ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ

Кафедра інформаційних систем та технологій

ЗАТВЕРДЖЕНО КАФЕДРОЮ

Завідувач кафедри

_____ Юрій УТКІН

(протокол «01» вересня 2025 р. №2)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(обов'язкова навчальна дисципліна)

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

(назва навчальної дисципліни)

освітньо-професійна програма «Інформаційні управляючі системи»

спеціальність 126 Інформаційні системи та технології

галузь знань 12 Інформаційні технології

рівень вищої освіти перший (бакалаврський)

навчально-науковий інститут економіки, управління, права та інформаційних технологій

Полтава

2025– 2026 н.р.

Робоча програма навчальної дисципліни «Безпека інформаційних систем»_для здобувачів вищої освіти за освітньо-професійною програмою «Інформаційні управляючі системи» спеціальності 126 Інформаційні системи та технології

Мова викладання: державна

Розробники: Юрій Поночовний, професор кафедри інформаційних систем та технологій, д.т.н., професор
Олександр Тищенко, асистент кафедри інформаційних систем та технологій

«01» вересня 2025 року _____ Юрій ПОНОЧОВНИЙ

«01» вересня 2025 року _____ Олександр ТИЩЕНКО

Погоджено гарантом освітньої програми
«Інформаційні управляючі системи»

«01» вересня 2025 року _____ Олена КОПІШИНСЬКА

Схвалено радою з якості вищої освіти
спеціальності «Інформаційні системи і технології»

протокол «01»вересня 2025 року № 1

Голова ради з якості вищої освіти
спеціальності «Інформаційні системи і технології»

_____ Олена КОПІШИНСЬКА

1. Опис навчальної дисципліни

Елементи характеристики	Денна форма здобуття освіти, 126ІСТ бд 2022	Заочна форма здобуття освіти, 126ІСТ бз 2022
Загальна кількість годин	90	90
Кількість кредитів	3	3
Місце в індивідуальному навчальному плані здобувача вищої освіти	обов‘язкова	обов‘язкова
Рік навчання	4	3; 4
Семестр	8	6; 7
Лекції (годин)	16	2; 6
Лабораторні заняття (годин)	16	0; 8
Самостійна робота (годин)	58	74
у т. ч. індивідуальні завдання (контрольна робота) (годин)	–	24
Форма семестрового контролю	екзамен	екзамен

2. Мета вивчення навчальної дисципліни

Формування у студентів комплексних знань, умінь і навичок для проектування, впровадження та управління системами інформаційної безпеки в інформаційних системах і мережах, з акцентом на застосування сучасних методів захисту даних, конфігурування засобів безпеки та розробку ефективних стратегій протидії кіберзагрозам у професійній діяльності.

3. Передумови для вивчення навчальної дисципліни

Перелік дисциплін, які передують її вивченню відповідно до структурно-логічної схеми освітньо-професійної програми: «Безпека життєдіяльності та основи охорони праці», «Вступ до інформаційних технологій», Курсова робота «Комп'ютерні мережі», «Паралельні та розподілені обчислення», «Програмні технології Інтернет речей».

4. Компетентності

Загальні:

КЗ 1. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ 2. Здатність застосовувати знання у практичних ситуаціях.

КЗ 3. Здатність до розуміння предметної області та професійної діяльності.

КЗ 5. Здатність вчитися і оволодівати сучасними знаннями.

КЗ 6. Здатність до пошуку, оброблення та узагальнення інформації з різних джерел.

Спеціальні (фахові):

КС 1. Здатність аналізувати об’єкт проектування або функціонування та його предметну область.

КС 2. Здатність застосовувати стандарти в області інформаційних систем та технологій при розробці функціональних профілів, побудові та інтеграції систем, продуктів, сервісів і елементів інфраструктури організації.

КС 3. Здатність до проектування, розробки, налагодження та вдосконалення системного, комунікаційного та програмно- апаратного забезпечення інформаційних систем та технологій, Інтернету речей (IoT), комп’ютерно-інтегрованих систем та системної мережної структури, управління ними.

