ПОЛТАВСЬКА ДЕРЖАВНА АГРАРНИЙ УНІВЕРСИТЕТ
Кафедра інформаційних систем та технологій

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Юрій УТКІН
«03» вересня 2024 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

(обов'язкова навчальна дисципліна)

освітньо-професійна програма Інформаційні управляючі системи

спеціальність 126 Інформаційні системи та технології

галузь знань 12 Інформаційні технології

освітній ступінь бакалавр

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

Полтава
2024/2025 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.

Розробник:

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

«01» вересня 2024 року _____ Олег ОДАРУЩЕНКО

Схвалено на засіданні кафедри інформаційних систем та технологій

Протокол від «03» вересня 2024 року № 2

Погоджено гарантом освітньої програми Інформаційні управляючі системи

«03» вересня 2024 року _____ Олена КОПІШИНСЬКА

Схвалено головою ради з якості вищої освіти спеціальності «Інформаційні системи та технології» _____ Олена КОПІШИНСЬКА

Протокол від «03» вересня 2024 року № 1

1. Опис навчальної дисципліни

Елементи характеристики	Денна форма навчання (126ІСТ бд 2021)	Заочна форма навчання (126ІСТ бз 2021)
Загальна кількість годин	90	90
Кількість кредитів	3	3
Місце в індивідуальному навчальному плані студента	Обов'язкова	
Рік навчання(курс)	4	3;4
Семестр	8	6;7
Лекції (годин)	14	2;4
Лабораторні роботи (годин)	16	6
Самостійна робота (годин)	60	78
в т. ч. індивідуальні завдання (контрольна робота) (годин)		30
Форма семестрового контролю	екзамен	екзамен

2. Мета вивчення навчальної дисципліни

Метою вивчення навчальної дисципліни «Безпека інформаційних систем» є формування системи теоретичних знань та практичних навичок щодо сучасних методів захисту інформації в інформаційних системах та мережах і ознайомлення з особливостями їх апаратної та програмної реалізацій.

3. Передумови для вивчення навчальної дисципліни

Дисципліна базується на окремих темах дисциплін «Комп'ютерні мережі», «Корпоративні інформаційні системи», «Інформаційні системи».

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

5. Програмні результати навчання

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.

Співвідношення програмних результатів навчання із очікуваними результатами навчання

Програмний результат навчання ***(визначений освітньою програмою)***	**Очікувані результати навчання навчальної дисципліни**
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.	Знати: основні проблеми безпеки в Інтернеті, електронному бізнесі та корпоративних інформаційних системах; основні загрози безпеці інформаційних систем та методи їх аналізу; принципи побудови підсистем інформаційної безпеки та розробки політики безпеки; технології міжмережевого екранування, їх принципи роботи та застосування на різних рівнях моделі OSI; архітектуру та принципи функціонування сучасних систем FireWall; методи створення захищених віртуальних приватних мереж (VPN) та використання відповідних протоколів безпеки (IPSec, SSL, L2TP тощо); основи криптографічного захисту та протоколи розподілу криптографічних ключів (SKIP, ISAKMP).
	Розуміти: особливості реалізації моделей безпеки інформаційних систем та їх адаптацію під корпоративні мережі; сучасні загрози безпеці інформаційних систем та способи їх виявлення і нейтралізації; принципи функціонування та налаштування міжмережевих екранів для захисту корпоративних мереж; технології захисту комунікаційних каналів, зокрема методи шифрування та розподілу ключів у захищених з'єднаннях; важливість експертизи захищеності комп'ютерних систем та процес сертифікації інформаційних систем.

	Вміти: аналізувати загрози безпеки інформаційних систем та мереж, будувати відповідні моделі загроз; проєктувати та реалізовувати політику інформаційної безпеки в організації; налаштовувати та конфігурувати міжмережеві екрани (FireWall) для забезпечення захисту інформаційних ресурсів; створювати та адмініструвати захищені віртуальні мережі (VPN) з використанням сучасних протоколів безпеки; реалізовувати та налаштовувати системи управління криптографічними ключами для захищених комунікацій; виконувати аудит та тестування захищеності інформаційних систем.

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. 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 331.

