ПОЛТАВСЬКИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТОРГІВЛІ

Навчально-науковий інститут денної освіти

Кафедра комп'ютерних наук та інформаційних технологій

СИЛАБУС

навчальної дисципліни

«Захист інформації»

на 2026-2027 навчальний рік

Курс та семестр вивчення	4 курс ,8 семестр
Освітня програма/спеціалізація	122 Комп'ютерні науки
Код і найменування спеціальності	122 Комп'ютерні науки
Шифр і найменування галузі знань	12 Інформаційні технології
Рівень освіти, за яким здійснюється підготовка	перший (бакалаврський)

ПІБ НПП, який веде дану дисципліну науковий ступінь і вчене звання посада	Карнаухова Г.В., ст. викладач кафедри комп'ютерних наук та інформаційних технологій

Контактний телефон	+380970268704
Електронна адреса	ta.annet@gmail.com
Розклад навчальних занять	http://schedule.puet.edu.ua/
Консультації	очна http://www.matmodel.puet.edu.ua/, он-лайн: електронною поштою, Viber, Telegram ,пн-пт з 10.00-17.00
Сторінка дистанційного курсу	https://el.puet.edu.ua/

Опис навчальної дисципліни

Мета вивчення навчальної дисципліни	Основною метою вивчення дисципліни "Захист інформації" 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	4 кредити ЄКТС/120 годин (лекції 16 год., лабораторні заняття 32 год., самостійна робота 72 год.)
Форми та методи навчання	Лекції та практичні заняття в аудиторії, самостійна робота поза розкладом Наочні методи: ілюстрування. демонстрування, інфографіка Практичні методи: практичнізаняття, вирішення задач; моделювання ситуацій і об'єктів, творчі завдання Методи самостійної роботи вдома: проблемно -пошукові; проектного навчання; колективної розумової діяльності; застосування новітніх інформаційно-комунікаційних 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
Базові знання	Вивчення дисципліни базується на знаннях, отриманих студентами при вивченні дисциплін Алгебра та геометрія, Дискретна математика, Математична логіка, Математичний аналіз Операційні системи та системне програмування
Мова викладання	Українська

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

Програмні результати навчання	***Компетентності, якими повинен оволодіти здобувач***
ПР16. 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 (ЗК2). Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури (СК14).

Тематичний план навчальної дисципліни

Назва теми	***Види робіт***	***Завдання самостійної роботи у розрізі тем***
Модуль 1. Основні відомості про захист інформації		
Тема 1. Основні положення захисту інформації Тема 2. Комплексна система захисту інформації. Тема 3. Програмні засоби, що містять небезпеку Тема 4. Захист інформації в розподілених системах Тема 5. Захист інформації в глобальних мережах	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 6.Криптографія та криптологія. Тема 7.Системи блочного шифрування Тема 8. Системи симетричного шифрування. Тема 9. Системи асиметричного шифрування. Тема 10.Засоби аутентифікації та ідентифікації.	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. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). 7. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)
2. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT)
3. Про захист інформації в інформаційних, телекомунікаційних та інформаційнотелекомунікаційних системах: Закон України від 5 липня 1994 р. № 80/94-ВР: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua
4. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua
5. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого

доступу: НД ТЗІ 1.1-002-99. – К. ДСТСЗІ СБ України, 1999 – 16 с
6. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99.–К.: ДСТС31 СБ України, 1999. - 26 с.
7. А.М. КОТЕНКО, О.Л. ТУРОВСЬКИЙ, Г.В. ШУКЛІН, Ю.В. ПЕПА, І.С. ІВАНЧЕНКО, І.М. АВЕРІЧЕВ. Компонентна база засобів кібербезпеки та захисту інформації: Навчальний посібник. - К.: ДУІКТ. – 2025. 236 с. [Електронний ресурс]. – Режим доступу: https://duikt.edu.ua/ua/lib/1/category/2351/view/2376
8. 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.
9. Вишняков В.М. В55 Захист інформації в комп'ютерних системах: навч. посіб. / В.М. Вишняков. – Київ: КНУБА, 2022. – 120 с. [Електронний ресурс]. – Режим доступу: https://repositary.knuba.edu.ua/server/api/core/bitstreams/d3f95867-c34e-451b-a9f6-78246b40a7a8/content
10. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.
11. 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.
12. 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.
13. Яремчук, Ю. Є. Я72 Основи криптографічного захисту інформації : електронний навчальний посібник комбінованого (локального та мережного) використання [Електронний ресурс] / Яремчук Ю. Є., Салієва О. В., Бондаренко І. О. – Вінниця : ВНТУ, 2024. – 139 с.

Додаткові:

14. Вербівський Д., Якимчук Б. Криптологія : опорний коспект лекцій. Житомир : Видво ЖДУ ім. Івана Франка, 2023. 173 с.
15. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник.– К.: Видавництво НА СБ України, 2022. – 256 с.
16. Інформаційна безпека/ За ред. Ю. Я. Бобала та І. В. Горбатого, Львівська політехніка, 2019.-540 с.
17. Інформаційна безпека та кібербезпека держави./ Присяжнюк М.М., Рідей Н.М., Титова Н.М.,Ліра, 2024-.224 с ISBN. 978-617-520-744-4
18. Кібербезпека: лабораторний практикум з основ крипографічного захисту/ Євсеєв С.П. , Король О.Г. Новий світ-2000, 2021.-241 с.
19. 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.
20. Криптоаналіз. 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..
21. Технічний захист інформації: Навч. Пос. /Богуш В.М., Бровко В.Д., Кобус О.С., В.Д. Козюра В.Д., Ліра-К.,2023.- 508с.
22. Технології захисту інформації: навчальний посібник/ Остапов С.Е., Євсеєв С.П., Король О.Г.. – Х.: Новий світ-2000, 2022. – 678 с.
23. Online SNIA Dictionary A glossary of storage networking, data, and information management terminology. URL: https://www.snia.org/education/online-dictionary
24. Matt Bishop. Introduction to Computer Security URL: http://www.uoitc.edu.iq/images/documents/informaticsinstitute/exam_materials/Introduction%20to%20Computer%20Security%20pdf%20DONE.pdf
25. Public-key encryption, revisited : tight security and richer functionalities Romain Gay URL:https://tel.archives-ouvertes.fr/tel-02137987/document

Програмне забезпечення навчальної дисципліни

Сервіси Google
On-line середовище JSLinux https://jslinux.org/
Комплекси антивірусних програм
Архіватори
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 інформації	
Тема 1. Основні положення захисту інформації Практичне заняття 1 Тема 2. Комплексна система захисту інформації. Практичне заняття 2 Тема 3. Програмні засоби, що містять небезпеку Практичне заняття 3 Тема 4. Захист інформації в розподілених системах Практичне заняття 4-5 Тема 5. Захист інформації в глобальних мережах Практичне заняття 6-7	 3 3 3 6 6
Модульний контроль	6
Тестування за модулем	20
Всього за модулем 1	47
Модуль 2 Засоби криптографічного захисту	
Тема 6.Криптографія та криптологія. Практичне заняття 8 Практичне заняття 9 Практичне заняття 10 Практичне заняття 11 Тема 7.Системи блочного шифрування Практичне 12-13 Тема 8. Системи симетричного шифрування. Практичне заняття 14 Тема 9. Системи асиметричного шифрування. Практичне заняття 15 Тема 10.Засоби аутентифікації та ідентифікації. практичне заняття 16	 3 3 3 3 6 3 3 3
Поточна модульна робота	6
Тестування за модулем	20
Разом за модулем	53
Разом за курс	100

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