КС 4. Здатність проектувати, розробляти та використовувати засоби реалізації інформаційних систем, технологій та інфокомунікацій (методичні, інформаційні, алгоритмічні, технічні, програмні та інші)

КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов’язків.

КС 7. Здатність застосовувати інформаційні технології у ході створення, впровадження та експлуатації системи менеджменту якості та оцінювати витрати на її розроблення та забезпечення.

КС 8. Здатність управляти якістю продуктів і сервісів інформаційних систем та технологій протягом їх життєвого циклу.

КС 11. Здатність до аналізу, синтезу і оптимізації інформаційних систем та технологій з використанням математичних моделей і методів.

КС 12. Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет).

КС 15. Здатність проводити заходи щодо організації робочих місць, їх технічного оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів організаційно-управлінської діяльності.

5. Результати навчання

ПР 3. **Використовувати** базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп’ютерних програм мовами високого рівня із застосуванням об’єктно-орієнтованого програмування для розв’язання задач проектування і використання інформаційних систем та технологій.

ПР 5. **Аргументувати** вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.

ПР 6. **Демонструвати** знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп’ютерних систем та середовищ з метою їх запровадження у професійній діяльності.

ПР 9. **Здійснювати** системний аналіз архітектури підприємства та його ІТ-інфраструктури, проводити розроблення та вдосконалення її елементної бази і структури.

ПР 13. **Виявляти** здатність до генерації нових ідей і варіантів розв’язання задач, до комбінування та експериментування, до оригінальності, конструктивності, економічності та простих рішень.

ПР 14. **Застосовувати** методи і засоби підтримки командної роботи, планування та ефективної організації праці, безперервного контролю якості результатів роботи, соціальної комунікації.

Співвідношення програмних результатів навчання із очікуваними результатами навчання

Програмний результат навчання (визначений освітньою програмою)	Очікувані результати навчання навчальної дисципліни
ПР 3. **Використовувати** базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.	Здатність застосовувати технології безпечної роботи в комп'ютерних мережах, включаючи протидію несанкціонованому доступу, фільтрацію трафіку та міжмережеве екранування на різних рівнях моделі OSI, для розв'язання задач захисту інформаційних систем. Вміння використовувати методи створення захищених віртуальних мереж (VPN) з застосуванням протоколів PPTP, L2TP, IPSec, SSL та Socks для забезпечення безпечної передачі даних в інтернет-ресурсах і корпоративних системах.
ПР 5. **Аргументувати** вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.	Вміння аргументувати вибір систем FireWall на основі аналізу їх властивостей, переваг, недоліків, підтримки платформ та ефективності управління для забезпечення захисту інформаційних систем. Навички налагодження та тестування засобів безпеки, таких як брандмауери, VPN-тунелі та протоколи розподілу ключів (SKIP, ISAKMP), з урахуванням вимог до системи та експлуатаційних умов.
ПР 6. **Демонструвати** знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп'ютерних систем та середовищ з метою їх запровадження у професійній діяльності.	Демонструвати знання сучасних технологій безпеки, включаючи IPv4 та IPv6, моделі загроз, а також практичні навички конфігурування FireWall і VPN для запровадження в інформаційних системах. Вміння застосовувати спеціалізовані середовища для розподілу криптографічних ключів та узгодження параметрів захищених каналів (протоколи SKIP, ISAKMP) у професійній діяльності з безпеки.
ПР 9. **Здійснювати** системний аналіз архітектури підприємства та його IT- інфраструктури, проводити розроблення та вдосконалення її елементної бази і структури.	Здатність проводити системний аналіз загроз безпеки корпоративних інформаційних систем та мереж, включаючи моделі загроз, потенційні загрози для електронного бізнесу та шляхи їх розв'язання. Вміння розробляти та вдосконалювати елементну базу IT-інфраструктури через побудову підсистеми інформаційної безпеки, експертизу захищеності та проектування комп'ютерних систем у захищеному виконанні.
ПР 13. **Виявляти** здатність до генерації нових ідей і варіантів розв'язання задач, до комбінування та експериментування, до оригінальності, конструктивності, економічності та простих рішень.	Здатність генерувати оригінальні ідеї для розв'язання проблем безпеки електронного бізнесу та корпоративних систем, комбінуючи методи фільтрації трафіку, тунелювання та криптографії для економічних і простих рішень. Вміння експериментувати з варіантами реалізації функцій підсистеми безпеки, включаючи узгодження параметрів захищених каналів та розподіл ключів, для конструктивного вдосконалення IT-інфраструктури.
ПР 14. **Застосовувати** методи і засоби підтримки командної роботи, планування та ефективної організації праці, безперервного контролю якості результатів роботи, соціальної комунікації.	Здатність застосовувати методи планування та організації праці для розробки концепції і політики інформаційної безпеки, включаючи експертизу та сертифікацію засобів захисту інформації. Вміння забезпечувати командну роботу та контроль якості при конфігуруванні систем FireWall і VPN, з урахуванням схем підключення та критеріїв оцінки для ефективної соціальної комунікації в проектах безпеки.