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 навчання (126ІСТ бд 2021)				Заочна форма навчання: (126ІСТ_бз_2021)			
	усього	у тому числі			**усього**	у тому числі		
		л	лр	с.р.		л	лр	с.р.
Тема 1. Проблеми безпеки в Інтернет	**12**	2	2	8	**11**		0	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	**13**	0	2	11
Тема 4. Принципи інформаційної безпеки.	**13**	2	2	9	**13**	2	0	11
Тема 5. Встановлення і конфігурування систем FireWall.	**13**	2	2	9	**11**	0	0	11
Тема 6. Побудова захищених віртуальних мереж VPN.	**13**	2	2	9	**13**	2	0	11
Тема 7. Розподіл криптографічних ключів	**15**	2	4	9	**14**	0	2	12
В т.ч. індивідуальне завдання: - контрольна робота								30
Усього годин	**90**	**14**	**16**	**60**	**90**	**6**	**6**	**78**

8. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання (126ІСТ бд 2021)	Заочна форма навчання (126ІСТ бз 2021)
1	**Л/р №1:** Робота з обліковими записами користувачів і груп ОС Windows Server. Встановлення правил доступу до об'єктів файлової системи	2	2
2	**Л/р №2:** Використання теорії чисел для захисту інформації	2	2
3	**Л/р №3:** Організація безпеки локальної мережі при використанні утиліт, що реалізують моніторинг трафіка	2	0
4	**Л/р №4:** Організація безпеки механізму аутентифікації при перехопленні парольних хешей і їхньої розшифровки	2	0
5	**Л/р №5:** Налаштовування та адміністрування міжмережних екранів	2	0
6	**Л/р №6:** Методика побудови захищеної телекомунікаційної мережі із використанням	2	0
7	**Л/р №7:** Криптографічні методи захисту даних:	4	2
	Разом	**16**	**6**

9. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання (126ІСТ бд 2021)	Заочна форма навчання (126ІСТ бз 2021)
1	**Тема 1.** Проблеми безпеки в Інтернет	8	11
2	**Тема 2.** Проблеми безпеки корпоративних інформаційних систем.	8	11
3	**Тема 3.** Побудова підсистеми інформаційної	8	11
4	**Тема 4.** Принципи інформаційної безпеки.	9	11
5	**Тема 5.** Встановлення і конфігурування систем FireWall.	9	11
6	**Тема 6.** Побудова захищених віртуальних мереж VPN.	9	11
7	**Тема 7.** Розподіл криптографічних ключів	9	12
	Разом	**60**	**78**

10. Індивідуальне завдання

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

11. Оцінювання результатів навчання

Програмні результати навчання	Форми контролю програмних результатів навчання
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.	Поточний контроль: - робота на лекціях; - виконання лабораторних робіт; - захист лабораторних робіт; - виконання завдань самостійної роботи; - розв'язування тестів; - виконання індивідуального завдання - контрольна робота*. Семестровий контроль: - 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 навчання 126ICT_бд_2021)

Назва теми/ Форма семестрового контролю	Форми контролю результатів навчання здобувачів вищої освіти						разом
	робота на лекціях	виконання лабораторних робіт	захист лабораторних робіт	розв'язування тестів	виконання вправ самостійної роботи	екзамен	
Тема 1. Проблеми безпеки в Інтернет	2	4	2		1		9
Тема 2. Проблеми безпеки корпоративних інформаційних систем.	2	4	2		1		9
Тема 3. Побудова підсистеми інформаційної безпеки.	2	4	2		1		9
Тема 4. Принципи інформаційної безпеки.	2	4	2		1		9
Тема 5. Встановлення і конфігурування систем FireWall.	2	4	2		1		9
Тема 6. Побудова захищених віртуальних мереж VPN.	2	4	2		1		9
Тема 7. Розподіл криптографічних ключів	2	8	4	11	1		26
Екзамен							
Разом балів за темами	**14**	**32**	**16**	**11**	**7**	**20**	**100**

Схема нарахування балів з навчальної дисципліни
(Заочна форма навчання 126ІСТ_бз_2021)

Назва теми/ Форма семестрового контролю	Форми контролю результатів навчання здобувачів вищої освіти							разом
	робота на лекціях	виконання лабораторних робіт	захист лабораторних робіт	розв'язування тестів	виконання вправ самостійної роботи	контрольна робота	екзамен	
Тема 1. Проблеми безпеки в Інтернет					2			2
Тема 2. Проблеми безпеки корпоративних інформаційних систем.	3	5	2		2			12
Тема 3. Побудова підсистеми інформаційної безпеки.		5	2		2			9
Тема 4. Принципи інформаційної безпеки.	3				2			5
Тема 5. Встановлення і конфігурування систем FireWall.					2			2
Тема 6. Побудова захищених віртуальних мереж VPN.	3			6	2			11
Тема 7. Розподіл криптографічних ключів		5	2		2			9
Контрольна робота						30		
Екзамен							20	20
Разом балів за темами	**9**	**15**	**6**	**6**	**14**	**30**	**20**	**100**

Шкала та критерії оцінювання результатів навчання при проведенні поточного контролю успішності здобувачів вищої освіти
(Денна форма навчання 126ІСТ_бд_2021)

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 на лабораторних робіт

Кількість балів	Критерії оцінювання
4 бали (максимальна)	Здобувач демонструє знання та практичні навички, виконав 100% завдання на лабораторну роботу, приступив до оформлення звіту і підготовки до захисту.
3 бали	Здобувач демонструє знання та практичні навички, виконав 75% завдання на лабораторну роботу.
2 бали	Здобувач демонструє знання та практичні навички, виконав 50% 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.

