ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД УКООПСПІЛКИ
«ПОЛТАВСЬКИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТОРГІВЛІ»
Навчально-науковий інститут денної освіти
Кафедра комп'ютерних наук та інформаційних технологій

ЗАТВЕРДЖУЮ
Завідувач кафедри КНІТ
_____ Олена ОЛЬХОВСЬКА
«25» січня 2023 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 25 січня 2023 року, №8

Полтава 2023

Укладач:
Парфьонова Т.О., доцент кафедри комп'ютерних наук та інформаційних технологій, к.ф.-м.н.
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

Оксана ЧЕРНЕНКО

«25» січня 2023 року

Зміст
робочої програми навчальної 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	4/2
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 - пмк	
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 - пмк	

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***
ПР1. Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук. ПР2. Використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв'язання задач теоретичного та прикладного характеру в процесі проектування та реалізації об'єктів інформатизації. ПР16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.	Здатність до абстрактного мислення, аналізу та синтезу (ЗК1). Здатність застосовувати знання у практичних ситуаціях (ЗК2). Знання та розуміння предметної області та розуміння професійної діяльності (ЗК3). Здатність спілкуватися державною мовою як усно, так і письмово (ЗК4). Здатність вчитися й оволодівати сучасними знаннями (ЗК6). Здатність до пошуку, оброблення та аналізу інформації з різних джерел (ЗК7). Здатність генерувати нові ідеї (креативність) (ЗК8). Здатність працювати в команді (ЗК9). Здатність бути критичним і самокритичним (ЗК10). Здатність приймати обґрунтовані рішення (ЗК11). Здатність оцінювати та забезпечувати якість виконуваних робіт (ЗК12) Здатність до математичного формулювання та досліджування неперервних та дискретних математичних моделей, обґрунтовування вибору методів і підходів для розв'язування теоретичних і прикладних задач у галузі комп'ютерних наук, аналізу та інтерпретування (СК1). 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	Лабораторна робота1 Лабораторна робота 2	2 2	Опрацьовувати лекційний матеріал, готуватись до лабораторних 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 персональних даних	2	Лабораторна робота 3	2		4
Тема 3. Апаратні засоби захисту інформації Основи апаратного захисту Класифікація технічних засобів зняття інформації Основні групи технічних засобів ведення розвідки		Лабораторна робота 4	2		8 4
Тема 4. Програмні засоби, що містять небезпеку Лекція 3. Перехоплювачі паролів Троянські програми Утиліти скритого адміністрування Вірусні програми Міжмережеві екрани Пакетні фільтри.	2	Лабораторна робота 5	2		4
Модуль 2 Засоби криптографічного захисту					
Тема 5. Криптографічний захист				Опрацьовувати	

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
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 Лекція 7 Використання міжмережевих екранів. Принцип роботи брандмауера. Різновиди брандмауерів Тема 7. Захист інформації в глобальних мережах Лекція 8 Політика безпеки при роботі в глобальній мережі. Загрози при роботі з глобальними мережами. Реагування на інциденти в глобальній мережі.	2 2 2 2 2 2 2 2 2	Лабораторна робота 6 Лабораторна робота 7 Лабораторна робота 8 Лабораторна робота 9 Лабораторна робота 10 Лабораторна робота 11 Лабораторна робота 12 Лабораторна робота 13 Лабораторна робота 14 Лабораторна робота 15 Лабораторна робота 16	2 2 2 2 2 2 2 2 2 2 2	лекційний матеріал, готуватись до лабораторних занять, виконувати індивідуальні завдання, опрацьовувати дистанційний курс, виконувати тести, працювати з тренажерами, розміщеними в дистанційному курсі, готуватися до модульної контрольної роботи та заліку	4 4 4 4 4 4 4 4 4 4 4
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**

Вид діяльності	Максимальна кількість балів за вид навчальної роботи
Модуль 1..Безпека і захист даних	
Тема 1. Теоретичні основи інформаційної безпеки Лабораторна робота 1 Лабораторна робота 2	 3 3
Тема 2. Інформаційна система персональних даних Лабораторна робота 3	 3
Тема 3. Апаратні засоби захисту інформації Лабораторна робота 4	 3
Тема 4. Програмні засоби, що містять небезпеку Лабораторна робота 5	 3
Модульний контроль	6
Всього за модулем 1	21
Модуль 2 Засоби криптографічного захисту	
Тема 5. Криптографічний захист інформації Лабораторна робота 6 Лабораторна робота 7 Лабораторна робота 8 Лабораторна робота 9 Лабораторна робота 10 Лабораторна робота 11 Лабораторна робота 12 Лабораторна робота 13	 3 3 3 3 3 3 3 3
Тема 6. Безпека в комп'ютерних мережах Лабораторна робота 14	 3
Тема 7. Захист інформації в глобальних мережах Лабораторна робота 15 Лабораторна робота 16	 3 3
Поточна модульна робота	6
Всього за модулем 2	39
Поточний контроль	60
Підсумковий контроль	40
Всього за курсом	100

Розділ 6. Інформаційні джерела

1. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.
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.
4. Інформаційна безпека/ За ред. Ю. Я. Бобала та І. В. Горбатого, Львівська політехніка, 2019.-540 с.
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. 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.
7. Кібербезпека в сучасному світі : матеріали III Всеукраїнської науково практичної конференції (м. Одеса, 19 листопада 2021 р.) / за ред. О. В. Дикого ;уклад.: С. А. Горбаченко, Н. І. Логінова. – Одеса, 2020. – 148 с.
8. Кібербезпека: лабораторний практикум з основ криптографічного захисту/ Євсеєв С.П. , Король О.Г. Новий світ-2000, 2021.-241 с.
9. 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..
10. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
11. Логінова Н. І. Правовий захист інформації : навч. посібн. / Н. І. Логінова, Р. Р. Дробожур. - Одеса : Фенікс, 2015. - 264 с.
12. 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.
13. 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 с
14. Стандарти захисту персональних даних в соціальній сфері / М. В. Бем,, І. М. Городиський. –Львів: б.в., 2018. - 110 с.
15. 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

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