6. Методи навчання і викладання

1. Методи організації та здійснення навчально-пізнавальної діяльності:

– словесні методи: лекція, інструктаж;

– наочні методи: демонстрування;

– практичні методи: лабораторні роботи.

2. Методи стимулювання і мотивації навчально-пізнавальної діяльності:

– методи формування пізнавальних інтересів: метод використання життєвого досвіду; метод відповідей на запитання і опитування думок здобувачів вищої освіти;

– методи стимулювання і мотивації обов'язку й відповідальності: роз’яснення мети навчальної дисципліни; висування вимог до вивчення дисципліни; заохочення і покарання; оперативний контроль; вказування на недоліки, зауваження.

3. Інноваційні та інтерактивні методи навчання:

– комп’ютерні, мультимедійні методи: використання мультимедійних презентацій; використання комп’ютерних навчальних програм.

4. Методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності:

– методи письмового контролю: контрольна робота (для заочної форми навчання);

– методи лабораторно-практичного контролю: перевірка виконання завдань лабораторних робіт;

– методи самоконтролю: самостійний пошук помилок.

7. Програма навчальної дисципліни:

Тема 1. Проблеми безпеки в Інтернет. Електронний бізнес і проблеми безпеки. Основні моделі електронної комерції. Здійснення електронних платежів через Інтернет. Потенційні загрози для електронного бізнесу. Шляхи розв`язання проблем безпеки електронного бізнесу.

Тема 2. Проблеми безпеки корпоративних інформаційних систем. Основні поняття інформаційної безпеки. Проблеми безпеки IP-мереж. IP версія 4. IP версія 6. Аналіз загроз безпеки інформаційних систем та мереж. Модель загроз безпеки.

Тема 3. Побудова підсистеми інформаційної безпеки. Експертиза захищеності комп`ютерної системи. Розробка концепції і політики інформаційної безпеки. Проектування комп`ютерної системи в захищеному виконанні. Варіанти реалізації основних функцій підсистеми інформаційної безпеки комп`ютерної системи. Експертиза та сертифікат ЗЗІ.

Тема 4. Принципи інформаційної безпеки. Протидія несанкціонованому міжмережевому доступу. Фільтрація трафіку. Виконання функцій посередництва. Особливості міжмережевого екранування на різних рівнях моделі OSI. Екранний маршрутизатор. Шлюз сеансового рівня. Прикладний шлюз.

Тема 5. Встановлення і конфігурування систем FireWall. Розробка політики міжмережевої взаємодії. Визначення схеми підключення міжмережевого екрану. Настройка параметрів функціонування брандмауера. Критерії оцінки міжмережевих екранів. Сучасні системи FireWall. Переваги і недоліки. Підтримка різних платформ і режимів роботи. Ефективність управління. Підтримка функцій захисту.

