ПОЛТАВСЬКИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТОРГІВЛІ
Навчально-науковий інститут денної освіти
Кафедра комп'ютерних наук та інформаційних технологій

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ О.В. Ольховська
«_28__» _____06_____ 2024 р.

РОБОЧА ПРОГРАМА

навчальної дисципліни **«Захист інформації»**
освітня програма **Комп'ютерні науки**
спеціальність **122 Комп'ютерні науки**
галузь знань **12 Інформаційні технології**
ступінь вищої освіти **бакалавр**

Робоча програма навчальної дисципліни «Захист інформації» рекомендована до використання в освітньому процесі на засіданні кафедри комп'ютерних наук та інформаційних технологій
Протокол від 28.06.24 року, №___13___

Полтава 2024

Укладач: Карнаухова Г.В., ст. викладач кафедри комп’ютерних наук та інформаційних технологій.

ПОГОДЖЕНО:

Гарант освітньої програми «Комп’ютерні науки» спеціальності 122 Комп’ютерні науки ступеня бакалавра, к.ф.-м.н, доцент

_____ О.О. Черненко

«__28__»_____06_____2024 року

Зміст
робочої програми начальної дисципліни

Зміст

Розділ 1. Опис навчальної дисципліни

Таблиця 1. Опис навчальної дисципліни «Захист інформації»

Місце у структурно-логічній схемі підготовки	*Пререквізити*: Алгебра та геометрія, Дискретна математика, Математична логіка, Математичний аналіз Операційні системи та системне програмування *Постреквізити*: Курсовий проект з фаху, Виробнича практика, Переддипломна практика
Мова викладання	Українська
Статус дисципліни	Вибіркова
Курс/семестр вивчення	4/8
Кількість кредитів ECTS/кількість модулів	4/2
Денна форма навчання:	
Кількість годин: 120 год – загальна кількість: 2 семестр – 120 год.	
- Лекції: 16 год.	
- Практичні (семінарські, лабораторні) заняття: 32 год.	
- Самостійна робота: 72 год.	
- Вид підсумкового контролю (ПМК, екзамен): 2 семестр - залік	
Заочна форма навчання:	
Кількість годин: 120 год – загальна кількість: 2 семестр – 90 год.	
- Лекції: 4 год.	
- Практичні (семінарські, лабораторні) заняття: 2 год.	
- Самостійна робота: 114 год.	
- Вид підсумкового контролю (ПМК, екзамен): 1 семестр - залік	

Розділ 2. Перелік компетентностей та програмні результати навчання

Метою навчальної 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

Таблиця 2. Перелік компетентностей та програмні результати навчання, які забезпечує навчальна дисципліна «Захист інформації»

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 до пошуку, оброблення та аналізу інформації з різних джерел (ЗК7). Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури (СК14).

Розділ 3. Програма навчальної дисципліни

Модуль 1.Безпека і захист даних

Тема 1. Теоретичні основи інформаційної безпеки

Вступ до захисту інформації Цілі підтримки безпеки. Атаки. Послуги і механізми. Методи Характеристика інформаційної безпеки Умови безпеки інформації Державна політика та система технічного захисту інформації в Україні. Нормативно-правова база України у сфері технічного захисту інформації Структура системи захисту інформації

Тема 2. Інформаційна система персональних даних

Нормативні документи захисту даних. Конфіденційність персональних даних Захист персональної інформації Європейська система захисту персональних даних

Тема 3. Апаратні засоби захисту інформації

Основи апаратного захисту Класифікація технічних засобів зняття інформації Основні групи технічних засобів ведення розвідки Радіомікрофони Основні методи прослуховування телефонних ліній Телефонні радіотранслятори. Системи прослуховування повідомлень, переданих по стільникових, пейджингових каналах і по факсу.Використання телефонної лінії для прослуховування приміщень. Спеціальні пристрої прослуховування Системи і пристрої відеоконтролю Пристрої дистанційного управління, відеодетектор рухуСистеми та засоби виявлення, пошуку та знешкоджування технічних засобів зняття інформації. Основні стаціонарні засоби захисту інформації. Пошукове устаткування

Тема 4. Програмні засоби, що містять небезпеку

Перехоплювачі паролів першого роду. Перехоплювачі паролів другого роду. Перехоплювачі паролів третього роду. Принципи роботи троянських програм . Принципи роботи утиліт скритого адміністрування Комп'ютерні віруси і механізми боротьби з ними Класифікація комп'ютерних вірусів. Методи і засоби боротьби з вірусами. Пакетні фільтри

