МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Кафедра права
(назва кафедри, яка забезпечує викладання дисципліни)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Нормативно-правове забезпечення інформаційної безпеки в національному та міжнародному співробітництві

(назва навчальної дисципліни)

рівень вищої освіти перший (бакалаврський)
перший (бакалаврський) / другий (магістерський)

галузь знань05 Соціальні та поведінкові науки
(шифр і назва)

Спеціальність054 Соціологія
(шифр і назва)

освітня програма Соціологія управління
(назви освітньої програми)

вид дисципліни загальна підготовка; вибіркова
(загальна підготовка /спеціальна (фахова) підготовка; обов'язкова/вибіркова)

форма навчання денна
(денна / заочна/дистанційна)

Харків – 2023 рік

ЛИСТ ЗАТВЕРДЖЕННЯ

Робоча програма з навчальної дисципліни Нормативно-правове забезпечення інформаційної безпеки в національному та міжнародному співробітництві

Розробники:

Проф., канд.філософ.наук, доцент  Л.В. Перевалова
(посада, науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

Робоча програма розглянута та затверджена на засіданні кафедри права
(назва кафедри, яка забезпечує викладання дисципліни)

Протокол від « 25»серпня 2023року № 1

Завідувач кафедри_____  І.В. Лисенко
(підпис) (ініціали та прізвище)

ЛИСТ ПОГОДЖЕННЯ

Шифр та назва освітньої програми 054 Соціологія управління

Кафедра соціології і публічного управління
(назва кафедри, на якій викладається дисципліна)

Гарант ОП Бірюкова М.В. 30.08.20 23
(ПІБ) (Підпис, дата)

Завідувач кафедрою Мороз В.М. 30.08.2023
(ПІБ) (Підпис, дата)

ЛИСТ ПЕРЕЗАТВЕРДЖЕННЯ РОБОЧОЇ НАВЧАЛЬНОЇ ПРОГРАМИ

№ зп	Дата засідання кафедри-розробника РПНД	Номер протоколу	Підпис завідувача кафедри (яка викладає)	Підпис завідувача кафедри (на якій викладається)	Підпис гаранта освітньої програми
1					
2					
3					
4					
5					

МЕТА, КОМПЕТЕНТНОСТІ, РЕЗУЛЬТАТИ НАВЧАННЯ ТА СТРУКТУРНО-ЛОГІЧНА СХЕМА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою навчальної дисципліниНормативно-правове забезпечення інформаційної безпеки в національному та міжнародному співробітництві є формування у майбутніх фахівців розуміння сутності явища інформаційна безпека, ознайомити з основними загрозами інформаційній безпеці та виробити уявлення про ефективність інструментів забезпечення інформаційної безпеки особистості, держави, суспільства.

Компетентності:

Загальні компетентності

ЗК-1. Здатність застосовувати знання в практичних ситуаціях.

ЗК- 6. Здатність діяти соціально відповідально та свідомо.

ЗК - 11. 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.

Результати навчання

Програмні результати навчання за спеціальністю

РН17. Знати визначальні правові норми, що регулюють економічну, політичну, трудову, природоохоронну діяльність, знати принципи раціонального ставлення до навколишнього середовища.

Структурно-логічна схема вивчення навчальної дисципліни

Вивчення цієї дисципліни безпосередньо спирається на:	На результати вивчення цієї дисципліни безпосередньо спираються:
Правознавство	Соціологія реклами
Соціологія організації	

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(розподіл навчального часу за семестрами та видами навчальних занять)

Семестр	Загальний обсяг			За видами аудиторних занять (годин)			Індивідуальні завдання студентів (КП, КР, РГ, Р, РЕ)	Поточний контроль	Семестровий контроль	
	Всього (годин) / кредитів ECTS	З них								
		Аудиторні заняття (годин)	Самостійна робота (годин)	Лекції	Лабораторні заняття	Практичні заняття, семінари		Контрольні роботи (кількість робіт)	Залік	Екзамен
1	2	3	4	5	6	7	8	9	10	11
7	**120 /4**	**48**	**72**	**32**		**16**	**20**		**+**	

Співвідношення кількості годин аудиторних занять до загального обсягу складає 40 (%)