Тема 6. Побудова захищених віртуальних мереж VPN. Способи створення захищених віртуальних каналів. Захищені віртуальні канали. Тунелювання на канальному рівні. Протокол PPTP. Протокол L2F. Протокол L2TP. Захист віртуальних каналів на мережевому рівні. Архітектура засобів безпеки IPSec. Протокол заголовку аутентифікації. Протокол інкапсульованого захисту. Управління захищеним тунелем. Захищені віртуальні канали на сеансовому рівні. Протокол SSL. Протокол Socks.

Тема 7. Розподіл криптографічних ключів. Узгодження параметрів захищеного каналу. Протокол SKIP. Розподіл криптографічних ключів. Протокол ISAKMP. Узгодження параметрів кожного захищеного з`єднання.

Структура (тематичний план) навчальної дисципліни

Назви тем	Кількість годин							
	Денна форма здобуття освіти 126ІСТ_бд_2022				Заочна форма здобуття освіти 126ІСТ_бз_2022			
	усього	у тому числі			усього	у тому числі		
		л	лаб	с.р.		л	лаб	с.р.
Тема 1. Проблеми безпеки в Інтернет	**14**	4	2	8	**15**	2	2	11
Тема 2. Проблеми безпеки корпоративних інформаційних систем.	**12**	2	2	8	**15**	2	2	11
Тема 3. Побудова підсистеми інформаційної безпеки.	**12**	2	2	8	**15**	2	2	11
Тема 4. Принципи інформаційної безпеки.	**12**	2	2	8	**13**	2	0	11
Тема 5. Встановлення і конфігурування систем FireWall.	**12**	2	2	8	**10**	0	0	10
Тема 6. Побудова захищених віртуальних мереж VPN.	**13**	2	2	9	**10**	0	0	10
Тема 7. Розподіл криптографічних ключів	**15**	2	4	9	**12**	0	2	10
у т.ч. індивідуальні завдання: *контрольна робота*	-	-		-		-	-	**24**
Усього годин	**90**	**16**	**16**	**58**	**90**	**8**	**8**	**74**

8. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма здобуття освіти 126ІСТ_бд_2022	Заочна форма здобуття освіти 126ІСТ_бз_2022
1	Робота з обліковими записами користувачів і груп ОС Windows Server. Встановлення правил доступу до об’єктів файлової системи	2	2
2	Використання теорії чисел для захисту інформації	2	2
3	Організація безпеки локальної мережі при використанні утиліт, що реалізують моніторинг трафіка	2	2
4	Організація безпеки механізму аутентифікації при перехопленні парольних хешей і їхньої розшифровки	2	0
5	Налаштовування та адміністрування міжмережних екранів	2	0
6	Методика побудови захищеної телекомунікаційної мережі із використанням VPN	2	0
7	Криптографічні методи захисту даних:	4	2
Усього годин		**16**	**8**

9. Теми самостійної роботи

Назви тем	Кількість годин	
	Денна форма здобуття освіти 126ІСТ_бд_2022	Заочна форма здобуття освіти 126ІСТ_бз_2022
Тема 1. Проблеми безпеки в Інтернет	8	11
Тема 2. Проблеми безпеки корпоративних інформаційних систем.	8	11
Тема 3. Побудова підсистеми інформаційної безпеки.	8	11
Тема 4. Принципи інформаційної безпеки.	8	11
Тема 5. Встановлення і конфігурування систем FireWall.	8	10
Тема 6. Побудова захищених віртуальних мереж VPN.	9	10
Тема 7. Розподіл криптографічних ключів	9	10
у т. ч. індивідуальні завдання (контрольна робота) (годин)		24
Усього годин	**58**	**74**

10. Індивідуальні завдання

Індивідуальна робота здобувача вищої освіти направлена на закріплення теоретичного матеріалу та практичних навичок. Реалізація даного виду роботи передбачається шляхом виконання індивідуального навчального завдання – контрольної

роботи, яке виконується здобувачами вищої освіти заочної форми навчання в позааудиторний час. Перевірка результатів контрольної роботи студентів викладачем відбувається до початку та під час екзаменаційної сесії.

