ПОЛТАВСЬКА ДЕРЖАВНА АГРАРНИЙ УНІВЕРСИТЕТ
Кафедра інформаційних систем та технологій

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Юрій УТКІН
(протокол від «01» вересня 2025 р. №2)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
(обов'язкова навчальна дисципліна)

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

освітньо-професійна програма Інформаційні управляючі системи та технології
спеціальність F6 Інформаційні системи і технології
галузь знань F Інформаційні технології
рівень вищої освіти другий (магістерський)
навчально-науковий інститут економіки, управління, права та інформаційних технологій

Полтава
2025-2026 н.р.

Робоча програма навчальної дисципліни «Технології захисту інформаційних систем» для здобувачів вищої освіти за освітньо-професійною програмою «Інформаційні управляючі системи та технології» спеціальності F6 Інформаційні системи і технології.

Мова викладання – державна.

Розробник: Олег Одарущенко, професор кафедри інформаційних систем та технологій, д.т.н., професор

«01» вересня 2025 року _____ Олег ОДАРУЩЕНКО

Погоджено гарантом освітньої програми
«Інформаційні управляючі системи та технології»
«01» вересня 2025 року _____ Юрій УТКІН

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

протокол від «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_мд_21)*	Заочна форма здобуття освіти *(126ІСТ_мз_21[1])*
Загальна кількість годин	90	
Кількість кредитів	3	
Місце в індивідуальному навчальному плані здобувача вищої освіти	***обов'язкова***	
Рік навчання (курс)	2	1;2
Семестр	3	2;3
Лекції (годин)	16	2;6
Лабораторні (семінарські) (годин)	16	0;10
Самостійна робота (годин)	58	72
у т. ч. індивідуальні завдання (контрольна робота), годин	-	30
Форма семестрового контролю	екзамен	

2. Мета вивчення навчальної дисципліни

Метою навчальної дисципліни є формування системи теоретичних знань здобувачів вищої освіти щодо сучасних методів та засобів забезпечення інформаційної безпеки, порядку проєктування, впровадження та супроводження комплексної системи захисту інформації, системи управління інформаційною безпекою, підготовки фахівців, здатних аналізувати, обирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки та цілісності даних відповідно до розв'язуваних прикладних завдань.

3. Передумови для вивчення навчальної дисципліни

Навчальна дисципліна «Технології захисту інформаційних систем» є обов'язковою у циклі дисциплін професійної підготовки здобувачів вищої освіти, які навчаються за освітньо-професійною програмою Інформаційні управляючі системи та технології та спирається на наступні навчальні дисципліни, які їй передують, а саме: «Моделювання інформаційних процесів та систем»; «Програмні технології створення інформаційних систем».

4. Компетентності:

Загальні:

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

- КЗ 5. Здатність оцінювати та забезпечувати якість виконуваних робіт.

Спеціальні (фахові):

- СК 1. Здатність розробляти та застосувати ІСТ, необхідні для розв'язання стратегічних і поточних задач;

- СК 5. Здатність використовувати сучасні технології аналізу даних для оптимізації процесів в інформаційних системах;

- СК 6. Здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки.

5. Програмні результати навчання:

- РН 10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації;

- РН 11. Розв’язувати задачі цифрової трансформації у нових або невідомих середовищах на основі спеціалізованих концептуальних знань, що включають сучасні наукові здобутки у сфері інформаційних технологій, досліджень та інтеграції знань з різних галузей.

Співвідношення програмних результатів навчання із очікуваними результатами навчання