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
1	2	3	4	5
1	Л	2	**<u>Тема 1.</u>Поняття інформаційної безпеки держави, суспільства та особи** Інформаційна безпека (поняття і визначення). Інформаційна безпека, її сутність. Інтереси особи, суспільства та держави в інформаційній сфері	1, 2, 3, 10 - 13
2	ПЗ	2	***Поняття інформаційної безпеки держави, суспільства та особи*** Правове забезпечення інформації та інформаційної безпеки. Інформація та види інформації. Інформаційні відносини. Інформаційний суверенітет. Сутність інформаційної безпеки. Види інформаційної безпеки. Інформаційна сфера та інтереси особи, держави та суспільства.	
3	СР	5	***Поняття інформаційної безпеки держави, суспільства та особи*** 1. Які основні підходи до визначення поняття «інформаційна безпека» Ви знаєте? 2. Назвіть основні ознаки інформаційної безпеки. 3. Назвіть основні визначення поняття «інформаційна безпека». 4. У чому полягають інтереси особи, суспільства та держави в інформаційній сфері? 5. Назвіть об'єкти, суб'єкти та види інформаційної безпеки. 6. Що таке інформація? 7. Що таке джерело інформації? 8. Які є носії інформації? 9. Що розуміють під інформаційними ресурсами? 10. Що таке загроза інформаційній безпеці?	1, 2, 16 - 18
4	Л	2	**<u>Тема 2.</u>Інформаційна безпека та кібербезпека.** Кіберпростір: поняття та склад.Проблеми забезпечення інформаційної та кібербезпеки.Стратегії забезпечення національної	

			безпеки держави. Закон України «Про національну безпеку».	
5.	ПЗ	2	***Проблеми забезпечення інформаційної безпеки та кібербезпеки в Україні*** Кіберпростір та його співвідношення з інформаційною безпекою. Кібербезпека склад та сутність. Стратегія забезпечення національної безпеки. Фундаментальні національні інтереси України.	
6	СР	5	***Проблеми забезпечення інформаційної безпеки та кібербезпеки в Україні*** 1. Що таке кіберборотьба? 2. Які основні особливості їй притаманні? 3. Дайте визначення поняття «кібернетична безпека». 4. Назвіть істотні ознаки, які його характеризують. 5. Причини головних проблем забезпечення кібернетичної безпеки. 6. Які стратегії затверджені в Законі України «Про національну безпеку України»? 7. Стратегія воєнної безпеки України. 8. Стратегія кібербезпеки України. 9. Стратегія громадської безпеки та цивільного захисту України.	1, 2, 10, 17, 18 - 20
7	Л	2	**<u>Тема 3.</u>Загрози для інформаційної безпеки держави, суспільства, людини** Поняття загроз інформаційній безпеці. Види загроз інформаційній безпеці. Фактори загроз інформаційній безпеці. Джерела загроз інформаційній безпеці**.** Етапи розвитку засобів інформаційних комунікацій	
8	ПЗ	2	***Інформаційна безпека та існуючі загрози*** Інформаційна безпека держави та життєво важливі інтереси особистості, суспільства та держави.Об'єкти та суб'єкти інформаційної безпеки. Концепція інформаційної безпеки. Класифікація видів загроз інформаційній безпеці України. Внутрішні та зовнішні джерела загроз інформаційній безпеці. України. Принципи забезпечення інформаційної безпеки. Система забезпечення інформаційної безпеки держави. Основні форми і способи забезпечення інформаційної безпеки держави.	
9	СР	7	***Інформаційна безпека та існуючі загрози*** 1. Яким чином розрізняються групи загроз інформації? 2. Дайте визначення поняттям «загроза»,	

			«небезпека». 3. Визначте види загроз за ймовірністю реалізації. 4. Визначте види загроз за джерелами походження. 5. Визначте види загроз за значенням. 6. Визначте види загроз за структурою та об'єктом впливу. 7. Визначте види загроз за характером реалізації. 8. Які основні підходи до визначення дестабілізуючих факторів ви знаєте? 9. Визначте політичні фактори загроз. 10. Визначте економічні фактори загроз. 11. Визначте організаційно-технічні фактори загроз. 12. Назвіть джерела загроз інформаційній безпеці особи. 13. Назвіть джерела загроз інформаційній безпеці суспільству. 14. Назвіть джерела загроз інформаційній безпеці держави. 15. Які існують етапи розвитку засобів інформаційних комунікацій?	1, 2, 10, 17, 18 – 20, 23
10	Л	4	**<u>Тема 4.</u>Принципи, форми та методи забезпечення інформаційної безпеки держави** Основні принципи забезпечення інформаційної безпеки держави. Основні форми забезпечення інформаційної безпеки держави. Методи забезпечення інформаційної безпеки	
11	ПЗ	2	***Основні принципи, форми та методи забезпечення інформаційної безпеки.*** Основні та специфічні принципи інформаційної безпеки. Основні форми забезпечення інформаційної безпеки: інформаційний патронат, інформаційна кооперація, інформаційне протиборство.	
12	СР	7	***Основні принципи, форми та методи забезпечення інформаційної безпеки.*** 1. Поняття забезпечення інформаційної безпеки держави. 2. Основні принципи забезпечення інформаційної безпеки держави. 3. Що таке превентивність? 4. Як можна тлумачити поняття адекватної інформованості? 5. Що таке інформаційний патронат? 6. Що таке інформаційна кооперація? 7. Дати визначення інформаційного протиборства. 8. Способи забезпечення інформаційної безпеки для конкретної особи. 9. Методи забезпечення інформаційної безпеки. 10. Рівні сфери інформаційної безпеки.	1, 2, 10, 17, 18 - 21