11. Оцінювання результатів навчання

Програмні результати навчання	Форми контролю
ПР 3. **Використовувати** базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.	Для поточного контролю: - розв'язування тестів; - виконання лабораторних робіт; - виконання завдань самостійної роботи; - контрольна робота*; Для семестрового контролю: - екзамен;
ПР 5. **Аргументувати** вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.	
ПР 6. **Демонструвати** знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп'ютерних систем та середовищ з метою їх запровадження у професійній діяльності.	
ПР 9. **Здійснювати** системний аналіз архітектури підприємства та його ІТ- інфраструктури, проводити розроблення та вдосконалення її елементної бази і структури.	
ПР 13. **Виявляти** здатність до генерації нових ідей і варіантів розв'язання задач, до комбінування та експериментування, до оригінальності, конструктивності, економічності та простих рішень.	
ПР 14. **Застосовувати** методи і засоби підтримки командної роботи, планування та ефективної організації праці, безперервного контролю якості результатів роботи, соціальної комунікації.	

* Форма контролю, яка застосовується лише для заочної форми навчання

Критерієм успішного навчання є досягнення здобувачем вищої освіти мінімальних порогових рівнів оцінок за кожним результатом навчання. Мінімальний пороговий рівень оцінки за кожним результатом навчання становить 60 % від максимально можливої кількості балів. Мінімальний пороговий рівень оцінки з освітнього компонента є єдиним в Університеті і не залежить від форм контролю і методів оцінювання результатів навчання.

Схема нарахування балів з навчальної дисципліни

Денна форма здобуття освіти 126ICT_бд_2022

Назва теми	Форми контролю результатів навчання здобувачів вищої освіти			Разом
	розв'язування тестів	виконання лабораторних робіт	виконання завдань самостійної роботи	
Тема 1. Проблеми безпеки в Інтернет		7	1	8
Тема 2. Проблеми безпеки корпоративних інформаційних систем.		7	1	8
Тема 3. Побудова підсистеми інформаційної безпеки.		7	1	8
Тема 4. Принципи інформаційної безпеки.		7	1	8
Тема 5. Встановлення і конфігурування систем FireWall.		7	1	8
Тема 6. Побудова захищених віртуальних мереж VPN.		7	1	8
Тема 7. Розподіл криптографічних ключів	24	7	1	32
Разом балів за темами	**24**	**49**	**7**	80
Екзамен				20
Разом				**100**

Схема нарахування балів з навчальної дисципліни

Заочна форма здобуття освіти 126ICT_бз_2022

Назва теми	Форми контролю результатів навчання здобувачів вищої освіти				Разом
	Розв'язування тестів	Виконання лабораторних робіт	Виконання завдань самостійної роботи	Контрольна робота	
Тема 1. Проблеми безпеки в Інтернет		7	1		8
Тема 2. Проблеми безпеки корпоративних інформаційних систем.		7	1		8
Тема 3. Побудова підсистеми інформаційної безпеки.		7	1		8
Тема 4. Принципи інформаційної безпеки.			1		1
Тема 5. Встановлення і конфігурування систем FireWall.			1		1
Тема 6. Побудова захищених віртуальних мереж VPN.			1		1
Тема 7. Розподіл криптографічних ключів	15	7	1		53
у т.ч. індивідуальне завдання: **контрольна робота**				30	30
Разом балів за темами та видами	**15**	**28**	**7**		**80**
Екзамен					**20**
Разом балів за дисципліну					***100***