Модуль 2 Засоби криптографічного захисту

Тема 5. Криптографічний захист інформації

Криптографічні методи захисту Основи криптоаналізу. Стеганографія Історія криптографії. Класифікація та вимоги до сучасних

криптосистем. Традиційні шифри із симетричним ключем. Шифри із симетричним ключем. Шифр підстановки Шифри із симетричним ключем. Шифр перестановки. Шифри потоку і блокові шифри. Алгебраїчні структури Криптографія із симетричними ключами. Сучасні блокові шифри Сучасні шифри потоку Стандарт шифрування даних (DES). Аналіз DES. Багатократне застосування. Загальний опис криптоалгоритму стандарту шифрування AESC. Симетричні криптосистеми. Шифр Калина. Режими роботи симетричних криптоалгоритмів Математичні основи асиметричної криптографії. Криптосистеми RSA та Ель-Гамаля. Поняття електронного цифрового підпису. Електронний цифровий підпис DSA та ECDSA. Криптографічні функції хешування.

Тема 6. Безпека в комп'ютерних мережах

Використання міжмережевих екранів. Політика безпеки під час роботи в мережі

Тема 7. Захист інформації в глобальних мережах

Загальні принципи побудови глобальних комп'ютерних мереж. Політика безпеки при роботі в глобальній мережі. Погрози при роботі з глобальними мережами. Реагування на інциденти в глобальній мережі.

Розділ 4. Тематичний план вивчення навчальної дисципліни

Таблиця 3. Тематичний план навчальної дисципліни

Назва теми (лекції) та питання теми (лекції)	Кількість годин	Назва теми та питання семінарського, практичного або лабораторного заняття	Кількість годин	Завдання самостійної роботи в розрізі тем	Кількість годин
Модуль 1.Безпека і захист даних					
Тема 1. Теоретичні основи інформаційної безпеки Лекція 1 Вступ до захисту інформації Характеристика інформаційної безпеки Умови безпеки інформації Державна політика та система технічного захисту інформації в Україні. Нормативно-правова база України у сфері технічного захисту інформації Структура системи захисту інформації	2	Практичне заняття1 Практичне заняття 2	2 2	Опрацьовувати лекційний матеріал, готуватись до практичних занять, виконувати індивідуальні завдання, опрацьовувати дистанційний курс, виконувати тести, готуватися до модульної контрольної роботи та заліку	4 4
Тема 2. Інформаційна система персональних даних Лекція 2. Нормативні документи захисту даних. Конфіденційність персональних даних Захист персональної інформації Європейська система захисту	2	Практичне заняття 3	2		4

Назва теми (лекції) та питання теми (лекції)	Кількість годин	Назва теми та питання семінарського, практичного або лабораторного заняття	Кількість годин	Завдання самостійної роботи в розрізі тем	Кількість годин
персональних даних Тема 3. Апаратні засоби захисту інформації Основи апаратного захисту Класифікація технічних засобів зняття інформації Основні групи технічних засобів ведення розвідки Тема 4. Програмні засоби, що містять небезпеку Лекція 3. Перехоплювачі паролів Троянські програми Утиліти скритого адміністрування Вірусні програми Міжмережеві екрани Пакетні фільтри.	2	Практичне заняття 4 Практичне заняття 5	2 2		8 4 4
Зарахування теми 1, 4 при опрацюванні та наявності сертифікату з курсу"Основи інформаційної безпеки" та "Інформаційна безпека", платформі Prometheus					
Модуль 2 Засоби криптографічного захисту					
Тема 5. Криптографічний захист інформації Лекція 4. Криптографія Шифрування, дешифрування, ключі шифрування Криптостійкість, криптоаналіз Лекція 5. Шифри з симетричним ключем Сучасні блокові шифри Сучасні шифри потоку Стандарт шифрування даних (DES). Загальний опис криптоалгоритму стандарту шифрування AESC Лекція 6.Асиметрична криптографія Математичні основи асиметричної криптографії. Криптосистеми RSA та Ель-Гамаля. Електронний цифровий підпис DSA та ECDSA. Криптографічні функції хешування. Тема 6. Безпека в комп’ютерних мережах	2 2 2 2	Практичне заняття 6 Практичне заняття 7 Практичне заняття 8 Практичне заняття 9 Практичне заняття 10 Практичне заняття 11 Практичне заняття 12 Практичне заняття 13 Практичне заняття 14	2 2 2 2 2 2 2 2 2	Опрацьовувати лекційний матеріал, готуватись до практичних занять, виконувати індивідуальні завдання, опрацьовувати дистанційний курс, виконувати тести, працювати з тренажерами, розміщеними в дистанційному курсі, готуватися до поточної контрольної роботи та заліку	4 4 4 4 4 4 4 4 4

