НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

ЗАТВЕРДЖЕНО
Факультет інформаційних технологій
02 червня 2025 р

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Стандарти інформаційної та кібернетичної безпеки

Галузь знань _____F Інформаційні технології_____

Спеціальність _____F5 Кібербезпека та захист інформації_____

Освітня програма _____«Кібербезпека»_____

Факультет (ННІ)_____інформаційних технологій_____

Розробники: _____професор, д.т.н., професор, Лахно В.А.,

_____ професор, д.т.н., професор, Криворучко О.В.

(посада, науковий ступінь, вчене звання)

Київ – 2025 р.

Опис навчальної дисципліни "Стандарти інформаційної та кібернетичної безпеки"

Навчальна дисципліна передбачає вивчення основних підходів до забезпечення інформаційної безпеки в організаціях різної форми власності; ґрунтовне ознайомлення здобувачів із основними нормативними документами в галузі інформаційної безпеки та особливостями їх застосування на практиці; ознайомлення здобувачів із основними типами технологічних рішень направленими на забезпечення інформаційної безпеки; формування у здобувачів знань, вмінь і навичок щодо впровадження та застосування теоретичних знань щодо забезпечення інформаційної безпеки в майбутній професійної діяльності.

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	*бакалавр*	
Спеціальність	*125 Кібербезпека та захист інформації*	
Освітня програма	*«Кібербезпека»*	
Характеристика навчальної дисципліни		
Вид	*вибіркова*	
Загальна кількість годин	*150*	
Кількість кредитів ECTS	*5*	
Кількість змістових модулів	*2*	
Курсовий проект (робота) (за наявності)	---	
Форма контролю	*екзамен*	
Показники навчальної дисципліни для денної та заочної форм здобуття вищої освіти		
	Форма здобуття вищої освіти	
	денна	**заочна**
Курс (рік підготовки)	3	
Семестр	6	
Лекційні заняття	*30 год.*	*---год.*
Практичні, семінарські заняття	*30 год.*	*---год.*
Лабораторні заняття	*год.*	*---год.*
Самостійна робота	*90 год.*	*---год.*
Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти	*4 год.*	----

1. Мета, компетентності та програмні результати навчальної дисципліни

Мета вивчення дисципліни полягає у формуванні у майбутніх фахівців 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.

Набуття компетентностей:

інтегральна компетентність (ІК):

Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

загальні компетентності (ЗК):

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.
ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.
спеціальні (фахові) компетентності (СК):
СК1. Здатність застосовувати законодавчу та нормативноправову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.
СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.
СК3. Здатність забезпечувати неперервність бізнеспроцесів згідно встановленої політики кібербезпеки та захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.
СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)
СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
Програмні результати навчання (ПРН):
ПРН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
ПРН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
ПРН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
ПРН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
ПРН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
ПРН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
ПРН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації
ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
ПРН14. Вирішувати задачі управляння процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.
ПРН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
ПРН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

2. **Програма та структура навчальної дисципліни**

Назви змістових модулів і тем	**Кількість годин**												
	денна форма							**заочна форма**					
	тижні	усього	у тому числі					усього	у тому числі				
			л	п	лаб	інд	с.р.		л	п	лаб	інд	с. р.
Модуль 1. ***Стандарти кібербезпеки.***													
Тема 1. Характеристика стандартів із забезпечення кібербезпеки.	1	14	2	-	2	-	10	-	-	-	-	-	-
Тема 2. Міжнародний стандарт з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).	2	18	4	-	4	-	10	-	-	-	-	-	-
Тема 3. Стандарт ISO/IEC 27002 «Інформаційні технології - Методики безпеки - Практичні правила управління безпекою інформації»	2	18	4	-	4	-	10	-	-	-	-	-	-