Шкала та критерії оцінювання

Денна та заочна форма здобуття освіти 126ІСТ_бд_2022, 126ІСТ_бз_2022

Виконання лабораторних робіт

Кількість балів	Критерії оцінювання
7 балів (максимальна)	Досягнення мети лабораторної роботи у повному обсязі запланованих результатів навчання, здобувач навів правильні відповіді на всі контрольні питання та продемонстрував вміння роботи на ПК із відповідним програмним продуктом
6 балів	завдання лабораторної роботи виконано самостійно та правильно, поставлений результат та мету досягнуто в повному обсязі, здобувач навів правильні відповіді на половину контрольних питань і продемонстрував посередні вміння роботи на ПК із відповідним програмним продуктом
5 балів	завдання лабораторної роботи виконано самостійно та правильно, поставлений результат та мету досягнуто в повному обсязі, здобувач не навів правильні відповіді контрольні питання, але продемонстрував посередні вміння роботи на ПК із відповідним програмним продуктом
4 бали	завдання лабораторної роботи виконано не в повному обсязі, або ж не самостійно, поставлений результат та мету досягнуто частково, здобувач навів правильні відповіді на всі контрольні питання та продемонстрував вміння роботи на ПК із відповідним програмним продуктом
3 бали	завдання лабораторної роботи виконано не в повному обсязі, або ж не самостійно, здобувач навів правильні відповіді на половину контрольних питань і продемонстрував посередні вміння роботи на ПК із відповідним програмним продуктом
2 бали	завдання лабораторної роботи виконано не в повному обсязі, або ж не самостійно, здобувач не навів правильні відповіді контрольні питання, але продемонстрував посередні вміння роботи на ПК із відповідним програмним продуктом
1 бал	завдання лабораторної роботи виконано не в повному обсязі, або ж не самостійно, здобувач не навів жодної правильної відповіді на контрольні питання і продемонстрував відсутність вмінь роботи на ПК із відповідним програмним продуктом
0 балів (мінімальна)	завдання лабораторної роботи не виконано, поставлений результат та мету не досягнуто, здобувач не навів жодної правильної відповіді на контрольні питання і продемонстрував відсутність вмінь роботи на ПК із відповідним програмним продуктом, що не дає можливість оцінити формування компетентностей і досягнення програмних результатів.

Самостійна робота

1 бал (максимальна)	здобувач навів правильні відповіді на всі контрольні питання та продемонстрував знання, що підтверджують високий рівень опанування результату навчання
0 балів (мінімальна)	здобувач не навів жодної правильної відповіді на контрольні питання і не продемонстрував відсутність опанування результату навчання

Розв'язування тестів

Розв'язування тестів: 0-24 бали 0-15 балів*	24 (15 балів*) – 100 % правильних відповідей; - за кожну правильну відповідь на питання тесту здобувач отримує 1 бал 0 балів – 0% правильних відповідей, що не дає можливість оцінити формування компетентностей і досягнення програмних результатів

**** для заочної форми навчання***

Контрольна робота (для заочної форми навчання)

Теоретичні питання 15 балів (максимальна оцінка) 0 балів (мінімальна оцінка)	Оцінюється повнота змісту, послідовність викладення теоретичного матеріалу завдання №1: 15 балів – відповідність представленого реферативного матеріалу тематиці варіанту, наявність узагальнень, повнота; в роботі проаналізовано сучасну наукову літературу, використано власні схеми, діаграми, є власні висновки. 10 балів - форматування частково відповідає стандартам оформлення технічних звітів; в роботі проаналізовано сучасну наукову літературу, використано запозичені схеми, діаграми, є висновки. 0 балів – теоретичне завдання не виконано або обсяг і точність виконання менше 50%, що не дає можливість оцінити формування компетентностей і досягнення програмних результатів
15 балів (максимальна оцінка) 0 балів (мінімальна оцінка)	Повнота і правильність виконання завдання №2 15 балів – за правильну відповідь та представлення повного розв'язку поставленої задачі. 10 балів - за правильну відповідь та представлення часткового розв'язку поставленої задачі. 7 балів - за неправильну відповідь та представлення часткового розв'язку поставленої задачі. 0 балів – частина практичного завдання не виконана, що не дає можливість оцінити формування компетентностей і досягнення програмних результатів

