Силабус навчальної дисципліни
«Технології захисту інформації»

Спеціальність	122 КОМП'ЮТЕРНІ НАУКИ
Освітня програма	Комп'ютерні науки
Освітній рівень	*перший (бакалаврський)*
Статус дисципліни	*обов'язкова*
Мова викладання	*Українська*
Курс / семестр	*4 курс, 7 семестр*
Кількість кредитів ЄКТС	4
Розподіл за видами занять та годинами навчання	*Лекції – 16 год.*
	Лабораторні - 32год.
	Самостійна робота - 38 год.
	Індивідуальна робота – 34 год.
Форма підсумкового контролю	Екзамен
Кафедра	Кафедра комп'ютерних та інформаційних технологій і систем, *Аудиторія 104-Л, https://nupp.edu.ua/page/kafedra-kompyuternikh-ta-informatsiynikh-tekhnologiy-i-sistem.html кафедри на сайті університету*
Викладач (-і)	*Головко Геннадій Вячеславович, к.т.н., доцент*
Контактна інформація викладача	*genvgolovko@ukr.net*
Дні занять	*За розкладом, відповідно до графіку навчального процесу*
Консультації	*аудиторія 103-Л, 206-Л відповідно до графіку*

Мета навчальної дисципліни –навчити студентів правильно проводити аналіз погроз безпеці інформації, організовувати політику безпеки згідно світовим стандартам, закласти математичний та термінологічний фундамент в галузі криптології, основним методам, механізмам, алгоритмам та протоколам криптографічного захисту інформації в інформаційно – комунікаційних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз та проведення криптографічного аналізу зі сторони потенційних порушників.

Передумови для навчання

Попередньо опановані дисципліни – «Комп'ютерні мережі»

Зміст навчальної дисципліни

Змістовий модуль 1. Поняття інформаційної безпеки та її місце в системі національної безпеки.

Тема 1. Види і джерела погроз ІБ. Система нормативно-правових актів, що регламентують забезпечення ІБ. Види інформації. Поняття політики забезпечення ІБ. Структура, задачі служби Інформаційної безпеки.

Тема 2. Основні поняття захисту інформації об'єкти, суб'єкти, канали витоку, несанкціонованого доступу, рівні доступу. Протиправна діяльність в інформаційній сфері.

Тема 3. Особливості захисту інформації в автоматизованих системах. Особливості автоматизованих систем, визначення та загальні властивості інформації. Сертифікація автоматизованих систем.

Змістовий модуль 2. Організація захисту інформації .

Тема 4. Модель Белла-Лападули, як основа побудови систем мандатного розмежування доступу. Основні положення моделі. Основна теорема безпеки. Види і джерела погроз ІБ: а) дискреційна політика безпеки; б) мандатна політика безпеки. Комп'ютерні віруси та боротьба з ними. Компютерні віруси. Боротьба з комп'ютерними вірусами. Використання програмного забезпечення для захисту інформації на ПК.

Тема 5. Криптографічний захист інформації Використання криптографії, криптосистеми. Теоретична і практична стійкість криптосистем. Узагальнена схема для криптосистем із закритими ключами шифрування. Класична шифри. Криптографічні і стеганографічні методи захисту інформації. Шифри. Математичні алгоритми. Стандарти асиметричних шифрів. Криптологічні протоколи

Сторінка курсу на платформі Moodle	Розміщено: робоча програма дисципліни, робочий план (технологічна карта), матеріали лекцій, завдання до практичних занять, завдання для самостійної роботи студентів. https://dist.nupp.edu.ua/course/view.php?id=2522

Рекомендовані джерела

Базові

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний підручник. Харків, ХНУРЕ, 2011 р.

2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. Харків, ХНУРЕ, 2011 р.

3. Горбенко І.Д. Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.

4. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2010 , 593с.

5. Головко Г.В., Руденко С.А. Конспект лекцій із дисципліни «Захист інформації» Національний університет «Полтавська політехніка імені Юрія Кондратюка.» – Полтава, 2021. – 117с

6. Головко Г.В**.,** Лисенко О.Д Методичні рекомендації До виконання індивідуальної роботи З дисципліни «Технології захисту інформації» Тема: основи криптології Напрям підготовки 6.050101 «комп'ютерні науки» Галузі знань 0501 «інформатика та обчислювальна техніка» Для студентів всіх форм навчання Полтавський національний технічний університет імені Юрія Кондратюка. – Полтава, 2016. – 45с.

