, 15, 26, 28-31	Лекція 1,2,3 6 год	20*	Лекція-візуалізація
	Практичне заняття 1,2,3 6 год		Практична робота, Аналітичний метод, , проблемно-пошуковий метод 1.Характеристика діяльності міжнародних організацій щодо правого забезпечення міжнародної інформаційної безпеки 2.Інформаційне суспільство: сутність та основні напрями розвитку. 3.Діджиталізація України та інформаційна безпека
	Самостійна робота 12 год		Аналітичний метод, Практична робота 1. Принципи та джерела правового забезпечення інформаційної безпеки в Україні 2. Аналіз основних загроз інформаційній безпеці України та відповідних пріоритетів державної політики
ЗМІСТОВИЙ МОДУЛЬ **2 «НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ»**			
Тема №2. Нормативно-правове забезпечення інформаційно-психологічної (медіа) безпеки людини, суспільства та держави ***Знати***: види інформаційної війни, суть інформаційного тероризму, основні загрози безпеці людини, суспільства та держави, правові механізми забезпечення інформаційної безпеки України в умовах гібридної війни, способи боротьби з пропагандою та неправдивою (фейковою) інформацією, ***Вміти***: застосовувати способи боротьби з пропагандою та неправдивою (фейковою) інформацією при виконанні функціональних обов'язків, ***Формування компетенцій:*** КЗ 1, КЗ 3, КЗ 6, КФ 4, КФ 7	Лекція 4,5,6 6 год	20*	Лекція-візуалізація
	Практичне заняття 4,5,6 6 год		Дедуктивний метод, Практична робота 4.Правові механізми забезпечення інформаційної безпеки України в умовах гібридної війни. 5. Медіаграмотність громадян як основний спосіб захисту від маніпулювання суспільною свідомістю 6.Способи боротьби з пропагандою та неправдивою (фейковою) інформацією.
	Самостійна робота 22 год		Аналітичний метод, Практична робота 1. Механізми охорони державної таємниці

Результати навчання: ПРН 7, ПРН 9 ***Рекомендовані джерела:*** 1-12, 13-14, 16-38			2. Правове регулювання захисту інформаційного простору України від негативного інформаційно-психологічного впливу 3. Захист інтелектуальної власності в Україні
Тема №3 Нормативно-правове забезпечення кібербезпеки ***Знати***: склад і структуру національної системи кібербезпеки України, стандарти інформаційної безпеки, сутність і зміст викликів та загроз кібербезпеці України ***Вміти***: визначати пріоритети забезпечення кібербезпеки України, застосовувати знання при створенні СУІБ і системи управління інцидентами інформаційної безпеки (СУІБ) організації відповідно до вимог із стандартизації систем і процесів управління інформаційною безпекою. ***Формування компетенцій:*** КЗ 1, КЗ 3, КЗ 6, КФ 1, КФ 4 , КФ 7 ***Результати навчання:*** ПРН 7, ПРН 8, ПРН 9, ***Рекомендовані джерела:*** 1-15, 17-38	Лекція 7,8,9 6 год	10*	Лекція-візуалізація, експрес-опитування
	Практичне заняття 7,8,9 6 год		Аналітичний метод, Практична робота 7.Сутність і зміст викликів та загроз кібербезпеці України. 8.Кіберзахист об'єктів критичної інфраструктури 9.Пріоритети забезпечення кібербезпеки України
	Самостійна робота 20 год		Практична робота, аналітичний, частково-пошуковий метод 1. Права людини в Інтернет 2. Боротьба з кіберзлочинністю 3. Захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- мультимедійна система Acer X113 DLP
- комп'ютери Asus
- комп'ютерний клас для проведення занять: Спеціалізована лабораторія: «Управління інформаційною та кібербезпекою».
- програмне забезпечення перевірки СУІБ

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Базова

1. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
2. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
3. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки». URL: https://zakon.rada.gov.ua/laws/show/537-16#Text
4. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
6. Закон України «Про державну таємницю». URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
7. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
8. Конвенція про кіберзлочинність, ратифікована Верховною Радою України 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
9. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
10. Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037
11. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013
12. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069
13. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін.; за заг. ред. проф. К. І. Бєлякова. Київ:КВІЦ, 2019. 344 с..URL: http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf
14. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія/О.Д. Довгань, І.М.Доронін; НАПрН України, НДІІП – К.: Видавничий дім «АртЕк». – 2017. – 107с. URL: http://ippi.org.ua/sites/default/files/eskalaciya_kiberzagroz.pdf