Шкала та критерії оцінювання результатів навчання здобувачів вищої освіти на екзамені

Вид завдання, кількість балів	Критерії оцінювання тестового завдання екзаменаційного білету в межах зазначеної кількості балів
Відповіді на теоретичні питання у вигляді тестів (відсоток правильних відповідей розраховується в програмі тестування автоматично), 20 балів (максимум) 0 балів (мінімум)	20 балів – більше 95 % правильних відповідей 19 балів – більше 90 % правильних відповідей 18 балів - більше 85 % правильних відповідей 17 балів – більше 80 % правильних відповідей 16 балів – більше 75 % правильних відповідей 15 балів – більше 70 % правильних відповідей 14 балів – більше 65 % правильних відповідей 13 балів – більше 60 % правильних відповідей 12 балів – більше 55 % правильних відповідей 11 балів – більше 50 % правильних відповідей 12 балів – більше 45 % правильних відповідей 11 балів – більше 40 % правильних відповідей 10 балів – більше 35 % правильних відповідей 9 балів – більше 30 % правильних відповідей 8 балів – більше 25 % правильних відповідей 7 бали – більше 20 % правильних відповідей 6 балів – більше 15% правильних відповідей 5 балів – більше 10 % правильних відповідей 4 бали – більше 5 % правильних відповідей 3 бали –більше 4% правильних відповідей 2 бали – більше 3% правильних відповідей 1 бал –більше 2% правильних відповідей 0 балів – правильних відповідей немає, що не дає можливість оцінити формування компетентностей і досягнення програмних результатів

12. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна (за потреби)

Засоби навчання: ПК, MS Windows, MS Office 365 або Libre Office, Google Docs, Internet-браузери, мультимедійне забезпечення (проектор), проекційний екран, інтерактивна дошка або дошка аудиторна, мережа Wi-Fi, презентації, електронна бібліотека ПДАУ (https://lib.pdau.edu.ua), електронний репозитарій ПДАУ (http://dspace.pdau.edu.ua), система дистанційного навчання (https://moodle.pdau.edu.ua), система електронного журналу АСУ ПДАУ (https://asu.pdau.edu.ua); а також прикладне ПЗ у вільному доступі Notepad++, Oracle VM VirtualBox, Microsoft Network Monitor, Wireshark, Comodo Firewall, Cain&Abel, системи генеративного ШІ (ChatGPT, Grok AI, Claude, Gemini).

Інструменти, обладнання та програмне забезпечення, необхідне для навчальної дисципліни, забезпечують центр підготовки користувачів інформаційної системи «Soft.Farm» – спеціалізована комп'ютерна лабораторія (аудиторія 212), навчально-дослідна лабораторія «Інтелектуальних безпілотних систем» 202, навчально-наукова лабораторія «Web-технологій та хмарних обчислень» 203, навчально-наукова лабораторія «Імітаційного моделювання та реінжинірингу бізнес-процесів» 213.

13. Політика навчальної дисципліни

Політика навчальної дисципліни визначається системою вимог, які викладач висуває до здобувача вищої освіти при вивченні дисципліни та ґрунтується на засадах справедливого об'єктивного оцінювання роботи кожного студента і дотримання академічної доброчесності.

Вимоги можуть стосуватися:

1. Термінів виконання та перескладання:

- обов'язковість виконання завдань лабораторних робіт, самостійної роботи і захист результатів у відведений термін;
- за активну участь у науковій роботі за тематикою кафедри, дисципліни, участь у олімпіадах, творчих конкурсах і т. ін. можуть нараховуватися додаткові бали;
- обов'язковість виконання завдань лабораторних робіт, самостійної роботи і захист результатів у відведений термін (за несвоєчасне подання звітів про виконання лабораторної роботи без поважних причин оцінка може бути знижена на 10%).

