Кам'янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет

Кафедра комп'ютерних наук

1. Загальна інформація про курс

Назва курсу, мова викладання	ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ, мова викладання – українська
Викладач	Мястковська Марина Олександрівна, кандидат педагогічних наук, старший викладач кафедри комп'ютерних наук; Кух Оксана Михайлівна, асистент кафедри комп'ютерних наук
Профайл викладача	https://cs.kpnu.edu.ua/2019/11/04/miastkovska-maryna-oleksandrivna/ https://cs.kpnu.edu.ua/2019/11/04/kukh-oksana-mykhajlivna/
E-mail:	myastkovska.maryna@kpnu.edu.ua okukh@kpnu.edu.ua
Сторінка курсу в MOODLE	https://moodle.kpnu.edu.ua/course/view.php?id=19762
Консультації	Розклад проведення консультацій: щовівторка з 15-10 до 16-10 в ауд. №29 корпусу №4; формат консультацій – групові та індивідуальні у вигляді співбесіди

2. Анотація до курсу

Навчальна дисципліна спрямована на застосування знань 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; розуміння концепції інформаційної безпеки, принципів безпечного проектування програмного забезпечення, забезпечення безпеки комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

3. Мета і завдання курсу

Метою викладання дисципліни є ознайомити з принципами побудови та використання програмних та програмно-апаратних засобів для захисту програмного забезпечення та іншої інформації в комп'ютерних системах.

4. Результати навчання

Програмні результати навчання, визначені освітньою програмою*:*

- ПРН 01 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.

– ПРН 15 Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних

5. Формат курсу

Стандартний курс (очний).

6. Обсяг і ознаки курсу

Інформація з робочої програми навчальної дисципліни:

Найменування показників	Характеристика навчального курсу
Освітня програма, спеціальність	Освітньо-професійна програма: *Комп’ютерні науки та інформаційні технології* спеціальність: 122 *Комп’ютерні науки*
Рік навчання/ рік викладання	Третій (другий)
Семестр вивчення	П’ятий та третій
нормативна/вибіркова	нормативна
Кількість кредитів ЄКТС	4 кредити ЄКТС
Загальний обсяг годин	120 год.
Кількість годин навчальних занять	48 год.
Лекційні заняття	16 год.
Лабораторні заняття	32 год.
Самостійна та індивідуальна робота	72 год.
Форма підсумкового контролю	екзамен

7. Пререквізити курсу

Знання розділів програмування, комп’ютерних мереж.

8. Технічне й програмне забезпечення /обладнання

Лабораторії обчислювальної техніки, довільне середовище програмування.

9. Політика курсу

Увесь навчальний контент розміщено в модульному середовищі навчання К-ПНУ імені Івана Огієнка – moodle. Підготовка та виконання завдань і модульної контрольної роботи є обов’язковим для кожного студента.

Академічна доброчесність. Очікується, що роботи студентів будуть їх власними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел списування, втручання в роботу інших студентів становлять приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.

Відвідання занять. Очікується, що всі студенти відвідають усі лекції та лабораторні заняття курсу. Студенти мають інформувати викладача про неможливість відвідати заняття. Для того, щоб опрацювати питання пропущеної лекції чи лабораторного заняття, студент повинен підготуватись і під час консультації відповісти на питання викладача, які дозволяють оцінити глибину освоєння відповідного матеріалу. Студенти зобов'язані дотримуватися термінів виконання усіх видів робіт, передбачених курсом.

Форми поточного та підсумкового контролю. Поточний контроль реалізується на лабораторних заняттях. Наприкінці змістового модуля студент виконує модульну контрольну роботу (МКР). Зразки завдань модульної контрольної роботи розміщено в модульному середовищі навчання К-ПНУ імені Івана Огієнка – moodle; варіант для виконання студент отримує у викладача. *Модульну контрольну роботу, що виконана неуспішно, студент повинен виконати повторно.*

Підсумковий контроль зі змістового модуля (допуск до екзамену) виставляється за результатами поточного контролю і модульної контрольної роботи.