			11. Які є методи впливу на інформацію?	
13	Л	4	**<u>Тема 5.</u> Інформаційне протиборство між країнами. Інформаційна війна** Основні форми інформаційного протиборства.Інформаційна війна та її завдання. Концепція інформаційної війни.Органи інформаційної війни.Основні форми інформаційної війни.Інформаційна зброя.	
14	ПЗ	2	***Інформаційна війна як найвищий ступень інформаційного протиборства*** Інформаційне протиборство та його види. Об'єкти впливу інформаційного протиборства. Концепція інформаційного протиборства. Ступені інформаційного протиборства. Інформаційна війна та її особливості. Завдання інформаційної війни. Основні форми та рівні інформаційної війни. Засоби інформаційної війни. Інформаційні переваги у сфері інформаційного протиборства.	
15	СР	5	***Інформаційна війна як найвищий ступень інформаційного протиборства*** 1. Дайте визначення поняття «інформаційне протиборство». 2. Назвіть рівні проведення інформаційного протиборства. 3. Назвіть основні ступені інформаційного протиборства. 4. Що відноситься до органів інформаційної війни? 5. Назвіть основні форми інформаційної війни. 6. Що являє собою оперативна безпека?	1, 2, 10, 17, 18 - 21
16	Л	2	**<u>Тема 6.</u> Інформаційна зброя в інформаційні війні** Інформаційна зброя та сфера її застосування. Основні об'єкти застосування інформаційної зброї. Види інформаційної зброї. Особливості застосування інформаційної зброї.	
17	ПЗ	2	***Інформаційна зброя та її складові*** Інформаційна зброя воєнного та невоєнного застосування. Засоби ураження комп'ютерних інформаційних систем. Програми з потенційно небезпечними наслідками.	
18	СР	4	***Інформаційна зброя та її складові*** 1.Яким чином відрізняється інформаційна зброя від звичайних засобів ураження? 2. Назвіть сферу застосування інформаційної зброї. 3. Назвіть основні об'єкти застосування інформаційної зброї. 4. Що таке комп'ютерні віруси?	1, 2, 10, 16, 17, 18 - 21

			5. Які існують види програмних закладок? 6. Назвіть та охарактеризуйте засоби несанкціонованого доступу. 7. Які існують особливості застосування інформаційної зброї?	
19	Л	4	**<u>Тема 7.</u> Основи теорії інформаційної боротьби** Зміст теорії інформаційної боротьби.Закони та закономірності інформаційної боротьби.Принципи інформаційної боротьби.Заходи інформаційної боротьби.Способи та форми інформаційної боротьби.	
20	ПЗ	1	***Теорія інформаційної боротьби та її сутність*** Поняття теорії інформаційної боротьби та її мета. Фактори впливу: економічний, воєнний та інформаційний. Загальні основи теорії інформаційної боротьби та її структура. Теорія сил та засобів ураження інформації. Теорія захисту інформації. Особливості законів та закономірностей інформаційної боротьби. Заходи інформаційної боротьби: інформаційне забезпечення, інформаційний захист, інформаційна протидія. Способи інформаційної боротьби та їх класифікація.	
21	СР	7	***Теорія інформаційної боротьби та її сутність*** 1. Дати визначення інформаційної боротьби. 2. Яка мета інформаційної боротьби? 3. Які фактори впливають на зміст інформаційної боротьби? 4. Які існують заходи інформаційної боротьби? 5. Охарактеризувати принципи інформаційної боротьби. 6. Дати визначення метода оцінки ефективності інформаційної боротьби. 7. Які існують форми ведення інформаційної боротьби? 8. Які існують способи інформаційної боротьби? 9. Що таке радіоелектронно-вогневий удар? 10.Формула для обчислення числового значення критерію ефективності інформаційної боротьби.	1, 2, 10, 16, 17, 18 - 24
22	Л	4	**<u>Тема 8.</u> Основи безпеки інформаційних ресурсів** Поняття та загальні властивості інформації. Поняття загроз.Загрози безпеки інформації та інформаційних ресурсів.Джерела загроз безпеці інформації.Класифікація вразливостей безпеки.Моделі порушень інформаційних ресурсів	
23	ПЗ	1	***Основи безпеки інформаційних технологій*** Інформація та її зміст. Одержувачі інформації. Загрози порушення конфіденційності, цілісностіта	

