ПОЛТАВСЬКИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТОРГІВЛІ

Навчально-науковий інститут денної освіти

Кафедра комп'ютерних наук та інформаційних технологій

СИЛАБУС

навчальної дисципліни

«Захист даних»

на 2025-2026 навчальний рік

Курс та семестр вивчення	4 курс,1 семестр
Спеціальність	ДЗВ
Ступінь вищої освіти	бакалавр

ПІБ НПП, який веде дану дисципліну науковий ступінь Карнаухова Г.В., ст. викладач кафедри КНІТ і вчене звання посада

Контактний телефон	+380970268704
Електронна адреса	ta.annet @ gmail.com
Розклад навчальних занять	http://schedule.puet.edu.ua/
Консультації	очна згідно розкладу консультацій на сайті кафедри http://www.matmodel.puet.edu.ua//, он-лайн: електронною поштою, Viber, Telegram
Сторінка дистанційного курсу	https://el.puet.edu.ua/

Опис навчальної дисципліни

Мета вивчення навчальної дисципліни	Основною метою вивчення дисципліни “Захист даних” є засвоєння основних понять та категорій комп’ютерної безпеки, вивчення принципів побудови комплексних систем захисту інформації, розробки, дослідження та застосування механізмів захисту інформації, що ґрунтуються на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення автентичності, цілісності та конфіденційності інформаційних систем та технологій
Тривалість	5 кредитів ЄКТС/150 годин (лекції 20 год., практичні заняття 40 год., самостійна робота 90 год.)
Форми та методи навчання	Лекції та практичні заняття в аудиторії, самостійна робота поза розкладом Наочні методи: ілюстрування. демонстрування, інфографіка Практичні методи: лабораторні роботи, вирішення задач; моделювання ситуацій і об'єктів, творчі завдання Методи самостійної роботи вдома: проблемно -пошукові; проектного навчання; колективної розумової діяльності; застосування новітніх інформаційнокомунікаційних технологій у навчанні; Методи дистанційного навчання; Комп’ютерні та мультимедійні методи: використання освітніх мультимедійних презентацій.
Система поточного та підсумкового контролю	Поточний контроль: відвідування занять; поточна модульна робота Підсумковий контроль: залік
Мова викладання	Українська

Перелік компетентностей, які забезпечує дана навчальна дисципліна, програмні результати навчання

Програмні результати навчання	***Компетентності, якими повинен оволодіти здобувач***
Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.	Здатність застосовувати знання у практичних ситуаціях . Здатність до пошуку, оброблення та аналізу інформації з різних джерел . Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури

Тематичний план навчальної дисципліни

Назва теми	***Види робіт***	***Завдання самостійної роботи у розрізі тем***
Модуль 1. Модуль 1.Безпека і захист даних		
Тема 1. Інформаціна безпека Тема 2. Система персональних даних Тема 3. Апаратні засоби захисту даних Тема 4.Засоби, що містять небезпеку	Відвідування занять; захист домашнього завдання; обговорення матеріалу занять; виконання навчальних завдань; завдання самостійної роботи; тестування	опрацьовують матеріал лекцій; готуються до практичних завдань; виконують домашні роботи; працюють із літературою.
Модуль 2 Засоби криптографічного захисту		
Тема 5. Криптографічний захист даних Тема 6. Захист даних інформаційних мереж Тема 7. Захист даних глобальних мереж	відвідування занять; опитування на заняттях; опитування в процесі індивідуально консультативних занять для перевірки засвоєння матеріалу пропущених занять; перевірка виконання модульних контрольних робіт.	опрацьовують матеріал лекцій; готуються до лабораторних завдань; виконують домашні роботи; працюють із літературою.

Інформаційні джерела Основні;

1. Cyber Security Tutorial URL: https://www.w3schools.com/cybersecurity/index.php
2. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ.ун-т внутріш. справ, 2020. 128 с.
3. Вступ до кібербезпеки : навч. посіб. / О. А. Смірнов, О. К. Конопліцька-Слободенюк, С. А. Смірнов [та ін.] ; М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т. - Кропивницькицкий : ЦНТУ, 2022. – 968 с. URI https://dspace.kntu.kr.ua/handle/123456789/12524
4. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов : Новий світ-2000, 2024.- 658с.
5. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.

6. Інформаційна безпека та кібербезпека держави: навчальний посібник / [Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк,. С. М. Мамченко,. С. В .Ліра-К., 2024.-224с...
7. Основи кібербезпеки : навчально-практичний посібник / уклад. С. П. Євсеєв, О. В. Шматко, О. Б. Ахієзер, Т. В. Горбач ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 95 с. – (Серія «Кібербезпека та штучний інтелект»).
8. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв,О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.
9. ЛісовськаЮ.П. Кібербезпека: ризики та заходи: навчальний посібник."Кондор",2024.-272с.
10. Киптоаналіз. КриптографічніI протоколи / О.М. Гапак // Навчальний посібник з курсу «Комп'ютерна криптографія» для студентів інженерно-технічного факультету спеціальності 123-«Комп'ютерна інженерія». Ужгород: видавництво ПП «АУТДОР-ШАРК», 2021р. – 96с..
11. Організаційно-правові основи захисту службової 0-64 інформації: навч. посіб. /1. П. Касперський, С. 0. Князєв, О. І. Матяш та ін. - Київ : Нац. акад. СБУ, 2017.-120 с.
12. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf

Додаткові:

13. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.Організація захисту інформації з обмеженим доступом: навч. посіб. /А.М.Гуз, І.П.Касперський, С.О.Князєв та ін. – К.: Нац. акад., СБУ, 2018. –252 сСтандарти захисту персональних даних в соціальній сфері / М. В. Бем,, І. М. Городиський. – Львів: б.в., 2018. - 110 с.Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p. 12. Кібербезпека в сучасному світі : матеріали III Всеукраїнської науковопрактичної конференції (м. Одеса, 19 листопада 2021 р.) / за ред. О. В. Дикого ;уклад.: С. А. Горбаченко, Н. І. Логінова. – Одеса, 2020. – 148 с.
14. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с. https://jurkniga.ua/contents/osnovi-kiberprostoru-kiberbezpeki-ta-kiberzakhistu.pdf?srsltid=AfmBOorKh2lqya5I3cFXpDes2JYkOPXEJ-pUxtUL-U8W16zA7g_OaLDn
15. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.Інформаційна безпека/ За ред. Ю. Я. Бобала та І. В. Горбатого, Львівська політехніка, 2019.-540 с.
16. Online SNIA Dictionary A glossary of storage networking, data, and information management terminology. URL: https://www.snia.org/education/online-dictionary
17. Matt Bishop. Introduction to Computer Security URL: http://www.uoitc.edu.iq/images/documents/informaticsinstitute/exam_materials/Introduction%20to%20Computer%20Securit y%20pdf%20DONE.pdf
18. Public-key encryption, revisited : tight securityand richer functionalities RomainGay URL:https://tel.archivesouvertes.fr/tel-02137987/document

Програмне забезпечення навчальної дисципліни

Google сервіси
On-line середовище JSLinux https://jslinux.org/
Тренажери
Лінійні діофантові рівняння. Порівняння
Стандарт шифрування DES
Шифри із симетричним ключем

Політика вивчення навчальної дисципліни та оцінювання

Політика оцінювання здобувачів вищої освіти. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності). Перескладання модулів відбувається із дозволу провідного викладача за наявності поважних причин (наприклад, лікарняний).

Положення про організацію освітнього процесу

Положення про порядок та критерії оцінювання знань, вмінь та навичок здобувачів вищої освіти

Порядок ліквідації здобувачами вищої освіти академічної заборгованості

Політика щодо відвідування. Відвідування занять є обов'язковим компонентом. За об'єктивних

причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в режимі он-лайн.

Політика щодо академічної доброчесності. Здобувач повинен дотримуватися принципів академічної доброчесності, зокрема недопущення академічного плагіату, фальсифікації, фабрикації, списування під час поточного, рубіжного та підсумкового контролю. Списування під час контрольних робіт та поточних тестів заборонені (в т.ч. із використанням мобільних девайсів).

Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття. В ПУЕТ діють:

Кодекс честі студента

Положення про академічну доброчесність

Положення про запобігання випадків академічного плагіату

Політика визнання результатів навчання визначена такими документами:

Положення про порядок перезарахування результатів навчання, здобутих в іноземних та вітчизняних закладах освіти

Положення про академічну мобільність здобувачів вищої освіти

Положення про порядок визнання результатів навчання здобутих шляхом неформальної та/або інформальної освіти*; інфографіка* (розділ Освіта/Організація освітнього процесу/Неформальна освіта)

Політика вирішення конфліктних ситуацій:

Положення про правила вирішення конфліктних ситуацій

Положення про апеляцію результатів підсумкового контролю у формі екзамену

Уповноважена особа з питань запобігання та виявлення корупції

Політика підтримки учасників освітнього процесу:

Положення про психологічну службу Полтавського університету економіки і торгівлі

Психологічна служба

Положення про студентського омбудсмена

Студентський омбудсмен (Уповноважений з прав студентів) ПУЕТ

Уповноважений з прав корупції

Безпека освітнього середовища:

Інформація про безпечність освітнього середовища ПУЕТ наведена у вкладці «Безпека життєдіяльності»

Оцінювання

Підсумкова оцінка за вивчення навчальної дисципліни розраховується через поточне оцінювання

Вид діяльності	**Максимальна кількість балів за вид навчальної роботи**
Модуль 1..Безпека і захист даних	
Тема 1. Інформаціна безпека Практичні завдання	6
Тема 2. Система персональних даних Практичні завдання	3
Тема 3. Апаратні засоби захисту даних Практичні завдання	3
Тема 4. Засоби, що містять небезпеку (Апаратні) Практичні завдання	3
Модульний контроль	6
Всього за модулем 1	21
Модуль 2 Засоби криптографічного захисту	
Тема 5. Криптографічний захист даних Практичні завдання	24
Тема 6. Захист даних інформаційних мереж Практичні завдання	3
Тема 7. Захист даних глобальних мереж Практичні завдання	6
Поточна модульна робота	6
Всього за модулем 2	39

Поточний контроль	60
Підсумкове тестування	40
Всього по курсу	

Система нарахування додаткових балів за видами робіт з вивчення навчальної дисципліни

Форма роботи	Вид роботи	Бали
1. Навчальна	1. Виконання індивідуальних навчально-дослідних завдань підвищеної складності	10
2. Науково-дослідна	1. Участь у наукових гуртках	10
	2. Участь в наукових студентських конференціях: університетських, міжвузівських, всеукраїнських, міжнародних	20

За додаткові види навчальних робіт студент може отримати не більше 30 балів. Додаткові бали додаються до загальної підсумкової оцінки за вивчення навчальної дисципліни, але загальна підсумкова оцінка не може перевищувати 100 балів.

Шкала оцінювання здобувачів вищої освіти за результатами вивчення навчальної дисципліни

Сума балів за всі види навчальної діяльності	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою
90-100	A	Відмінно
82-89	B	Дуже добре
74-81	C	Добре
64-73	D	Задовільно
60-63	E	Задовільно достатньо
35-59	FX	Незадовільно з можливістю проведення повторного підсумкового контролю
0-34	F	Незадовільно з обов’язковим повторним вивченням навчальної дисципліни та проведенням підсумкового контролю