10. Схема курсу

Назви змістових модулів і тем	Кількість годин			
	разом	у тому числі		
		Лекційні заняття	Лабораторні заняття	Самостійна та індивідуальна робота
Змістовий модуль 1. Основи інформаційної безпеки. Способи та методи захисту інформації				
Тема 1. Основи інформаційної безпеки. Класифікація загроз.	16	4	4	8
Тема 2. Засоби антивірусного захисту інформації.	10	2		8
Тема 3. Системний підхід до захисту інформації.	10	2		8
Тема 4. Стандарти і нормативне забезпечення захисту інформації.	10	2		8
Тема 5. Криптографічні методи захисту інформації.	42	4	18	20
Тема 6. Інфраструктура відкритого ключа. Цифровий підпис.	18		6	12
Тема 7. Комплекс заходів із захисту інформації.	14	2	4	8
Разом годин	**120**	**16**	**32**	**72**

11. Система оцінювання та вимоги

Оцінювання на навчальних заняттях здійснюється за 12-ти бальною шкалою. Для визначення рейтингу поточної успішності враховуються оцінки за практичні заняття. Рейтингова оцінка поточної успішності студента визначається лише за умови відсутності у нього академічної заборгованості за навчальні заняття за формулою: (0,05 × середня оцінка навчальної діяльності на навчальних заняттях + 0,4) × ваговий бал оцінювання результатів навчальної діяльності на навчальних заняттях і повинна бути ≥ 60% від вагового балу оцінювання (табл. 1).

Модульна контрольна робота (МКР) вважається виконаною, якщо її оцінено в ≥ 60% від вагового балу за МКР. Невиконання МКР оцінюється в 0 балів. Рейтингова оцінка за змістовий модуль є сумою рейтингової оцінки поточної успішності студента та оцінки за МКР.

Таблиця 1

Розподіл балів за поточний і модульний контроль відповідно до робочої програми навчальної дисципліни

Поточний і модульний контроль (60 балів)		**Екзамен**	**Сума**
Змістовий модуль 1 (60 балів)		40	100
Поточний контроль	МКР		
50 балів	10 балів		

Підсумковий семестровий контроль з навчальної дисципліни передбачений у формі екзамену.

Відповідно до Положення про екзамени і заліки та порядок перезарахування навчальних дисциплін, (від 01.11.2019 р. за № 109-ОД) здобувач вищої освіти вважається допущеним до семестрового екзамену, якщо він виконав усі види робіт, передбачені робочою програмою навчальної дисципліни на семестр. Студенти, які мають академічну заборгованість за результатами поточного контролю, не допускаються до складання семестрового екзамену. Семестровий екзамен студенти складають у період екзаменаційної сесії за розкладом, складеним деканатом.

Рейтингова оцінка з навчальної дисципліни, підсумковий контроль з якої передбачений у формі семестрового екзамену, визначається як сума рейтингової оцінки за результатами поточної успішності студентів та рейтингової оцінки за результатами семестрового екзамену. Оцінювання здобувачів вищої освіти здійснюється відповідно до Таблиці відповідності шкал оцінювання навчальних досягнень студентів (табл. 2).

Студенти, які були не допущені або отримали незадовільну оцінку на екзамені, ліквідовують академічну заборгованість після належної підготовки до початку наступного семестру в терміни, визначені графіком ліквідації академічної заборгованості, який розробляє деканат і затверджує декан факультету.

Таблиця 2

Таблиця відповідності шкал оцінювання навчальних досягнень студентів

Рейтингова оцінка з кредитного модуля (навчальної дисципліни)	Підсумкова оцінка за шкалою ECTS	Рекомендовані системою ECTS статистичні значення (у %)	Підсумкова оцінка за національною шкалою	
			екзаменаційна	залікова
90-100	A (відмінно)	10	відмінно	зараховано
82-89	B (добре)	25	добре	
75-81	C (добре)	30		
67-74	D (задовільно)	25	задовільно	
60-66	E (достатньо)	10		
35-59	FX (незадовільно з можливістю повторного складання)		незадовільно	не зараховано
34 і менше	F (незадовільно з обов'язковим проведенням додаткової роботи щодо вивчення навчального матеріалу кредитного модуля)			

