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

«Управління проєктами розробки систем захисту інформації»

Галузь знань F Інформаційні технології

Спеціальність F5 Кібербезпека та захист інформації

Освітня програма «Кібербезпека»

Факультет (ННІ) інформаційних технологій

Розробники: професор, д.т.н., професор, Криворучко О.В.,

професор, д.т.н., професор, Лахно В.А.

(посада, науковий ступінь, вчене звання)

Київ – 2025 р.

Опис навчальної дисципліни "***Управління проєктами розробки систем захисту інформації***"
Навчальна дисципліна передбачає забезпечити засвоєння основних теоретичних, методичних та організаційних основ проектного менеджменту; дати можливість оволодіти методами управління проєктами (УП розробки СЗІ) на всіх фазах життєвого циклу проєкту СЗІ; виробити вміння застосовувати інструменти методології УП в діяльності, пов'язаній з СЗІ; навчити студентів виділяти і аналізувати проєкти, які пов'язані із розробкою СЗІ різних типів з метою побудови ефективних способів розробки та супроводу комплексних систем захисту інформації об'єктів інформаційної 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**

Метою вивчення дисципліни "Управління проєктами розробки систем захисту інформації" є формування у майбутніх фахівців необхідного рівня професійних знань з управління проєктами, який визначається у світовій практиці у формі "Project Management Body of Knowledge" (PMBOK), набуття практичних навичок використання основ знань з управління проєктами розробки систем захисту інформації для розв'язання різних задач у роботі за фахом.

Набуття компетентностей:

інтегральна компетентність (ІК):

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в галузі забезпечення інформаційної безпеки та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

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.
ЗК4. Здатність спілкуватися іноземною мовою.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
ЗК8. Здатність зберігати та приумножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя..
спеціальні (фахові) компетентності (СК):
СК1 Здатність застосовувати законодавчу та нормативно- правову 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.
СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)
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):
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.
ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

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. ***Проєкт і сутність проєктної діяльності. Типи проєктів.***													
Тема1 Проєкти: визначення і класифікація. Теоретико-методичні засади управління проєктами.	1	18	4	-	4	-	10	-	-	-	-	-	-
Тема 2. Організація проєктно-орієнтованої	2	18	4	-	4	-	10	-	-	-	-	-	-

діяльності.													
Тема 3. Функції та елементи управління проєктами розробки систем захисту інформації	2	18	4	-	4	-	10	-	-	-	-	-	-
Тема 4. Стандарти організації життєвих циклів проєктів інформатизації.	2	18	4	-	4	-	10	-	-	-	-	-	-
Разом за модулем 1			16	-	16	-	40	-	-	-	-	-	-
Модуль 2 ***Особливості управління проєктами розробки систем захисту інформації***													
Тема 1 Управління змістом (предметною областю) проєктів розробки систем захисту інформації.	2	18	4	-	4	-	20	-	-	-	-	-	-
Тема 2. Учасники і оточення проєкту розробки систем захисту інформації. Лідерство в управлінні проєктами.	2	18	4	-	4	-	10	-	-	-	-	-	-
Тема 3. Інформаційні та програмно-апаратні засоби управління проєктами. Мультипроєктне управління в проєктах розробки систем захисту інформації.	2	18	4	-	4	-	10	-	-	-	-	-	-
Тема 4. Інструментарій грантового фінансування в реалізації проєктів розробки систем захисту інформації.	2	14	2	-	2	-	10	-	-	-	-	-	-
Разом за модулем 2			14	-	14	-	50	-	-	-	-	-	-
Усього годин			**30**	**-**	**30**	**-**	**90**	**-**	**-**	**-**	**-**	**-**	**-**

3. **Теми лекцій**

№ з/п	Назва теми	Кількість годин
1	Проєкти: визначення і класифікація. Теоретико-методичні засади управління проєктами.	4
2	Організація проєктно-орієнтованої діяльності.	4
3	Функції та елементи управління проєктами розробки систем захисту інформації.	4
4	Стандарти організації життєвих циклів проєктів інформатизації.	4
5	Управління змістом (предметною областю) проєктів розробки систем захисту інформації	4
6	Учасники і оточення проєкту розробки систем захисту інформації. Лідерство в управлінні проєктами.	4