			доступності інформації. Загрози безпеки інформації та інформаційних ресурсів. Порушення та їх види. Джерела загроз безпеки інформації: антропогенні, техногенні та викликані стихійними джерелами. Порушники,цілі та мета їх дій.	
24	СР	7	***Основи безпеки інформаційних технологій*** 1. Що є джерелом та фактором загрози інформації? 2. Які є види загроз комп'ютерної інформації? 3. Які є групи джерел загроз безпеці інформації? 4. Наведіть класифікацію вразливостей безпеці інформації? 5. Які класи (види) загроз розрізняються в інформаційній сфері? 6. Які загрози відносяться до рівня порушення конфіденційності ? 7. Які загрози відносяться до рівня порушення цілісності ? 8. Які існують категорії джерел конфіденційної інформації? 9. Які є моделі порушень інформаційних ресурсів? 10. Яка мета та цілі порушника об'єктів інформаційної діяльності? 11. Наведіть класифікацію порушника за характером дій?	1, 2, 10, 14 - 17, 18 - 24
25	Л	4	**<u>Тема 9.</u> Забезпечення безпеки інформації та інформаційних ресурсів** Напрями захисту інформації. Правовий захист. Організаційний захист. Інженерно-технічний захист. Захист інформаційних систем	
26	СР	7	***Забезпечення безпеки інформації та інформаційних ресурсів*** 1. Які напрями захисту інформації ви знаєте? 2. Сформулюйте поняття права. 3. Яка структура правових актів, які орієнтовані на правовий захист інформації? 4. Дати визначення ліцензії. 5. Що таке комерційна таємниця? 6. Що забезпечує організаційний захист? 7. Назвіть основні організаційні заходи. 8. Функції служби безпеки підприємства (фірми, організації). 9. Завдання служби безпеки підприємства (фірми, організації). 10. Що таке інженерно-технічний захист? Його завдання. 11. Фізичні засоби захисту та їх завдання. 12. Які апаратні засоби захисту інформації Ви знаєте? 13. Що таке криптографія?	1, 2, 10, 16, 17, 18 - 24

			14. Назвіть переваги цифрового шифрування.	
27	Л	2	**<u>Тема 10.</u> Захист інформаційних систем** Джерела конфіденційної інформації. Інформаційна система як об'єкт захисту. Рівні захисту інформаційних систем. Основні принципи захисту інформаційних систем.	
28	ПЗ	1	***Захист інформаційних систем*** Джерела інформації. Люди як джерела інформації. Інформаційна система, її структура. Інформаційні ресурси та їх властивості. Рівні захисту інформації: локальний, мережевий, на рівні користувачів. Корпоративні інформаційні системи (КІС).	
29	СР	9	***Захист інформаційних систем*** 1. Які існують категорії джерел конфіденційної інформації? 2. Які складові має інформаційна система? 3. Розкрийте поняття «цілісність». 4. Розкрийте поняття «доступність». 5. Розкрийте поняття конфіденційності інформації. 6. Назвіть основні напрями забезпечення безпеки інформації. 7. Розкрийте зміст моделі системи захисту інформації. 8. Якими показниками може бути оцінено якість розподілу доступу? 9. Назвіть основні принципи та рівні захисту інформаційних систем. 10. Розкрийте поняття інформаційно-комунікаційної системи. 11. Назвіть рівні інформаційно-комунікаційних мереж. 12. Сутність випадкового методу доступу до ресурсів системи. 13. Основні завдання захисту інформації в мережі? 14. Різновиди побудови комп'ютерних мереж? 15.Що повинні включати угоди обміну програмним забезпеченням? 16.Назвіть заходи управління обробкою й зберіганням інформації.	1, 2, 10, 14 - 17, 18 - 24
30	Л	2	**<u>Тема 11.</u> Інформаційна безпека України** Інформаційна безпека та її місце в національній безпеки України. Основні реальні та потенційні загрози інформаційній безпеці України. Стан та перспективи розвитку інформаційної безпеки. Система та політика забезпечення інформаційної безпеки.	
31	ПЗ	1	***Забезпечення інформаційної безпеки України***	

32	СР	9	Національна безпека та її структура. Принципи забезпечення національної безпеки. Загрози інформаційної безпеки: зовнішні та внутрішні загрози. Сутність інформаційної безпеки. Мета та завдання забезпечення інформаційної безпеки України. ***Забезпечення інформаційної безпеки України*** 1. Що розуміється під «інформаційною безпекою України»? 2. Яке її місце в системі національної безпеки України? 3. Основні напрями політики інформаційної безпеки України? 4. Найважливіші завдання у сфері інформаційної безпеки? 5. В яких сферах проявляються реальні та потенційні загрози безпеці України? 6. Охарактеризуйте загрози інформаційній безпеці України у воєнній сфері. 7. Охарактеризуйте загрози інформаційній безпеці України в економічній сфері. 8. Охарактеризуйте загрози інформаційній безпеці України в екологічній сфері. 9. Які завдання реалізації інформаційної політики з питань євроінтеграції? 10. Яким чином розрізняються групи загроз інформації? 11. Дайте визначення поняттям «загроза», «небезпека». 12. Визначте види загроз за ймовірністю реалізації. 13. Визначте види загроз за джерелами походження. 14. Визначте види загроз за значенням. 15. Визначте види загроз за структурою та об’єктом впливу. 16. Визначте види загроз за характером реалізації. 17. Які основні підходи до визначення дестабілізуючих факторів ви знаєте? 18. Визначте політичні фактори загроз. 19. Визначте економічні фактори загроз. 20. Визначте організаційно-технічні фактори загроз. 21. Назвіть джерела загроз інформаційній безпеці особи. 22. Назвіть джерела загроз інформаційній безпеці суспільству. 23. Назвіть джерела загроз інформаційній безпеці держави. 24. Які існують етапи розвитку засобів інформаційних комунікацій?	
Разом (годин)		120		