12. Рекомендована література

основна

1. Анин Б.Ю. Защита компьютерной информации. СПб.: БХВ-Петербург. 2000. 384 с.
2. Вакалюк Т.А. Захист інформації в комп'ютерних системах. Навчально-методичний посібник для студентів напряму 6.040302 Інформатика*. Житомир: Вид-во ЖДУ, 2013. 136 с.
3. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. / Л.Л. Гончарова, А.Д. Возненко, О.І. Стасюк, Ю.О. Коваль. К: Редакційно-видавничий відділ ДЕТУТ, 2013. 435 с.
4. Основы криптографии: Учебное пособие / А.Алферов, А. Зубов, А. Кузьмин, А. Черемушкин. Москва: Гелиос АРВ, 2002. 480 с.
5. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник. / В. В. Поповский, А.В. Персиков. – Харьков: Компания СМИТ, 2006. Ч. 1. 350 с.
6. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник. / В. В. Поповский, А.В. Персиков. Харьков: Компания СМИТ, 2006. Ч. 2. 294 с.
7. Технології захисту інформації : навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. Х. : Вид. ХНЕУ, 2013. 476 с. (Укр. мов.)

додаткова

8. ISO 17799: 2002. Управление информационной безопасностью. Практические правила.

9. Аграновский А.В., Хади Р.А. Практическая криптография. М.: СОЛОН-Пресс. 2002. 256 с.
10. Барсуков В. Современные технологии безопасности. М.: Нолидж, 2001
11. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-001-98, ДСТСЗІ СБ України, Київ, 1998.
12. Зак Диана. Самоучитель Visual Basic .NET К., 2003.
13. Закон України "Про захист інформації в автоматизованих системах". Відомості Верховної Ради (ВВР). 1994. № 31.
14. Закон України "Про інформацію". № 2658 від 2 жовтня 1992 року.
15. Закон України "Про науково-технічну інформацію". Відомості Верховної Ради (ВВР). 1993. № 33.
16. Закон України "Про телекомунікації" (Проект 01.06.2000).
17. Закон України «Про державну таємницю», від 21.01.94.
18. Закон України «Про захист інформації в автоматизованих системах», від 05.07.94.
19. Закон України «Про інформацію», від 02.10.92.
20. Закон України «Про науково-технічну інформацію», від 25.06.93.
21. Закон України про Національну програму інформатизації, від 04.02.98.
22. Зима В. Безопасность глобальных сетевых технологий. СПб.: BHV-СПб, 2001.
23. Ивьен, Билл, Берес, Джейсон Visual Basic .NET Библия пользователя. Пер. с англ. - М.: Изд. дом «Вильямс», 2002, 1024с., ил.
24. Информатика. Базовый курс/ Симонович С.В. и др. СПб: Издательство «Питер», 2000. 640 с.: ил.
25. Информатика: учебное пособие для студентов пед. вузов. / А.В. Могилев, Н.И. Пак, Е.К. Хеннер; Под редакцией Е.К. Хеннера М., 1999 816 с.
26. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави від 27 листопада 1998 року № 1893.
27. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.2.-002 98, ДСТСЗІ СБ України, Київ, 1998.
28. Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року № 2171-III.
29. Концепція технічного захисту інформації в Україні від 8 жовтня 1997 року № 1126.
30. Корнелл Г., Моррисон Дж. Програмирование на VB.NET: учебный курс СПб: Питер, 2002. 400с.:ил.
31. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. НД ТЗІ 2.2-001-98, ДСТСЗІ СБ України, Київ, 1998.
32. Медведовский Илья. Программные средства проверки и создания политики безопасности, соответствующей ISO 17799.
33. Методические указания по работе с программным комплексом Digital Security Office 2006. Спб.: Digital Security Company. 2006.
34. Методичні вказівки для виконання лабораторних робіт з курсу «Захист комп’ютерної інформації» студентами спеціальності 6.080200 «Прикладна математика». / Слободянюк О.В. Кам’янець-Подільський: Кам’янець-