Тема 4. Міжнародний стандарт безпеки ISO/IEC 17799.	2	18	4	-	4	-	10	-	-	-	-	-	-
Разом за модулем 1			14	-	14	-	40	-	-	-	-	-	-
Модуль 2 ***Нормативно-правове забезпечення кібербезпеки в зарубіжних країнах та Україні***													
Тема 1 Порівняння підходів за ISO 17799 і BSI.	2	18	4	-	4	-	20	-	-	-	-	-	-
Тема 2. Інформаційна безпека як об'єкт правовідносин.	2	18	4	-	4	-	10	-	-	-	-	-	-
Тема 3. Поняття кібербезпеки, кіберзлочинності та кібертероризму в різних країнах.	2	18	4	-	4	-	10	-	-	-	-	-	-
Тема 4. Основна правова база забезпечення інформаційної та кібернетичної безпеки в Україні.	2	18	4	-	4	-	10	-	-	-	-	-	-
Разом за модулем 2			16	-	16	-	50	-	-	-	-	-	-
Усього годин			**30**	**-**	**30**	**-**	**90**	**-**	**-**	**-**	**-**	**-**	**-**

3. **Теми лекцій**

№ з/п	Назва теми	Кількість годин
1	Характеристика стандартів із забезпечення кібербезпеки.	2
2	Міжнародний стандарт з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).	4
3	Стандарт ISO/IEC 27002 «Інформаційні технології - Методики безпеки - Практичні правила управління безпекою інформації».	4
4	Міжнародний стандарт безпеки ISO/IEC 17799.	4
5	Порівняння підходів за ISO 17799 і BSI.	4
6	Інформаційна безпека як об'єкт правовідносин.	4
7	Поняття кібербезпеки, кіберзлочинності та кібертероризму в різних країнах.	4
8	Основна правова база забезпечення інформаційної та кібернетичної безпеки в Україні.	4
		30

4. **Теми лабораторних (практичних, семінарських) занять**

№ з/п	Назва теми	Кількість годин
1	Вимоги основних міжнародних стандартів у сфері інформаційної безпеки та стан їх впровадження в Україні.	2
2	Міжнародний стандарт з оцінювання безпеки інформаційних технологій (ISO/IEC 15408) на суб'єктах господарювання.	4
3	Порядок вибору заходів безпеки під час впровадження системи управління інформаційною безпекою.	4
4	Реалізація управління інформаційною безпекою на підприємстві, будь-якої форми власності.	4
5	Стандартизація аудиту системи управління інформаційною безпекою на основі стандарту ISO 17799.	4

6	Розподіл відповідальності стосовно забезпечення безпеки. Класифікація та управління інформаційними ресурсами.	4
7	Організаційна робота із захисту інформації з обмеженим доступом в країнах НАТО і ЄС.	4
8	Міжнародні правові інструменти і механізми протидії інформаційним порушенням та кіберзлочинності.	4
		30

5. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Міжнародні правові інструменти і механізми протидії інформаційним порушенням та кіберзлочинності.	10
2	Основні чинники визначення об'єктів інформаційної небезпеки. Основні чинники визначення ієрархії об'єктів інформаційної небезпеки.	10
3	Міжнародні правові інструменти і механізми протидії інформаційним порушенням та кіберзлочинності.	10
4	Характеристика ефективних стандартів з кібербезпеки.	20
5	Оцінювання ефективності існуючої системи захисту ІС на основі стандарту	10
6	Доктринальні та стратегічні нормативно-правові акти України в сфері забезпечення інформаційної безпеки.	10
7	Основні суб`єктивні причини складності правового забезпечення інформаційної безпеки.	10
8	Національна стратегія кібербезпеки Європейського Союзу. Конвенція про кіберзлочинність.	10
		90

6. Методи та засоби діагностики результатів навчання:

- усне або письмове опитування;
- тестування;
- захист індивідуальних проєктів;

7. Методи навчання:

- метод проблемного навчання;
- метод практико-орієнтованого навчання;
- метод проєктного навчання;
- метод навчання через дослідження;
- метод командної роботи, мозкового штурму;

8. Оцінювання результатів навчання.