Програмний результат навчання ***(визначений освітньою програмою)***	**Очікувані результати навчання навчальної дисципліни**
РН 10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.	Здобувач має знати: основні поняття інформаційної безпеки, зокрема в інформаційному просторі України, класифікацію загроз та методів захисту інформації; основи криптографії, включаючи симетричну криптографію, системи з відкритим ключем, криптографічні стандарти, хеш-функції та цифровий підпис; методи забезпечення безпеки програмного забезпечення, операційних систем, баз даних, мережевих і вебсервісів; основи мережевої та веббезпеки, типи атак, методи захисту, такі як IPsec, TLS/SSL, віртуальні приватні мережі; процес проєктування комплексної системи захисту інформації (КСЗІ), етапи її формування, впровадження та супроводу.
	Здобувач має розуміти: важливість і значення комплексного підходу до забезпечення інформаційної безпеки; принципи побудови політик безпеки та моделі безпеки для різних організаційних потреб; основи криптографічного захисту та його застосування для забезпечення конфіденційності, цілісності та автентичності даних; потенційні загрози та види атак на ІСТ, а також як ці загрози можуть бути пом'якшені або усунені; процедури і методи планування, організації, впровадження та контролю КСЗІ на підприємствах.
	Здобувач має вміти: використовувати методи та засоби захисту інформації для протидії кіберзагрозам, забезпечувати розмежування доступу та захищати конфіденційні дані; застосовувати криптографічні методи, такі як шифрування, цифровий підпис, хешування для захисту інформації; розробляти та налаштовувати захист програмного забезпечення, операційних систем та баз даних; забезпечувати мережеву та веббезпеку, включаючи налаштування міжмережевих екранів, систем виявлення та запобігання атак, анонімних комунікацій; планувати, організовувати та контролювати впровадження комплексної системи захисту інформації, забезпечуючи ефективний кіберзахист ІСТ.

РН 11. Розв’язувати задачі цифрової трансформації у нових або невідомих середовищах на основі спеціалізованих концептуальних знань, що включають сучасні наукові здобутки у сфері інформаційних технологій, досліджень та інтеграції знань з різних галузей.	Здобувач має знати: **с**учасні концепції інформаційної безпеки та цифрової трансформації, включаючи останні досягнення в галузі ІТ, кібербезпеки та цифрових рішень для бізнесу та організацій; поширені загрози в цифрових середовищах та передові технології захисту інформації в умовах цифрової трансформації; методи захисту та шифрування даних, зокрема криптографічні алгоритми, хеш-функції та цифровий підпис, а також їх роль у забезпеченні безпеки в цифрових платформах; принципи розробки політики інформаційної безпеки, її адаптацію до нових і невідомих цифрових середовищ; основи проєктування безпечних інформаційних систем, зокрема інтеграцію інформаційної безпеки в інноваційні ІТ-рішення.
	Здобувач має розуміти: вимоги цифрової трансформації до інформаційної безпеки, зокрема як технології кіберзахисту можуть адаптуватися для нових і швидкозмінних цифрових платформ; способи застосування інновацій у криптографії, мережевій безпеці та захисті даних для забезпечення безпеки у нових середовищах; методи досліджень і концептуальної інтеграції інформаційної безпеки з іншими сферами ІТ для адаптації до сучасних загроз у цифрових трансформаціях; виклики та ризики, що виникають під час впровадження цифрових інновацій у непередбачуваних умовах, і як наукові дослідження сприяють створенню нових методів захисту.
	Здобувач має вміти: оцінювати нові цифрові середовища та невідомі ризики для розробки комплексних заходів захисту інформації; застосовувати передові криптографічні та мережеві технології для захисту інформаційних систем у процесі цифрової трансформації; інтегрувати інноваційні наукові здобутки з різних галузей ІТ для вирішення завдань кібербезпеки у нових середовищах; розробляти і впроваджувати комплексні рішення, що відповідають потребам безпеки у нових цифрових платформах та підходах до трансформації; застосовувати міждисциплінарний підхід до створення рішень кібербезпеки, враховуючи сучасні досягнення в ІТ, кібербезпеці, системному аналізі та цифрових комунікаціях.

6. Методи навчання і викладання

1. Методи організації та здійснення навчально-пізнавальної діяльності:

– словесні методи: лекція, розповідь, пояснення;

– наочні методи: ілюстрування;

– практичні методи: вправи, практичні роботи, робота з навчально-методичною літературою (конспектування, тезування, анотування).

2. Методи стимулювання і мотивації навчально-пізнавальної діяльності:

– методи формування пізнавальних інтересів: створення ситуації інтересу й новизни навчального матеріалу; метод використання життєвого досвіду; метод відповідей на запитання і опитування думок здобувачів вищої освіти.

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

– методи усного контролю: опитування; бесіда; доповідь;

– методи письмового контролю: контрольна робота; самостійна робота.

7. Програма навчальної дисципліни

Тема 1. Основні поняття безпеки інформаційних систем.

Основні положення інформаційного простору України. Основні поняття та визначенні теорії інформаційної безпеки. Загрози інформаційної безпеки. Порушники інформаційної безпеки. Класифікація методів та засобів забезпечення інформаційної безпеки. Розмежування доступу. Означення політики інформаційної безпеки та принципи політики безпеки. Типи політики безпеки. Моделі політики безпеки. Організаційно-технічні та адміністративні методи захисту інформації. Організація секретного діловодства та заходів із захисту інформації.