САМОСТІЙНА РОБОТА

№ з/п	Назва видів самостійної роботи	Кількість годин
1	Опрацьовуваннялекційного матеріалу	16
2	Підготовка до практичних (лабораторних) занять	16
3	Самостійне вивчення тем та питань, які не викладаються на лекційних заняттях	20
4	Виконання індивідуального завдання:	20
5	Інші види самостійної роботи	
	Разом	72

ІНДИВІДУАЛЬНІ ЗАВДАННЯ

№	Теми презентацій	Тиждень
1	**Тема 2. Проблеми забезпечення інформаційної безпеки та кібербезпеки в Україні** 1. Загальний аналіз Доктрини національної безпеки України, яка введена в дію Указом Президента від 25.02.2017 р 2. Національні інтереси України в інформаційній сфері (з використанням положень Доктрини та іншого матеріалу) 3. Загрози національним інтересам та національної безпеки України. 4. Пріоритети державної політики в інформаційній сфері. 5. Механізми реалізації інформаційній безпеки в Україні. 6. Стратегія національної безпеки України 7. Стратегія кібербезпеки України 8. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»	2-3

	(загальний аналіз). 9. Загальний аналіз Закону України «Про захист персональних даних» 10. Загальний аналіз Закону України «Про державну таємницю» 11. Загальний аналіз Постанов КМУ «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», «Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію»	
2	**Тема 4. Основні принципи, форми та методи забезпечення інформаційної безпеки** 1. Основні завдання системи забезпечення інформаційної безпеки. 2. Мета функціонування системи забезпечення інформаційної безпеки. 3. Основні способи та засоби забезпечення інформаційної безпеки людини. 4. Опис та класифікація як методи аналізу стану забезпечення інформаційної безпеки. 5. Загальні методи забезпечення інформаційної безпеки. 6. Метод розвитку та його значення для забезпечення інформаційної безпеки. 7. Країни Європи в світовому інформаційному просторі. 8. Світовий інформаційний простір і місце країн Європи в ньому. 9. Системи інформаційної безпеки в країнах Європи 10. Система інформаційної безпеки у США.	4-5
3	**Тема 6. Інформаційна зброя та її складові** . Програми з потенційно-небезпечними наслідками та їх функції. 2. Комп'ютерні віруси. 3. Засоби несанкціонованого доступу. 4. Програмні закладки 5. Троянські програми. 6. Логічні бомби та люки.	7

	7. Засоби ураження людей та їхньої психіки. 8. Особливості застосування інформаційної зброї.	
4	**Тема 7. Теорія інформаційної боротьби та її сутність** .Інтелектуальні способи інформаційної боротьби. 2. Способи блокування інформації. 3.Мета та завдання інформаційної операції. 4. Інформаційне забезпечення в умовах інформаційної боротьби. 5. Загальна характеристика принципів інформаційної боротьби.	9
5	**Тема 9. Основні напрями забезпечення безпеки інформації та інформаційних ресурсів** 1. Загальна характеристика міжнародних актів та національного законодавства, спрямованого на захист інформації та інформаційних ресурсів. 2. Конституційні права на інформацію та забезпечення її захисту. 3. Страхове забезпечення захисту інформації як напрям правового захисту. 4. Ліцензія як офіційний засіб захисту інформації. 5. Комерційна таємниця та способи її захисту. 6. Основні організаційні засоби захисту інформації та їх види. 7. Особливості організаційного захисту комп'ютерних інформаційних систем. 8. Правовий статус служби безпеки підприємства. 9. Особливості програмного захисту інформації. 10. Криптографічні засоби захисту інформації.	11
6	**Тема 10. Захист інформаційних систем** Інформаційна система як об'єкт захисту. 2. Характерні ознаки інформаційних систем. 3. Рівні захисту інформаційних систем. 4. Основні види експлуатації інформаційних систем. 5. Європейські критерії безпеки інформаційних технологій.	12-13

	6. Канадські критерії безпеки комп'ютерних систем. 7. Основні положення загальних критерії безпеки інформаційних технологій. 8. Функціональні вимоги до засобів захисту. 9. Загальні вимоги та структуру гарантій безпеки. 10. Загальні вразливості корпоративних інформаційних систем	
7	**Тема 11. Забезпечення інформаційної безпеки України** 1. Закон України «Про національну безпеку України». 2.Національні інтереси України в інформаційній сфері та шляхи їх забезпечення. 3. Особливості забезпечення інформаційної безпеки у різних сферах суспільного життя. 4. Перспективи міжнародного співробітництва України в галузі забезпечення інформаційної безпеки. 5. Заходи щодо реалізації політики забезпечення інформаційної безпеки України.	14-15

МЕТОДИ НАВЧАННЯ

Під час проведення занять знавчальної дисципліни «Нормативно-правове забезпечення інформаційної безпеки в національному та міжнародному співробітництві» використовуються такі методи навчання як: інноваційні методи з використанням мультимедійних презентацій, співбесіда, пояснення, ділова гра, вирішення конкретних правових ситуацій із застосуванням нормативно-правових актів України.