Подільський державний університет, редакційно-видавничий відділ, 2008. 62 с.
35. Методичні вказівки для виконання лабораторних та самостійних робіт з дисципліни «Основи захисту та кодування інформації» студентами спеціальностей 7.080200, 8.080200 «Прикладна математика». Частина І./ П.В. Ольшанський, Рівне: УДУВГП, 2004, 52 с.
36. Методичні вказівки для виконання лабораторних та самостійних робіт з дисципліни «Основи захисту та кодування інформації» студентами спеціальностей 7.080200, 8.080200 «Прикладна математика». Частина ІІ./ П.В. Ольшанський, Рівне: УДУВГП, 2004, 60 с.
37. Положення про порядок здійснення криптографічного захисту інформації в Україні від 22 травня 1998 року № 505/98.
38. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99.
39. Поповский В.В. Основы криптографической защиты информации в телекоммуникационных системах / В. В. Поповский, А. В. Персиков. Харьков: Компания СМИТ, 2010 . Ч. 1. 350 с.
40. Поповский В.В. Основы криптографической защиты информации в телекоммуникационных системах / В. В. Поповский, А. В. Персиков. - Харьков: Компания СМИТ, 2010. Ч. 2. 294 с.
41. Постанова Кабінет Міністрів України "Про деякі питання захисту інформації, охорона якої забезпечується державою" від 13 березня 2002 р.
42. Смит Ричард. Аутентификация: от паролей до открытых ключей. : Пер. с англ. М.: Издательский дом «Вильямс», 2002. 432 с. : ил.
43. Соколов А.В. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ – Петербург; Арлит. – 2002. 496 с.
44. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-002-98, ДСТСЗІ СБ України, Київ, 1998.
45. Щербаков Л.Ю., Домашев А.В. Прикладная криптография. Использование и синтез криптографических интерфейсов. М: Издательско-торговый дом «Русская Редакция», 2003. 416 с.

Рекомендовані джерела інформації

1. Cryptography API: Next Generation https://learn.microsoft.com/en-us/windows/win32/seccng/cng-portal
2. Автозавантаження програм Windows 10 – Поради для всіх (poradu.com.ua)
3. Вакалюк Т.А. Захист інформації в комп'ютерних системах. Навчально-методичний посібник для студентів напряму 6.040302 Інформатика*. [Електронний ресурс]. 2013. Режим доступу до ресурсу: http://eprints.zu.edu.ua/9650/1/1.pdf
4. Електронний навчально-методичний комплекс «Захист інформації». [Електронний ресурс]. 2013. Режим доступу: https://sites.google.com/site/zahinf/
5. Електронний навчально-методичний комплекс «Захист інформації». [Електронний ресурс]. 2016. Режим доступу: http://moodle.kpnu.edu.ua/course/view.php?id=187
6. Огляд диспетчера завдань Windows 10 і його процесів (pro-computer.pp.ua)
7. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. [Електронний ресурс] / Л.Л. Гончарова, А.Д. Возненко, О.І. Стасюк, Ю.О. Коваль. 2013. Режим доступу до ресурсу: https://goo.gl/2ZW5zB.

8. Саксонов Г.М. Методи побудови та аналізу криптосистем. Методичні рекомендації до виконання лабораторних робіт з дисципліни для студентів-магістрів спеціальності 125 Кібербезпека галузі знань 12 Інформаційні технології / Упоряд.: Г.М. Саксонов, О.А. Жукова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». Дніпро: НТУ, 2019. 51 с. [Електронний ресурс]. – Режим доступу до ресурсу: http://ir.nmu.org.ua/handle/123456789/154142

9. Технології захисту інформації : навчальний посібник. [Електронний ресурс] / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. 2013. Режим доступу до ресурсу: https://goo.gl/7iQfoM.

10.Як Видалити Тимчасові Файли В Windows 10 - M'який (Cyberschool.Ac)

11.Як переглянути технічні характеристики ПК з Windows 10 | Новини Windows (windowsnoticias.com)