Тема 2. Криптографічний захист інформації.

Основні поняття криптографії. Онови симетричної криптографії. Криптографічні системи з відкритим ключем. Огляд основних міжнародних та національних стандартів асиметричного шифрування даних. Криптографічні хеш-функції та електронний цифровий підпис. Практичне застосування криптографії (Bouncy Castle Crypto, протоколи автентифікації та обміну ключами, блокчейн, стеганографія).

Тема 3. Безпека програм та даних.

Безпека програмного забезпечення. Безпека операційних систем. Захист та безпека баз даних.

Тема 4. Мережева та веббезпека.

Мережева безпека. Етапи реалізації атаки. Основні типи атак на комп'ютерні мережі. Пасивний та активний збір інформації про мережу. Сніфери. Безпека безпроводових мереж. IPsec. Технології віртуальних приватних мереж. Безпека TLS/SSL.

Безпека Веб. Атаки на вебзастосунки та сайти. Атака відмова в обслуговуванні. Атака міжсайтовий скриптинг (XSS). Безпека вебсерверів та вебзастосувань. Безпека прикладних протоколів Інтернет. Парольна автентифікація.

Засоби забезпечення безпеки мереж. Системи аналізу захищеності мережі. Міжмережеве екранування. Системи виявлення та попередження атак. Анонімні комунікації. Тимчасові сервіси електронної пошти. Анонімайзери.

Тема 5. Етапи проєктування комплексної системи захисту інформації.

Визначення, призначення та функції комплексної системи захисту інформації. Формування загальних вимог до комплексної системи захисту інформації. Обґрунтування необхідності створення комплексної системи захисту інформації. Порядок впровадження комплексної системи захисту інформації. Супроводження комплексної системи захисту інформації.

Структура (тематичний план) навчальної дисципліни

Назви тем	Кількість годин							
	денна форма здобуття освіти *(126ІСТ_мд_21)*				заочна форма здобуття освіти *(126ІСТ_мз_21[1])*			
	усього	у тому числі			усього	у тому числі		
		л	л.р	с.р.		л	л.р.	с.р.
Тема 1. Основні поняття безпеки інформаційних систем.	14	2	-	12	16	2	-	14
Тема 2. Криптографічний захист інформації.	26	4	8	14	22	2	6	14
Тема 3. Безпека програм та даних.	18	2	4	12	18	2	2	14

Тема 4. Мережева та веббезпека.	18	4	4	12	18	2	2	14
Тема 5. Етапи проєктування комплексної системи захисту інформації.	12	4	-	8	16	-	-	16
В т.ч. індивідуальне завдання: контрольна робота	**-**	**-**	**-**	**-**	**30**	**-**	**-**	**30**
Усього годин	**90**	**16**	**16**	**58**	**90**	**8**	**10**	**72**
Екзамен	**27**				**27**			

8. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна форма здобуття освіти (126ІСТ_мд_21)	заочна форма здобуття освіти (126ІСТ_мз_21[1])
1	**Тема 2.** Криптографічний захист інформації. **Лабораторне заняття 1. Тема:** «Дослідження сучасних методів криптографії з відкритим ключем PKI (Public-Key Infrasructure)». **Лабораторне заняття 2.Тема:** «Дослідження принципів безпеки, які реалізує протокол TLS (Transport layer Security)». **Лабораторне заняття 3.Тема:** «Дослідження алгоритма RSA (Rivest-Shamir-Adleman)».	8	6
2	**Тема 3.** Безпека програм та даних. **Лабораторне заняття 4-5. Тема:** «Дослідження атаки на програмне забезпечення - вразливість переповнення буфера».	4	2
3	**Тема 4.** Мережева та веббезпека. **Лабораторне заняття 6.Тема:** «Дослідження технологій, що лежать в основі засобів перехоплення та підробки даних». **Лабораторне заняття 7.Тема:** «Дослідження вразливостей протокола TCP/IP». **Лабораторне заняття 8.Тема:** «Дослідження міжсайтового сценарію XSS (Cross-site scripting».	4	2
	Разом	16	10

9. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин	
		денна форма здобуття освіти (126ІСТ_мд_21)	заочна форма навчання (126ІСТ_мз_21[1])
1	**Тема 1.** Основні поняття безпеки інформаційних систем.	12	14
2	**Тема 2.** Криптографічний захист інформації.	14	14
3	**Тема 3.** Безпека програм та даних.	12	14
4	**Тема 4.** Мережева та веббезпека.	12	14
5	**Тема 5**. Етапи проєктування комплексної системи захисту інформації.	8	16
	Разом	58	72

10. Індивідуальне завдання

Індивідуальна робота здобувача вищої освіти направлена на закріплення теоретичного матеріалу та практичних навичок. Реалізація цього напряму роботи передбачається шляхом виконання контрольної роботи, яка виконується самостійно здобувачем вищої освіти заочної форми навчання в поза аудиторний час. Перевірка результатів індивідуальної роботи студентів викладачем відбувається до та під час екзаменаційної сесії.

11. Оцінювання результатів навчання

Програмні результати навчання/Результати навчання	Форми контролю програмних результатів навчання/результатів навчання
РН 10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації .	- опитування; - виконання лабораторних робіт та їх захист; - виконання завдань самостійної роботи; - розв'язування тестів; - контрольна робота*; - екзамен.
РН 11. Розв'язувати задачі цифрової трансформації у нових або невідомих середовищах на основі спеціалізованих концептуальних знань, що включають сучасні наукові здобутки у сфері інформаційних технологій, досліджень та інтеграції знань з різних галузей.	- опитування; - виконання лабораторних робіт та їх захист; - виконання завдань самостійної роботи; - розв'язування тестів; - контрольна робота*; - екзамен.

* 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 126ІСТ_мд_21)

Назва теми	Форми контролю результатів навчання ЗВО					
	Робота на лекціях	Виконання завдань лабораторних робіт та їх захист	Виконання завдань самостійної роботи	Розв' язування тестів	Екзамен	Разом
Тема 1. Основні поняття безпеки	2	-	2			12

інформаційних систем.						
Тема 2. Криптографічний захист інформації.	4	15	2			12
Тема 3. Безпека програм та даних.	2	10	2	7		18
Тема 4. Мережева та веббезпека.	4	15	2			15
Тема 5. Етапи проєктування комплексної системи захисту інформації.	4	-	2	7		23
Екзамен					20	20
Разом балів за темами	**16**	**40**	**10**	**14**	**20**	**100**

Схема нарахування балів з навчальної дисципліни
(Заочна форма здобуття освіти 126ІСТ_мз_21[1])

Назва теми	Форми контролю результатів навчання ЗВО						
	Робота на лекціях	Виконання завдань лабораторних робіт та їх захист	Виконання завдань самостійної роботи	Розв’язування тестів	Контрольна робота	Екзамен	Разом
Тема 1. Основні поняття безпеки інформаційних систем.			3				3
Тема 2. Криптографічний захист інформації.			3				3
Тема 3. Безпека програм та даних.	4		3	10			17
Тема 4. Мережева та веббезпека.	4		3				7
Тема 5. Етапи проєктування комплексної системи захисту інформації.		7	3	10			20
Контрольна робота					30		30
Екзамен						20	20
Разом балів за темами	**8**	**7**	**15**	**20**	**30**	**20**	**100**

Шкала та критерії оцінювання результатів навчання при проведенні поточного контролю успішності здобувачів вищої освіти
(Денна форма здобуття освіти 126ІСТ_мд_21)

Робота на лекціях

Кількість балів	Критерії оцінювання
2 бали (максимальна)	Здобувач бере активну участь в обговоренні проблемних питань під час лекції, бере участь в опитуванні, веде конспект лекції.
1 бал	Здобувач відповів на питання, але не повному обсязі.
0 балів (мінімальна)	Здобувач не опрацював матеріал з теми, що не дає можливість оцінити формування компетентностей і досягнення програмних результатів.

Виконання завдань на лабораторних заняттях

Кількість балів	Критерії оцінювання
5 балів (максимальна)	Здобувач демонструє знання та практичні навички, виконав 100% завдання на лабораторну роботу та захистив її.
4 бали	Здобувач демонструє знання та практичні навички, виконав 75% завдання на лабораторну роботу.
3 бали	Здобувач демонструє знання та практичні навички, виконав 50% завдання на лабораторну роботу.
2 бали	Здобувач демонструє знання та практичні навички, виконав 25% завдання на лабораторну роботу.
1 бал	Здобувач на лабораторному занятті засвоїв лише теоретичні відомості та встановив необхідне програмне забезпечення
0 балів (мінімальна)	Здобувач не опрацював лабораторну роботу.