7	Інформаційні та програмно-апаратні засоби управління проєктами. Мультипроєктне управління в проєктах розробки систем захисту інформації.	4
8	Інструментарій грантового фінансування в реалізації проєктів розробки систем захисту інформації.	2
		30

4. Теми лабораторних (практичних, семінарських) занять

№ з/п	Назва теми	Кількість годин
1	Сутність управління проєктами розробки систем захисту інформації. Класифікація проєктів.	4
2	Основні задачі та правила структуризації проєкту розробки систем захисту інформації. Технологія процесу структуризації проекту (послідовність дій).	4
3	Життєвий цикл проєкту розробки систем захисту інформації.	4
4	Стандарти життєвих циклів систем захисту інформації.	4
5	Загальні підходи до планування проєктів розробки систем захисту інформації. Сіткове і календарне планування проєкту проєкту розробки систем захисту інформації.	4
6	Лідерство, командна робота та взаємодії в управлінні проєктом розробки систем захисту інформації.	4
7	Особливості програми Microsoft Project та GanttPro.	4
8	Вигоди і перешкоди запровадження аутсорсингу в проєкті розробки систем захисту інформації.	2
		30

5. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Стан та перспективи застосування методології управління проєктами в Україні. Сутність системи управління проєктами розробки систем захисту інформації, її елементи.	10
2	Формування ідеї проєкту розробки систем захисту інформації. Безкоштовний модуль на платформі Prometheus «IT-продукт з нуля: з чого розпочати та як розвивати?» https://prometheus.org.ua/course/course-v1:Prometheus+IT101+2022_T1	10
3	Характеристика видів діяльності, які є основною діяльністю щодо проекту, а також видів діяльності, які стосуються забезпечення проєкту розробки систем захисту інформації.	10
4	Стан та перспективи застосування методології управління проектами інформатизації в Україні. Визначте поняття, якими оперує стандарт ISO–9000.	20
5	Структурні моделі проєкту: RBS (resource brakedown structure) – розподіл робіт по виконавцям; BOM (bill of materials) –структура матеріальних ресурсів; PBS (project brake structure) - проєктна структурна робіт	10
6	Безкоштовний модуль на платформі Prometheus «Основи управління командами та проєктами в IT. Підготовчий». https://prometheus.org.ua/course/course-v1:LITS+ITPM101+FREE_2021_T1	10
7	Програмне забезпечення для управління проєктами: FlexiProject, Wrike, Planview, Monday.com, Trello, BlueAnt.	10
8	Модуль Маркетинг IT-продуктів (курс Genesis) https://www.genesis-for-univ.com/marketing-course	10

	Лінк на курс надається викладачем на початку вивчення дисципліни – курс безкоштовний, але кожен студент отримує індивідуальний код авторизації.	
		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. ***Проєкт і сутність проєктної діяльності. Типи проєктів.***		
Тема 1. Проєкти: визначення і класифікація. Теоретико-методичні засади управління проєктами.	ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.	-
Лабораторна/практична робота 1. Сутність управління проєктами розробки систем захисту інформації. Класифікація проєктів.	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. ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.	**5**
Самостійна робота 1. Стан та перспективи застосування методології управління проєктами в Україні. Сутність системи управління проєктами розробки систем захисту інформації, її елементи.		**5**
Лекція 2. Організація проєктно-орієнтованої діяльності.	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. ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі	-
Лабораторна/практична робота 2. Основні задачі та правила структуризації проєкту розробки систем захисту інформації. Технологія процесу структуризації проекту (послідовність дій).		**10**
Самостійна робота 2. Формування ідеї проєкту розробки систем захисту інформації. Безкоштовний модуль на платформі		**10**