МЕТОДИ КОНТРОЛЮ

Контроль складової робочої програми, яка освоюється під час самостійної роботи студента, проводиться:

- з лекційного матеріалу – шляхом перевірки конспектів;

- з практичних занять – за допомогою виступів. перевірки виконаних завдань, тестів, реферату за обраною темою, проведення контрольних робіт тощо.

- з індивідуальних завдань – за допомогою перевірки реферату за обраною темою.

Семестровий контроль проводиться у формі заліку (з оцінкою) відповідно до навчального плану в обсязі навчального матеріалу, визначеного навчальною програмою та у терміни, встановлені навчальним планом.

Питання до заліку

1. Що розуміється під «інформаційною безпекою України»?
2. Місце інформаційної безпеки в системі національної безпеки України.
3. Основні напрями політики інформаційної безпеки України.
4. Основні завдання у сфері інформаційної безпеки.
5. Сфери прояву реальних та потенційних загроз безпеці України.
6. Охарактеризуйте загрози інформаційній безпеці України у воєнній сфері.
7. Охарактеризуйте загрози інформаційній безпеці України в економічній сфері.
8. Охарактеризуйте загрози інформаційній безпеці України в екологічній сфері.
9. Завдання України у сфері реалізації інформаційної політики з питань євроінтеграції.
10. Критерії загроз інформації
11. Дайте визначення поняттям «загроза» та «небезпека», їх особливості.
12. Визначте види загроз за ймовірністю реалізації.
13. Визначте види загроз за джерелами походження.
14. Визначте види загроз за значенням.
15. Визначте види загроз за структурою та об’єктом впливу.
16. Визначте види загроз за характером реалізації.
17. Основні підходи до визначення дестабілізуючих факторів.
18. Політичні фактори загроз.
19. Економічні фактори загроз.
20. Організаційно-технічні фактори загроз.
21. Джерела загроз інформаційній безпеці особи та їх характеристика.
22. Джерела загроз інформаційній безпеці суспільству.
23. Джерела загроз інформаційній безпеці держави.
24. Охарактеризуйте етапи розвитку засобів інформаційних комунікацій.
25. Джерела конфіденційної інформації та їх категорії.
26. Складові інформаційної системи.
27. Конфіденційність інформації:поняття та ознаки.
28. Основні напрями забезпечення безпеки інформації.
29. Розкрийте зміст моделі системи захисту інформації.
30. Основні принципи та рівні захисту інформаційних систем.
31. Інформаційно-комунікаційна система та її рівні.

32. Основні завдання захисту інформації в мережі.
33. Різновиди побудови комп'ютерних мереж.
34. Напрями захисту інформації.
35. Структура правових актів, що орієнтовані на правовий захист інформації.
36. Ліцензія як засіб захисту інформації
37. Комерційна таємниця та її захист.
38. Основні організаційні заходи та їх характеристика.
39. Функції служби безпеки підприємства (фірми, організації).
40. Завдання служби безпеки підприємства (фірми, організації).
41. Інженерно-технічний захист, його завдання.
42. Фізичні засоби захисту та їх завдання.
43. Апаратні засоби захисту інформації.
44. Криптографія, її сутність та завдання.
45. Переваги цифрового шифрування.
46. Джерела та фактори загрози інформації.
47. Види загроз комп'ютерної інформації.
48. Класифікація вразливостей безпеці інформації.
49. Класи (види) загроз в інформаційній сфері.
50. Мета та цілі порушників об'єктів інформаційної діяльності.
51. Класифікація порушників за характером дій.
52. Інформаційна боротьба та її мета.
53. Принципи інформаційної боротьби.
54. Заходи інформаційної боротьби.
55. Форми та способи ведення інформаційної боротьби.
56. Інформаційна зброя та сфера її застосування.
57. Основні об'єкти застосування інформаційної зброї.
58. Види інформаційної зброї.
59. Охарактеризуйте засоби несанкціонованого доступу.
60. Особливості застосування інформаційної зброї.
61. Інформаційне протиборство та рівні його проведення.
62. Основні ступені інформаційного протиборства.
63. Органи інформаційної війни.
64. Основні форми інформаційної війни.
65. Забезпечення інформаційної безпеки держави: поняття та принципи.
66. Адекватна інформованість, її значення.
67. Інформаційний патронат, сутність та значення.
68. Інформаційна кооперація: поняття та сутність.
69. Інформаційне протиборство.
70. Способи та методи забезпечення інформаційної безпеки конкретної особи.
71. Рівні сфери інформаційної безпеки.
72. Групи загроз інформації, критерії їх виділення.
73. Визначте види загроз за ймовірністю реалізації.
74. Визначте види загроз за джерелами походження.
75. Визначте види загроз за значенням.