Захист лабораторних робіт

Кількість балів	Критерії оцінювання
2 бали (максимальна)	Здобувач надав звіт з лабораторної роботи та захистив її
1 бал	Здобувач надав звіт з лабораторної роботи
0 балів (мінімальна)	Здобувач не надав звіт з лабораторної робот.

Виконання завдань самостійної роботи

Кількість балів	Критерії оцінювання
1 бал (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)
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
11 балів (максимальна)	Здобувач навів 30 вірних відповідей.
10 балів	Здобувач навів від 28 до 29 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.

** 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 навчання 126ІСТ_бз_2021)

Робота на лекціях

Кількість балів	Критерії оцінювання
3 бали (максимальна)	Здобувач бере активну участь в обговоренні проблемних питань під час лекції, бере участь в опитуванні, веде конспект лекції.
2 бали	Здобувач бере активну участь в обговоренні проблемних питань під час лекції, бере участь в опитуванні
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 лабораторних робіт

Кількість балів	Критерії оцінювання
5 балів (максимальна)	Здобувач демонструє знання та практичні навички, виконав 100% завдання на лабораторну роботу, приступив до оформлення звіту і підготовки до захисту.
4 бали	Здобувач демонструє знання та практичні навички, виконав 90% завдання на лабораторну роботу, приступив до оформлення звіту і підготовки до захисту.
3 бали	Здобувач демонструє знання та практичні навички, виконав 60% завдання на лабораторну роботу, приступив до оформлення звіту і підготовки до захисту.
2 бали	Здобувач демонструє знання та практичні навички, виконав 30% 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.

Захист лабораторних робіт

Кількість балів	Критерії оцінювання
2 бали (максимальна)	Здобувач надав звіт з лабораторної роботи та захистив її
1 бал	Здобувач надав звіт з лабораторної роботи
0 балів (мінімальна)	Здобувач не надав звіт з лабораторної робот.

Виконання завдань самостійної роботи

Кількість балів	Критерії оцінювання
2 бали (максимальна)	Здобувач виконав і захистив 100% вправ самостійної роботи за окремою темою.
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**
11 балів (максимальна)	Здобувач навів від 29 до 30 вірних відповідей.
10 балів	Здобувач навів від 27 до 28 вірних відповідей.
9 балів	Здобувач навів від 24 до 26 вірних відповідей.
8 балів	Здобувач навів від 22 до 23 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; контрольна робота не виконана, що не дає можливість оцінити формування компетентностей і досягнення програмного результату – 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	5	розрахунки практичного завдання виконані правильно, сформовані повні висновки, що свідчать про високий рівень засвоєння програмних результатів навчання

завдання 5 балів за одне завдання (максимум) 0 балів за одне завдання (мінімум)	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)

Перелік інструментів, обладнання та програмного забезпечення необхідного для вивчення навчальної дисципліни забезпечує спеціалізована комп'ютерна лабораторія 202: персональний комп'ютер (15 шт. – 2021 р.), платформа MS Windows 10 Pro (43 ліцензій), Windows 10 Edu (15 ліцензій), MS Ofice 365 (58 ліцензій) або Libre Ofice, Google Docs, Internet-браузери, мережа Wi-fi, мультимедійне забезпечення (проектор), проекційний екран, презентації, дошка аудиторна.

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. Семенов С.Г., Подорожняк А.О., Баленко О.І., Гавриленко С.Ю. Захист інформації в комп'ютерних системах та мережах, навч. посіб. Х.: НТУ «ХШ», 2018. 251 с.
2. Хорошко В. О. Проектування комплексних систем захисту інформації. Видавництво Львівської політехніки, 2020. 317 с.
3. Кузнецов О.О. Захист інформації в інформаційних системах. Вид. ХНЕУ, 2017. 286 с.

Допоміжні

1. Яковенко Є., Журавель І, Горбатий І. Інформаційна безпека. Львів: Львівська політехніка, 2019. 580 с.
2. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Вид-во SIDCON, 2021. 372 с.
3. Лисенко С. Теорія адміністративно-правового забезпечення інформаційної безпеки підприємництва: монографія. Видавничий дім "Персонал", 2017. 404 с.

Інформаційні ресурси

1. Державна служба спеціального зв'язку та захисту інформації України URL: https://cip.gov.u a/.(дата звернення: 27.08.2024).
2. Coursera: Cybersecurity Fundamentals.
URL: https://www.coursera.org/learn/introduction-to-cybersecurity-fundamentals (дата звереннння 25.08.2024).
3. Coursera: Introduction to Cybersecurity Fundamentals.
URL: https://www.coursera.org/learn/introduction-to-cybersecurity-fundamentals (дата звереннння 25.08.2024).