Назва теми (лекції) та питання теми (лекції)	Кількість годин	Назва теми та питання семінарського, практичного або лабораторного заняття	Кількість годин	Завдання самостійної роботи в розрізі тем	Кількість годин
Лекція 7 Використання міжмережевих екранів. Принцип роботи брандмауера. Різновиди брандмауерів	2				
Тема 7. Захист інформації в глобальних мережах		Практичне заняття 15	2		4
Лекція 8 Політика безпеки при роботі в глобальній мережі. Загрози при роботі з глобальними мережами. Реагування на інциденти в глобальній мережі.	2	Практичне заняття 16	2		4
Зарахування теми 7 при опрацюванні та наявності сертифікату з курсу"Основи інформаційної безпеки" та "Інформаційна безпека", платформі Prometheus					
Всього, годин	16		32		72

Розділ 5. Оцінювання результатів навчання

Таблиця 5. Розподіл балів за результатами вивчення навчальної дисципліни

Вид діяльності	Максимальна кількість балів за вид навчальної роботи
Модуль 1..Безпека і захист даних	
Тема 1. Теоретичні основи інформаційної безпеки Практичне заняття 1 Практичне заняття 2	 3 3
Тема 2. Інформаційна система персональних даних Практичне заняття 3	 3
Тема 3. Апаратні засоби захисту інформації Практичне заняття 4	 3
Тема 4. Програмні засоби, що містять небезпеку Практичне заняття 5	 3
Модульний контроль	6
Всього за модулем 1	21
Модуль 2 Засоби криптографічного захисту	
Тема 5. Криптографічний захист інформації Практичне заняття 6 Практичне заняття 7 Практичне заняття 8 Практичне заняття 9 Практичне заняття 10 Практичне заняття 11 Практичне заняття 12 Практичне заняття 13	 3 3 3 3 3 3 3 3

Вид діяльності	Максимальна кількість балів за вид навчальної роботи
Тема 6. Безпека в комп'ютерних мережах Практичне заняття 14	 3
Тема 7. Захист інформації в глобальних мережах Практичне заняття 15 Практичне заняття 16	 3 3
Поточна модульна робота	6
Всього за модулем 2	39
Поточний контроль	60
Підсумковий контроль	40
Всього за курсом	100

Таблиця 5.2. 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

Таблиця 6 – Шкала оцінювання знань 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

Розділ 6. Інформаційні джерела

Інформаційні джерела

Основні;

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. 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.
4. 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.
5. 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.
6. Кібербезпека: лабораторний практикум з основ крипографічного захисту/ Євсеєв С.П. , Король О.Г. Новий світ-2000, 2021.-241 с.
7. Комплексні системи захисту інформації : навчальний посібник / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. – Вінниця : ВНТУ, 2018. – 118 с. [Електронний ресурс]. – Режим доступу: http://pdf.lib.vntu.edu.ua/books/IRVC/Yaremchuk_2018_118.pdf
8. Криптоаналіз. КриптографічніІ 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..
9. Логінова Н. І. Правовий захист інформації : навч. посібн. / Н. І. Логінова, Р. Р. Дробожур. - Одеса : Фенікс, 2015. - 264 с.
10. 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.
11. 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:

12. 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.

13. 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. Online SNIA Dictionary A glossary of storage networking, data, and information management terminology. URL: https://www.snia.org/education/online-dictionary

15. Matt Bishop. Introduction to Computer Security URL: http://www.uoitc.edu.iq/images/documents/informaticsinstitute/exam_materials/Introduction%20to%20Computer%20Security%20pdf%20DONE.pdf

16. Public-key encryption, revisited : tight security and richer functionalities Romain Gay URL:https://tel.archives-ouvertes.fr/tel-02137987/document

Розділ 7. Програмне забезпечення навчальної дисципліни

- Пакет програмних продуктів Microsoft Office.
- Дистанційний курс з навчальної дисципліни «Теорія програмування» на платформі «Moodle»
- On-line середовище JSLinux https://jslinux.org/
- Тренажери
    - Лінійні діофантові рівняння. Порівняння
- Стандарт шифрування DES
- Шифри із симетричним ключем