Оцінювання знань здобувача вищої освіти відбувається за 100-бальною шкалою і переводиться в національну оцінку згідно чинного «Положення про екзамени та заліки у НУБіП України»

8.1. Розподіл балів за видами навчальної діяльності

Вид навчальної діяльності	Результати навчання	Оцінювання
Модуль 1. ***Стандарти кібербезпеки.***		
Тема 1. Характеристика стандартів із забезпечення кібербезпеки.	ПРН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	-
Лабораторна/практична робота 1.		**5**

Вимоги основних міжнародних стандартів у сфері інформаційної безпеки та стан їх впровадження в Україні.	ПРН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.	
Самостійна робота 1. Міжнародні правові інструменти і механізми протидії інформаційним порушенням та кіберзлочинності.	ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. ПРН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. ПРН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. ПРН14. Вирішувати задачі управляння процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. ПРН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.	**5**

	ПРН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.	
Лекція 2. Міжнародний стандарт з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).	ПРН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. ПРН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. ПРН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. ПРН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. ПРН14. Вирішувати задачі управляння процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення	**-**
Лабораторна/практична робота 2. Міжнародний стандарт з оцінювання безпеки інформаційних технологій (ISO/IEC 15408) на суб'єктах господарювання.		**10**
Самостійна робота 2. Основні чинники визначення об’єктів інформаційної небезпеки. Основні чинники визначення ієрархії об’єктів інформаційної небезпеки.		**10**

	щодо захисту та відновлення інформації. ПРН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. ПРН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.	
Лекція 3. Стандарт ISO/IEC 27002 «Інформаційні технології - Методики безпеки - Практичні правила управління безпекою інформації».	ПРН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. ПРН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. ПРН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. ПРН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. ПРН8. Застосовувати знання й розуміння математики та фізики в професійній	**-**
Лабораторна/практична робота 3. Порядок вибору заходів безпеки під час впровадження системи управління інформаційною безпекою.		**10**
Самостійна робота 3. Характеристика ефективних стандартів з кібербезпеки.		**10**

	діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. ПРН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. ПРН14. Вирішувати задачі управляння процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. ПРН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. ПРН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.	
Лекція 4. Міжнародний стандарт безпеки ISO/IEC 17799.	ПРН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	
Лабораторна/практична робота 4. Реалізація управління інформаційною безпекою на підприємстві, будь-якої форми власності.	ПРН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.	**10**
	ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких	**10**

	інших проявів недоброчесності у професійній діяльності. ПРН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. ПРН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. ПРН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. ПРН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. ПРН14. Вирішувати задачі управляння процесами відновлення штатного функціонування інформаційних та	

	інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. ПРН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. ПРН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.	
Модульна контрольна робота 1.		**30**
Всього за модулем 1		**100**
Модуль 2. ***Нормативно-правове забезпечення кібербезпеки в зарубіжних країнах та Україні.***		
Лекція 1. Порівняння підходів за ISO 17799 і BSI.	ПРН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	**-**
Лабораторна/практична робота 1. Стандартизація аудиту системи управління інформаційною безпекою на основі стандарту ISO 17799.	ПРН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.	**10**
Самостійна робота 1. Оцінювання ефективності існуючої системи захисту ІС на основі стандарту.	ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. ПРН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.	**10**

	ПРН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. ПРН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. ПРН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. ПРН14. Вирішувати задачі управляння процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. ПРН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. ПРН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.	