2. Академічної доброчесності:

Здобувач вищої освіти повинен дотримуватись Кодексу академічної доброчесності [7] та Кодексу про етику викладача та здобувача вищої освіти [8] Полтавського державного аграрного університету. Дотримання академічної доброчесності здобувачами вищої освіти передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; дотримання норм законодавства про авторське право і суміжні права; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Здобувачі вищої освіти можуть використовувати системи генеративного штучного інтелекту для покрокового роз'яснення виконання завдання, для пояснення виправлення помилок компіляції коду, для створення добірок тематичних літературних джерел, для створення покрокових рекомендацій – пояснень з налаштування проєктів зі складною архітектурою, для генерування наборів вхідних даних для тестування розроблених додатків. Але, суворо забороняється безпосереднє виконання практичних завдань з розроблення коду за допомогою будь-якої системи генеративного штучного інтелекту, а також використання таких систем при виконанні тестів та контрольної роботи.

При виявленні академічного плагіату під час виконання запланованих видів робіт такі

роботи не зараховуються та повертаються на доопрацювання зі зниженням загальної оцінки мінімум на 20 %.

3. Відвідування занять:

Обов'язковість відвідування занять (неприпустимість пропусків без поважних причин, запізнень і т. ін.).

4. Зарахування результатів неформальної/інформальної освіти:

Врахування результатів навчання, отриманих під час неформальної/інформальної освіти та зарахування результатів відбувається згідно Положення про порядок визнання результатів навчання, здобутих у неформальній та інформальній освіті здобувачами вищої освіти Полтавського державного аграрного університету [9].

5. Оскарження результатів оцінювання:

Порядок оскарження результатів оцінювання здійснюється згідно процедур, затверджених у Положенні про оцінювання результатів навчання здобувачів вищої освіти в Полтавському державному аграрному університеті

14. Рекомендовані джерела інформації

Основні

1. Тарнавський, Ю. А. Безпека інформаційних систем: підручник. Київ : КПІ ім. Ігоря Сікорського, 2023. 163 с.
2. Безпека інформаційно-комунікаційних систем : підручник / Ю.В. Костюк, П.М. Складанний, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзаєва, М.В. Ворохоб. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 1016 с.

Допоміжні

3. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. Київ : Держ. торг.-екон. ун-т, 2023. 376 с.
4. Муравський В. Облік та кібербезпека : монографія. Тернопіль : ЗУНУ. 2023. 200 с.
5. Cloud Video System Availability Assessment Using Markov and Semi-Markov Models / O. Ivanchenko et al. *2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 22–26 February 2022. 2022. URL: https://doi.org/10.1109/tcset55632.2022.9767064.
6. Models for Assessing the Dependability of Programmable Devices with Controlled Multi-Level Degradation / V. Kharchenko et al. *Lecture Notes in Networks and Systems*. Cham, 2025. P. 85–95. URL: https://doi.org/10.1007/978-3-031-92734-8_9.

Інформаційні ресурси мережі Інтернет

7. Кодекс академічної доброчесності Полтавського державного аграрного університету. URL: https://www.pdau.edu.ua/sites/default/files/node/9854/kodeksdobrochesnostinasayt.pdf
8. Кодекс про етику викладача та здобувача вищої освіти Полтавського державного аграрного університету. URL: https://www.pdau.edu.ua/sites/default/files/node/4518/etykaetyka.pdf
9. Положення про порядок визнання результатів навчання, здобутих у неформальній та інформальній освіті, здобувачами вищої освіти Полтавського державного аграрного університету. URL: https://www.pdau.edu.ua/sites/default/files/node/5555/polozhennyaproneformalnuosvitu2025.pdf
10. Prometheus: каталог курсів. URL: https://prometheus.org.ua/courses-catalog/it
11. Coursera. URL: https://www.coursera.org/
12. ChatGPT AI, URL: https://chatgpt.com/
13. Grok AI, URL: https://grok.com
14. Claude AI, URL: https://claude.ai
15. Gemini AI, URL: https://gemini.google.com/app