Виконання завдань самостійної роботи

Кількість балів	Критерії оцінювання
2 бали (максимальна)	Здобувач виконав і захистив 100% вправ самостійної роботи за окремою темою. Додаткові бали можуть нараховуватись за окремі додаткові види робіт (написання тез доповіді, виступ на студентській конференції в межах 5 балів)
1 бал	Здобувач виконав і захистив 50% вправ самостійної роботи за окремою темою.
0 балів (мінімальна)	Здобувач не представив виконане завдання самостійної роботи, що не дає можливість оцінити формування компетентностей і досягнення програмних результатів.

Розв'язування тестів

Кількість балів	Критерії оцінювання
7 балів (максимальна)	
6 балів	
5 балів	Здобувач навів від 21 до 25 вірних відповідей.
4 бали	Здобувач навів від 16 до 20 вірних відповідей.
3 бали	Здобувач навів від 11 до 15 вірних відповідей.
2 бали	Здобувач навів від 6 до 10 вірних відповідей.
1 бал	Здобувач навів від 1 до 5 вірних відповідей.
0 балів (мінімальна)	Здобувач навів 0 вірних відповідей.

** Додаткові бали можуть нараховуватись за окремі додаткові види робіт (написання тез доповіді, виступ на студентській конференції в межах 5 балів)*

Шкала та критерії оцінювання результатів навчання при проведенні поточного контролю успішності здобувачів вищої освіти
(Заочна форма здобуття освіти 126ІСТ_мз_21[1])

Робота на лекціях

Кількість балів	Критерії оцінювання
4 бали	Здобувач бере активну участь в обговоренні проблемних питань під час

(максимальна)	лекції, бере участь в опитуванні, веде конспект лекції.
3 бали	Здобувач активно працював на лекції, конспект повний.
2 бали	Здобувач працював на лекції, конспект не повний.
0 балів (мінімальна)	Здобувач не опрацював матеріал з теми, що не дає можливість оцінити формування компетентностей і досягнення програмних результатів.

Виконання завдань на лабораторних заняттях

Кількість балів	**Критерії оцінювання**
7 балів (максимальна)	Здобувач демонструє знання та практичні навички, виконав 100% завдання на лабораторну роботу та захистив її.
6 балів	Здобувач демонструє знання та практичні навички, виконав 90% завдання на лабораторну роботу. Досягнуто достатній рівень програмного результату навчання.
5 балів	Здобувач демонструє знання та практичні навички, виконав 75% завдання на лабораторну роботу.
4 бали	Здобувач демонструє знання та практичні навички, виконав 60% завдання на лабораторну роботу.
3 бали	Здобувач демонструє знання та практичні навички, виконав 40% завдання на лабораторну роботу.
2 бали	Здобувач демонструє знання та практичні навички, виконав 20% завдання на лабораторну роботу.
1 бал	Здобувач на лабораторному занятті засвоїв лише теоретичні відомості та встановив необхідне програмне забезпечення.
0 балів (мінімальна)	Здобувач не опрацював лабораторну роботу.

Виконання завдань самостійної роботи

Кількість балів	**Критерії оцінювання**
3 бали (максимальна)	Здобувач виконав 100% вправ самостійної роботи за окремою темою.
2 бали	Здобувач виконав і захистив 75% завдань самостійної роботи за окремою темою.
1 бал	Здобувач виконав і захистив 50% завдань самостійної роботи за окремою темою.
0 балів (мінімальна)	Здобувач не представив виконане завдання самостійної роботи, що не дає можливість оцінити формування компетентностей і досягнення програмних результатів.

Розв'язування тестів

Кількість балів	**Критерії оцінювання**
10 балів (максимальна)	Здобувач навів від 28 до 30 вірних відповідей.
9 балів	Здобувач навів від 25 до 27 вірних відповідей.
8 балів	Здобувач навів від 22 до 24 вірних відповідей.
7 балів	Здобувач навів від 19 до 21 вірних відповідей.
6 балів	Здобувач навів від 16 до 18 вірних відповідей.
5 балів	Здобувач навів від 13 до 15 вірних відповідей.
4 бали	Здобувач навів від 10 до 12 вірних відповідей.
3 бали	Здобувач навів від 7 до 9 вірних відповідей.
2 бали	Здобувач навів від 4 до 6 вірних відповідей.
1 бал	Здобувач навів від 1 до 3 вірних відповідей.