Лекція 2. Інформаційна безпека як об’єкт правовідносин.	ПРН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. ПРН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. ПРН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. ПРН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. ПРН14. Вирішувати задачі управляння процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.	**-**
Лабораторна/практична робота 2. Розподіл відповідальності стосовно забезпечення безпеки. Класифікація та управління інформаційними ресурсами.		**10**
Самостійна робота 2. Доктринальні та стратегічні нормативно-правові акти України в сфері забезпечення інформаційної безпеки.		**10**

	ПРН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. ПРН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.	
Лекція 3. Поняття кібербезпеки, кіберзлочинності та кібертероризму в різних країнах.	ПРН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. ПРН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. ПРН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. ПРН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. ПРН12. Застосовувати методи та засоби	**-**
Лабораторна/практична робота 3. Організаційна робота із захисту інформації з обмеженим доступом в країнах НАТО і ЄС.		**10**
Самостійна робота 3. Основні суб`єктивні причини складності правового забезпечення інформаційної безпеки.		**5**

	захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. ПРН14. Вирішувати задачі управляння процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. ПРН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. ПРН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.	
Лекція 4. Основна правова база забезпечення інформаційної та кібернетичної безпеки в Україні.	ПРН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	**-**
Лабораторна/практична робота 4. Міжнародні правові інструменти і механізми протидії інформаційним порушенням та кіберзлочинності.	ПРН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.	**10**
Самостійна робота 4. Національна стратегія кібербезпеки Європейського Союзу. Конвенція про кіберзлочинність.	ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. ПРН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН6. Адаптуватися до нових умов і	**5**

	технологій професійної діяльності, прогнозувати кінцевий результат. ПРН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. ПРН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. ПРН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. ПРН14. Вирішувати задачі управляння процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. ПРН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. ПРН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації,	

	зокрема відповідно до вимог нормативних документів.	
Модульна контрольна робота 2.		**30**
Всього за модулем 2		**100**
Навчальна робота		**(М1 + М2)/2*0,7 ≤ 70**
Екзамен/залік		**30**
Всього за курс		**(Навчальна робота + екзамен) ≤ 100**

8.2. Шкала оцінювання знань здобувача вищої освіти

Рейтинг здобувача вищої освіти, бали	Оцінка за національною системою (екзамени/заліки)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

8.3. 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 девайсів). Курсові роботи, реферати повинні мати коректні текстові посилання на використану літературу
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)

9. Навчально-методичне забезпечення:

- електронний навчальний курс навчальної дисципліни (на навчальному порталі НУБіП України eLearn - *https://elearn.nubip.edu.ua/course/)*;
- посилання на цифрові освітні ресурси;
- підручники, навчальні посібники, практикуми;
- методичні матеріали щодо вивчення навчальної дисципліни для здобувачів вищої освіти денної та заочної форм здобуття вищої освіти.

10. Рекомендовані джерела інформації

1. *Інформаційний бюлетень "Біла книга 2021. Оборонна політика України " підготовлений робочою групою фахівців Міністерства оборони України, Генерального штабу Збройних Сил України та Адміністрації Державної спеціальної служби транспорту URL: https://www.mil.gov.ua/content/files/whitebook/WhiteBook_2021_Draft_Final_03.pdf (дата звернення 02.06.2025р.)*
2. *ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення». URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69175 (дата звернення 02.06.2025р.)*
3. *ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт». URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69173 (дата звернення 02.06.2025р.)*