Prometheus «IT-продукт з нуля: з чого розпочати та як розвивати?» https://prometheus.org.ua/course/course-v1:Prometheus+IT101+2022_T1	встановленою політикою кібербезпеки з урахування вимог до захисту інформації.	
Лекція 3. Функції та елементи управління проєктами розробки систем захисту інформації.	ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.	**-**
Лабораторна/практична робота 3. Життєвий цикл проєкту розробки систем захисту інформації	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. ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.	**10**
Самостійна робота 3. Характеристика видів діяльності, які є основною діяльністю щодо проекту, а також видів діяльності, які стосуються забезпечення проєкту розробки систем захисту інформації.		**10**
Лекція 4. Стандарти організації життєвих циклів проєктів інформатизації.	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. ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.	
Лабораторна/практична робота 4. Стандарти життєвих циклів систем захисту інформації.		**10**
Самостійна робота 4. Стан та перспективи застосування методології управління проектами інформатизації в Україні. Визначте поняття, якими оперує стандарт ISO–9000.		**10**
Модульна контрольна робота 1.		**30**
Всього за модулем 1		**100**
Модуль 2. ***Особливості управління проєктами розробки систем захисту інформації.***		
Лекція 1. Управління змістом (предметною областю) проєктів розробки систем захисту інформації.	ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.	**-**
Лабораторна/практична робота 1. Загальні підходи до планування проєктів розробки систем захисту інформації. Сіткове і календарне планування проєкту проєкту розробки систем захисту інформації.	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.	**10**
Самостійна робота 1. Структурні моделі проєкту: RBS (resource brakedown structure) – розподіл робіт по виконавцям; BOM	ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з	**10**

(bill of materials) –структура матеріальних ресурсів; PBS (project brake structure) - проєктна структурна робіт.	урахування вимог до захисту інформації.	
Лекція 2. Учасники і оточення проєкту розробки систем захисту інформації. Лідерство в управлінні проєктами.	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. ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.	**-**
Лабораторна/практична робота 2. Лідерство, командна робота та взаємодії в управлінні проєктом розробки систем захисту інформації.		**10**
Самостійна робота 2. Безкоштовний модуль на платформі Prometheus «Основи управління командами та проєктами в IT. Підготовчий». https://prometheus.org.ua/course/course-v1:LITS+ITPM101+FREE_2021_T1		**10**
Лекція 3. Інформаційні та програмно-апаратні засоби управління проєктами. Мультипроєктне управління в проєктах розробки систем захисту інформації.	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. ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.	**-**
Лабораторна/практична робота 3. Особливості програми Microsoft Project та GanttPro.		**10**
Самостійна робота 3. Програмне забезпечення для управління проєктами: FlexiProject, Wrike, Planview, Monday.com, Trello, BlueAnt.		**5**
Лекція 4. Інструментарій грантового фінансування в реалізації проєктів розробки систем захисту інформації.	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. ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.	**-**
Лабораторна/практична робота 4. Вигоди і перешкоди запровадження аутсорсингу в проєкті розробки систем захисту інформації.		**10**
Самостійна робота 4. Модуль Маркетинг IT-продуктів (курс Genesis) https://www.genesis-for-univ.com/marketing-course *Лінк на курс надається викладачем на початку вивчення дисципліни – курс безкоштовний, але кожен студент отримує індивідуальний код авторизації.*		**5**
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/enrol/index.php?id=5212*);
- 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. *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.)*
2. *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.)*
3. *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.)*
4. *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.)*
5. *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.)*

6. *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.)*
7. *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.*
8. *Катренко А.В. «Управління ІТ-проєктами. Підручник. Книга 1. Стандарти, моделі та методи управління проєктами» (Львів: Новий Світ-2000, 2024, 550 с., ISBN 978-966-418-148-5) – ґрунтовне видання про цикли життя, методи та інструменти управління ІТ-проєктами (ns2000.com.ua). Це останнє перевидання першої книги (2025 за технічним релізом).*
9. *Моделювання бізнес-процесів та управління ІТ-проектами: навчальний посібник [Електронний ресурс] / Є. М. Крижановський, А.Р. Яцолт, С.О. Жуков, О. М. Козачко – Вінниця : ВНТУ, 2018. – (PDF, 91 с.) https://pdf.lib.vntu.edu.ua/books/2023/Kryzhanov_2022_129.pdf*
10. *Катренко А.В. Управління ІТ-проектами. [Книга 1. Стандарти, моделі та методи управління проектами]:[підручник]. – Львів: «Новий світ – 2000», 2018. - 550 с.*
11. *Загородніх О.А., Ліщинська В.В. Управління проектами: Навч. посібник. – К.: КНЕУ, 2003. – 531 с.*