7. Головко Г.В**.** Лабораторний практикум З дисципліни «Захист інформації» Для студентів всіх форм навчання Полтавський національний технічний університет імені Юрія Кондратюка. – Полтава, 2016. – 59с.

Допоміжні

1. Задірака В. Комп'ютерна криптологія. Підручник. К, 2002 ,504с.

2. Бессалов А., Телиженко А. Криптосистеми на еліптичних кривих. – К.: «Політехніка», 2004. – 224 с.

3. Радіотехніка № 114, 119, 126, 134, 141, 142,145. Всеукраїнський міжвідомчий збірник. Харків, ХНУРЕ, 2000- 2008 рр.

4. Прикладна радіоелектроніка. Наук. техн. журнал. Академія наук прикладної радіоелектроніки, ХНУРЕ. Тематичні випуски «Безпека інформації» №2- 2006; №2, №3-2007, №3-2008, №3 – 2009, № 3 – 2010, №2 – 2011рр.

Інформаційні ресурси

1. Закон України від 15 грудня 2005 року № 3200-IV "Про основи національної безпеки України".
2. Закон України "Про інформацію". Із змінами, внесеними згідно із Законом від 07.02.2002 № 3047-III-ВР.
3. Закон України "Про Національну програму інформатизації" Із змінами, внесеними згідно із Законом від 13.09.2001 № 2684-III-ВР.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 № 2594-IV.
5. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IX.
6. Закон України «Про електронний документ та електронний документообіг» від 22.05.2003 № 851-IV.
7. Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства.

Система оцінювання результатів навчання

За результатами поточного контролю протягом семестру студент може отримати максимально 50 балів, за результатами підсумкового контролю 50 балів; мінімальна сума балів, що дозволяє студенту бути атестованим з дисципліни - 60 балів.

Більш детальна інформація щодо оцінювання наведена в робочій навчальній програмі дисципліни.

Накопичування балів з навчальної дисципліни

(вказати лише ті види робіт, за які передбачено нарахування балів)

Види навчальної роботи	Мах кількість балів
Виконання лабораторних робіт	**20**
Контрольна робота	**10**
Модульне тестування	**20**
Індивідуальнізавдання	**20**
Семестровий екзамен	**50**
Максимальна кількість балів	**100**

Відповідність шкали оцінювання ЄКТС національній системі оцінювання та шкалі оцінювання Національного університету «Полтавська політехніка імені Юрія Кондратюка»

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою
90 - 100	A	відмінно
82 - 89	B	добре
74 - 81	C	
64 - 73	D	задовільно
60 - 63	E	
35 - 59	FX	незадовільно

Політики навчальної дисципліни:

Вивчення навчальної дисципліни потребує роботи з інформаційними джерелами, підготовки до лекцій і практичних занять, виконання усіх завдань згідно з навчальним планом.

Підготовка до практичних занять передбачає: ознайомлення з питаннями, які виносяться на заняття з відповідної теми; вивчення лекційного матеріалу. Рішення практичних завдань повинно демонструвати ознаки самостійності виконання здобувачем такої роботи, відсутність ознак повторюваності та плагіату.

Присутність здобувачів вищої освіти на практичних і лекційних заняттях є обов'язковою, важливою також є їх участь в обговоренні всіх питань теми. Пропущені заняття мають бути відпрацьовані. Здобувач вищої освіти повинен дотримуватися навчальної етики, поважно ставитися до учасників процесу навчання, дотримуватися дисципліни й часових (строкових) параметрів навчального процесу.

Більш детальну інформацію щодо компетентностей, результатів навчання, методів навчання, форм оцінювання, самостійної роботи наведено у Робочій програмі навчальної дисципліни
Силабус затверджено на засіданні кафедри комп'ютерних та інформаційних технологій і систем 27 серпня 2021 р. Протокол № 1