4. *ДСТУ ISO/IEC 27000:2015 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник». URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=66893 (дата звернення 02.06.2025р.)*
5. *ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги». URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910 (дата звернення 02.06.2025р.)*
6. *ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки». URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=85805 (дата звернення 02.06.2025р.)*
7. *ДСТУ ISO/IEC 27003:2018 «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою». URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=78517 (дата звернення 02.06.2025р.)*
8. *ДСТУ ISO/IEC 27005:2011 «Інформаційні технології. Методи захисту. Менеджмент ризику інформаційної безпеки». URL: https://zakon.rada.gov.ua/rada/show/v0312774-19#Text (дата звернення 02.06.2025р.)*
9. *ДСТУ ISO/IEC 15408-1:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель». URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104382 (дата звернення 02.06.2025р.)*
10. *ДСТУ ISO/IEC 15408-2:2022 «Інформаційні технології. Методи захисту. Критерії оцінювання. Частина 2. Функціональні вимоги». URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=102013 (дата звернення 02.06.2025р.)*
11. *ДСТУ ISO/IEC 15408-3:2022 «Інформаційні технології. Методи захисту. Критерії оцінювання. Частина 3. Вимоги до гарантії безпеки». URL: https://online.budstandart.com/ru/catalog/doc-page?id_doc=101798 (дата звернення 02.06.2025р.)*
12. *НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». URL: https://tzi.ua/ua/nd_tz_2.5-004-99.html (дата звернення 02.06.2025р.)*
13. *НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу». URL: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024 (дата звернення 02.06.2025р.)*
14. *Загальні рекомендації Державного центру кіберзахисту та протидії кіберзагрозам Держспецзв'язку для підвищення рівня захисту інформаційних ресурсів та систем і для запобігання кіберінцидентам в установах, на підприємствах і в організаціях. URL: https://www.kmu.gov.ua/news/250099405 (дата звернення 02.06.2025р.)*
15. *Конвенція про кіберзлочинність від 23 листопада 2001 року. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення 02.06.2025р.)*
16. *Конценція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 року, № 1009-р. URL: http://zakon2.rada.gov.ua/laws/show/1009- 2017-р (дата звернення 02.06.2025р.)*
17. *Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 07 листопада 2018 року, № 2155-VIII. Відомості Верховної Ради України (ВВР). 2006. № 30*
18. *Про державну таємницю : Закон України від 21 січня 1994 року, № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення 02.06.2025р.)*
19. *Мамченко С.М. Комплексні системи захисту інформації: навчальний посібник / С.М.Мамченко, Козюра В.Д., Бровко В.Д. – К.: Нац. акад. СБУ, 2018. – 361 с.*
20. *Lakhno V., Kasatkin D.Yu., Dubovyk O., Kryvoruchko O., Desiatko A., Chubaievskyi V. Tutorial «Methods and means of information protection» - K .: NPE Yamchynskyi O.V., 2022. - 267 p. ISBN 978-617-8184-30-8*
21. *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. URL: https://spadok.org.ua/books/Buryachok-Osnovy-info-ta-ciberbezpeky.pdf (дата звернення 02.06.2025р.)*

22. *Луцький М.Г., Хорошко В.О., Хохлачова Ю.Є., Козловський В.В., Баланюк Ю.В., Прав Ю.Г. Новітні технології захисту інформації: підручник. К.: НАУ, 2023 - 312 с.*
23. *Браіловський М.М., Зибін С.В., Кобозєва А.А., Хорошко В.О., Хохлачова Ю.Є. Аналіз кіберзахищеності інформаційних систем Київ: ФОП Ямчинський О.В. 2021. 360 с.*
24. *Хорошко О.В. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с. ISBN 978-966-629-970-6*
25. *Остапов С. Е., Євсеєв С. П., Король О.Г. Кібербезпека : сучасні технології захисту: навчальний посібник. Львів: Новий Світ-2000, 2020. URL: https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf (дата звернення 02.06.2025р.)*
26. *Ананьїн В. О. Національна безпека держави в сучасних умовах: монографія / В.О. Ананьїн, О. В. Ананьїн, В. В. Горлинський; за загальною редакцією В.О. Ананьїна. – К.: КПІ ім. Ігоря Сікорського, 2021. – 345 с.*
27. *Ситник Г. П., Орел М. Г. Національна безпека в контексті європейської інтеграції України: підручник / Г. П. Ситник, М. Г. Орел; за ред. Г. П. Ситника. – К.: Міжрегіональна Академія управління персоналом, 2021. – 372 с.*
28. *Гулак Г.М., Жильцов О.Б., Складанний П.М., Киричок Р.В., Коршун Н.В. Інформаційна та кібернетична безпека підприємства / Навчальний підручник. КУБГ. – К. 2022. 451с.*