76. Визначте види загроз за структурою та об’єктом впливу.
77. Визначте види загроз за характером реалізації.
78. Основні підходи до визначення дестабілізуючих факторів.
79. Політичні фактори загроз.
80. Визначте економічні фактори загроз.
81. Визначте організаційно-технічні фактори загроз.
82. Джерела загроз інформаційній безпеці особи та їх характеристика.
83. Джерела загроз інформаційній безпеці суспільству.
84. Джерела загроз інформаційній безпеці держави.
85. Етапи розвитку засобів інформаційних комунікацій.
86. Кіберборотьба, її основні особливості.
87. Кібернетична безпека: поняття та істотні ознаки.
88. Охарактеризуйте причини головних проблем забезпечення кібернетичної безпеки.
89. Які стратегії затверджені в Законі України «Про національну безпеку України»? Надайте їх характеристику.
90. Охарактеризуйте стратегію воєнної безпеки України.
91. Охарактеризуйте стратегію кібербезпеки України.
92. Стратегія громадської безпеки та цивільного захисту України.
93. Інформаційна безпека та її ознаки.
94. У чому полягають інтереси особи, суспільства та держави в інформаційній сфері?
95. Об’єкти, суб’єкти та види інформаційної безпеки.
96. Інформація: поняття та види.
97. Джерела та носії інформації.
98. Законодавче забезпечення захисту інформації та інформаційних ресурсів.
99. Інформаційні ресурси: поняття та види
100. Загрози інформаційній безпеці людині, державі, суспільству.

РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ, ТА ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ТА УМІНЬ (НАЦІОНАЛЬНА ТА ECTS)

Таблиця 1. – Розподіл балів для оцінювання успішності студента для заліку

Перевірка конспектів	Індивідуальні завдання	КР (КП)	РГЗ	Поточний контроль	Тощо	Залік	Сума
15	15	….	…	15	….	55	100

Таблиця 2 – Шкала оцінювання знань та умінь: національна та ECTS

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
1	**2**	**3**	**4**	**5**
90-100	A	Відмінно	- Глибоке знання навчального матеріалу, що містяться в основних і додаткових літературних джерелах; - вміння аналізувати явища, які вивчаються, в їхньому взаємозв'язку і розвитку; - вміння проводити теоретичні розрахунки; - відповіді на запитання чіткі, лаконічні, логічно послідовні; - вміння вирішувати складні практичні задачі.	Відповіді на запитання можуть містити незначні неточності
82-89	B	Добре	- Глибокий рівень знань в обсязі обов'язкового матеріалу, - вміння давати аргументовані відповіді на запитання і проводити теоретичні розрахунки; - вміння вирішувати складні практичні задачі.	Відповіді на запитання містять певні неточності;
75-81	C	Добре	- Міцні знання матеріалу, що вивчається, та його практичного застосування; - вміння давати аргументовані відповіді на запитання і проводити теоретичні розрахунки; - вміння вирішувати практичні задачі.	- невміння використовувати теоретичні знання для вирішенняскладних практичних задач.
64-74	D	Задовільно	- Знання основних фундаментальних положень матеріалу, що вивчається, та їх практичного застосування; - вміння вирішувати прості практичні задачі.	Невміння давати аргументовані відповіді на запитання; - невміння аналізувати викладений матеріал і виконувати розрахунки; - невміння

				вирішувати складні практичнізадачі.
60-63	E	Задовільно	- Знання основних фундаментальних положень - вміння вирішувати найпростіші практичні задачі.	Незнання окремих (непринципових) питань з матеріалу модуля; - невміння послідовно і аргументовано висловлювати думку; - невміння застосовувати теоретичні положення при розв’язанні практичних задач
35-59	FX (потрібне додаткове вивчення)	Незадовільно	Додаткове вивчення матеріалу може бути виконане в терміни, що передбачені навчальним планом.	Незнання основних фундаментальних положень навчального матеріалу модуля; - істотні помилки у відповідях на запитання; - невміння розв’язувати прості практичні задачі.
1-34	F (потрібне повторне вивчення)	Незадовільно	-	- Повна відсутність знань значної частини навчального матеріалу модуля; - істотні помилки у відповідях на запитання; -незнання основних фундаментальних положень; - невміння орієнтуватися під час розв’язання простих практичних задач

НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Конспект лекцій, плани практичних занять, завдання для самостійної роботи, питання, задачі, завдання для поточного та підсумкового контролю знань і вмінь студентівта інші методичні матеріали, які є в наявності.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова література:

1.Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві: навч.-метод. посіб. / Л. В. Перевалова, І. В. Лисенко, А.М. Лисенко, Г. М. Гаряєва – Харків: НТУ «ХПІ», 2023. – 110 с. URL: https://web.kpi.kharkov.ua/pravo/uk/publikatsiyi/metodichki/

2. Методичні вказівки до практичних занять з навчального курсу «Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві» / уклад.: Л.В. Перевалова, І.В. Лисенко, Г. М. Гаряєва. – Харків: НТУ «ХПІ», 2023. – 68 с. URL: https://web.kpi.kharkov.ua/pravo/uk/publikatsiyi/metodichki/

3. Тезаурус з правознавства: / Перевалова Л.В., Гаєвая О.В., Гаряєва Г.М., Кузьменко О.В., Лисенко І.В., Ткачов М.М. – Харків НТУ «ХПІ», 2021. – 194с. URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/53286

4. Правове регулювання договірних відносин: навчальний посібник/ Г.М. Гаряєва, О.В.Гаєвая, О.В. Кузьменко, І.В. Лисенко, Л.В. Перевалова.- Харків: НТУ «ХПІ», 2020. - 404 с.URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/55377

5.Правове регулювання підприємницької діяльності в Україні: текст лекцій / В. Г. Вергун, Г. М. Гаряєва, О. В. Кузьменко. - Харків : ФОП Панов А. М., 2021. - 128 с. URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/51920

6. Правове регулювання господарської діяльності в Україні. LegalregulationofeconomicactivitiesinUkraine (на англійської мові). /Навчальний посібник / Л.В. Перевалова, І.В. Лисенко, А.М. Лисенко, О.В. Гаєвая, Г.М. Гаряєва . – Харків: НТУ «ХПІ», 2020.-130с. URL:https://repository.kpi.kharkov.ua/handle/KhPI-Press/48578

7.Правові засади управлінської діяльності: навч.-метод. посіб. / Л.В. Перевалова, О.В. Гаєвая, Г.М. Гаряєва, І.В. Лисенко. Харків : ФОП Панов А.М., 2020. - 50 с. URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/48902
8.Правове регулювання внутрішнього ринку Європейського Союзу : навч.-метод. посіб. / Л.В. Перевалова, О.В. Гаєвая, Г.М. Гаряєва. Харків : ФОП Панов А.М., 2020. - 68 с. URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/49203
9. Методичні вказівки до виконання контрольних робіт з правових дисциплін для студентів заочної форми навчання усіх спеціальностей / уклад.: О. В. Гаєвая, Г. М. Гаряєва, І. В. Лисенко, Л. В. Перевалова. – Харків: НТУ «ХПІ», 2021 – 128 с. URL: http://web.kpi.kharkov.ua/pravo/wp-content/uploads/sites/90/2021/06/Metodichni-vkazivki_dlya-napisannya-kr-dlya-zo-1-1.docx

Допоміжна література

10.Конституція України // Відомості Верховної Ради України (ВВР), 1996, №30, ст. 141. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
11.Цивільний кодекс України // Відомості Верховної Ради України (ВВР), 2003, №№ 40-44, ст.356. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/435-15#Text
12.Господарський кодекс України // Відомості Верховної Ради України (ВВР), 2003, № 18, № 19-20, № 21-22, ст.144. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/436-15#Text
13.Кодекс законів про працю України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/322-08#Text
14.Кодекс України про адміністративні правопорушення // Відомості Верховної Ради Української РСР (ВВР) 1984, додаток до № 51, ст.1122 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/80731-10#Text
15.Кримінальний кодекс України // Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2341-14#Text
16.Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України– від 7.09.2005 року № 2824-IV. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/994_575#Text

17. Про інформацію: Закон України // Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text
18. Про національну безпеку України: Закон України// Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#Text
19. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України// Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
20. Про доступ до публічної інформації: Закон України // Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2939-17#Text
21. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України// Відомості Верховної Ради України (ВВР), 2006, № 30, ст.258. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/3475-15#Text
22. Резолюция 60/45, принятая Генеральной Ассамблеей ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://zakon.rada.gov.ua/laws/show/995_e45#Text
23. Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі». URL: https://zakon.rada.gov.ua/laws/show/994_243#Text
24. Решение № 1106 «Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий» от 03.12.2013. URL: https://www.osce.org/files/f/documents/0/a/109648.pdf

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

1. Верховна Рада України. Офіційний веб-портал парламенту України. [Електронний ресурс]. Режим доступу: https://www.rada.gov.ua/
2. Президент України. Офіційне інтернет-представництво. Президента України. [Електронний ресурс]. Режим доступу: https://www.president.gov.ua/

3. Кабінет Міністрів України. Урядовий портал. Єдиний веб-портал виконавчий органів України. [Електронний ресурс]. Режим доступу: https://www.kmu.gov.ua/
4. Національний технічний університет «Харківський політехнічний інститут». Кафедра права. [Електронний ресурс]. Режим доступу: http://web.kpi.kharkov.ua/pravo/uk/