15. Манжай О. В., Манжай І.А. Правові засади захисту інформації: підручник. – Харків : Панов, 2020. – 162 с. URL: http://univd.edu.ua/science-issue/issue/4315;

Допоміжна

16. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;
17. Закон України «Про боротьбу з тероризмом»;
18. Закон України «Про телекомунікації»;
19. Закон України «Про авторське право та суміжні права»;
20. Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних»;
21. Указ Президента України від 23 листопада 2011 року 1067/2011 «Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації»
22. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 року N 1229/99;
23. Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22 травня 1998 року N 505/98;
24. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені Постановою Кабінету Міністрів України від 19 червня 2019 р. № 518;
25. Міжнародні стандарти серії ISO/IEC 2700x:2018 «Information technology. Security techniques»;
26. Стандарт безпеки даних індустрії платіжних карток Payment Card Industry Data Security Standard (PCI DSS);
27. Стандарти інформаційної безпеки США NIST Special Publications 800 Series;
28. Відкритий IT-стандарт Асоціації з аудиту та контролю інформаційних система (ISACA) спільно із Інститутом управлінням IT (ITGI) CoBiT (Control Objectives for Information and Related Technology – «Контрольні цілі для інформаційних та суміжних технологій»);
29. Загальний регламент про захист даних ЄС GDPR (General Data Protection Regulation, GDPR; Regulation (EU) 2016/679
30. Указ Президента України від 15 травня 2017 року № 133/2017 «Про введення в дію Рішення РНБО України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»;
31. Наказ Служби безпеки України від 12.08.2005 № 440 «Про затвердження Зводу відомостей, що становлять державну таємницю»;
32. Указ Президента України від 29.10.2014 № 828/2014 «Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації»;
33. Постанова Кабінету Міністрів України від 29 березня 2006 р. N 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;
34. Постанова Кабінету Міністрів України від 16.11.2002 р. № 1772 «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах»
35. Наказ Адміністрації ДССЗЗІ України від 02.12.2014 № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;
36. Загальна теорія права : підручник / О. В. Петришин, В. В. Лемак, С. І. Максимов та ін.; Національний юридичний університет ім. Ярослава Мудрого. Харків: Право, 2020. 568 с.
37. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. – К. : НІСД, 2017. – 496 с.
38. Окінавська хартія глобального інформаційного суспільства.

Інформаційні ресурси

1. Презентації лекцій та практичних занять (електронний варіант).
2. Електронна бібліотека ДУТ.
3. Інтернет-ресурси:
   - Міжнародні договори, що набули чинності для України та включені до Єдиного державного реєстру нормативно-правових актів (по роках: 1991 – 2022). Сайт Міністерства юстиції України: https://minjust.gov.ua/;
   - Зібрання чинних міжнародних договорів України. Сайт Верховної Ради України, URL: https://zakon.rada.gov.ua/laws/main/b94 ;
   - Зібрання навчальних матеріалів державної освітньої програми «Дія. Цифрова освіта» URL: https://osvita.diia.gov.ua/;
   - Онлайн-бібліотека з питань медіаграмотності та інформаційної безпеки Міністерства культури та інформаційної політики України. URL: https://mip.gov.ua/news/10/;

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації, студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів.
- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент видаляється з заняття, за заняття отримує 0 балів.

***КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання студентом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,55 бала
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 бала
	• доповідь з презентацією за тематикою самостійного вивчення дисципліни (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді), підготовка реферату	за кожну презентацію (реферат) максимум 3 бали
	• усне опитування, тестування, рішення практичних задач	за кожну правильну відповідь 0,5 бала
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 2 бали
	• участь у діловій грі	за кожну участь 1 бал
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1 «ОСНОВИ ПРОФЕСІЙНОЇ ТА КОРПОРАТИВНОЇ ЕТИКИ»»	максимальна оцінка – 15балів
	Модульний контроль № 2 «ЕТИКА ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ В УПРАВЛІННІ КІБЕРБЕЗПЕКОЮ»	максимальна оцінка –15 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових робіт за спеціальністю, створення кейсів тощо.	Звільняється від іспиту
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Іспит***	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій формі.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90 -	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що	Відмінно / Зараховано (A)

	дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об ‘єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов’язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об’єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	
82-89	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	Добре / Зараховано (B)
75-81	Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)

	основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.		
64-74	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі іспиту.	**Незадовільний** Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*