0 балів (мінімальна)	Здобувач навів 0 вірних відповідей.

Контрольна робота

Виконання контрольної роботи та оформлення звіту 30 балів (максимальна) 0 балів (мінімальна)	Контрольна робота містить 5 завдань. Кожне практичне завдання оцінюється в 6 балів: – оформлення звіту згідно вимог, наведено повне та вірне рішення окремого завдання – 6 балів; – оформлення звіту з недотриманням вимог, неповне рішення окремого завдання – 3 бали; звіт не підготовлений – 0 балів.

** Додаткові бали можуть нараховуватись за окремі додаткові види робіт (написання тез доповіді, виступ на студентській конференції в межах 5 балів)*

Шкала та критерії оцінювання результатів навчання здобувачів вищої освіти на екзамені

Вид завдання	Бали	Критерії оцінювання
Завдання 1, 2 Відповіді на теоретичні питання 5 балів за одне питання (максимум) 0 балів за одне питання (мінімум)	5	теоретичне питання розкрито повністю, що свідчить про сформовані компетентності та отримання високої оцінки
	4	зміст питання розкрито на 80%, що дає відносну можливість оцінити формування компетентностей та отримання позитивної оцінки;
	3	зміст питання розкрито на 60%
	2	зміст питання розкрито на 40%
	1	зміст питання розкрито на 20%
	0	відсутність відповіді на теоретичне питання, що не дає можливість оцінити формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти
Завдання 3, 4 Розв'язання практичного завдання 5 балів за одне завдання (максимум) 0 балів за одне завдання (мінімум)	5	розрахунки практичного завдання виконані правильно, сформовані повні висновки, що свідчать про високий рівень засвоєння програмних результатів навчання
	4	допущені 1 обчислювальна помилки або виправлення, що вказує на достатній рівень формування компетентностей та отримання позитивних програмних результатів навчання у здобувача вищої освіти
	3	допущені 2 обчислювальні помилки та виправлення
	2	допущені 3-4 обчислювальні помилки та виправлення
	1	наведено неправильний розв'язок задачі
	5	розрахунки практичного завдання виконані правильно, сформовані повні висновки, що свідчать про високий рівень засвоєння програмних результатів навчання

**екзамен складається з 2 теоретичних питань та 2-х практичних завдань. Максимальна кількість балів за екзамен - 20.*

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 11 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++, Apache Spark, системи генеративного ШІ (ChatGPT, Grok AI, Claude, Gemini). Інструменти, обладнання та програмне забезпечення, необхідне для навчальної дисципліни, забезпечує 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 практичних робіт, самостійної роботи і захист результатів у відведений термін;
- за активну участь у науковій роботі за тематикою кафедри, дисципліни, участь у творчих конкурсах і т. ін. можуть нараховуватися додаткові бали;
- обов'язковість виконання завдань практичних робіт, самостійної роботи і захист результатів у відведений термін. Виконання завдань з порушенням термінів без поважних причин оцінюється на 25 % нижче за одержаний бал. Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.

2. **Академічної доброчесності**:

Здобувач вищої освіти повинен дотримуватись Кодексу академічної доброчесності та Кодексу про етику викладача та здобувача вищої освіти 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.

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.

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. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра та ін. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. 144 с.

2. Комплексні системи захисту інформації : навчальний посібник / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. Вінниця : ВНТУ, 2017. 120 с.

3. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги. [Чинний від 2015-06-27]. Київ, 2015. 24 с. (Інформація та документація).

Допоміжні

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»/ База законодавства України № 80/94-ВР. URL: http://zakon4.rada.gov.ua/laws/ show/80. (дата звернення: 27.08.2025).

2. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05 / Нормативна база Дер спецзв'язку 2015.URL: http ://www.dstszi. gov.ua/dstszi/control/uk/ publish/article?art id=46074. (дата звернення: 27.08.2025).

3. ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.

4. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

5. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

6. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

7. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

8. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.

9. НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.

10. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

Інформаційні ресурси мережі інтернет

1. Державна служба спеціального зв'язку та захисту інформації України URL: https://cip.gov.ua/.(дата звернення: 27.08.2025).

2. Coursera. URL: https://www.coursera.org/