Форма ХНАДУ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний автомобільно-дорожній університет

Група _МП-31_

ЗАТВЕРДЖУЮ
Перший проректор
професор _____ С.Я. Ходирев
"_2_" ___09___ 2019 року

РОБОЧА ПРОГРАМА

навчальної дисципліни _____Безпека програм і даних_____
(назва навчальної дисципліни згідно освітньої програми)

підготовки _____бакалавра_____
(назва освітньо-кваліфікаційного рівня)

в галузі знань _____12 Інформаційні технології_____
(шифр і назва галузі знань)

спеціальності __121 Інженерія програмного забезпечення_____
(шифр і назва спеціальності)

за освітньою програмою[1] _Програмне забезпечення систем_
(назва освітньо-професійної (освітньо-наукової) програми)

мова навчання _____державна_____
(мова, на якій проводиться навчання за робочою програмою)

2019 рік

[1] *якщо програма навчальної дисципліни розроблена для декількох освітніх програм за даною спеціальністю, то вказуються усі освітні програми*

1. Мета вивчення навчальної дисципліни є отримання теоретичних знань про методи кодування, шифрування та захисту інформації; типові загрози методи боротьби із ними; особливості проектування, програмування та налаштування контролів захисту для програмних систем та даних, що у них зберігаються для безперебійного та ефективного використання комп'ютерних технологій.

2. Передумови для вивчення дисципліни: основи інформаційних технологій, алгоритмізація та програмування, дискретна математика, окремі розділи вищої математики.

3. Опис навчальної дисципліни

Найменування показників	Характеристика навчальної дисципліни[2]	
	денна форма навчання	**заочна (дистанційна) форма навчання[3]**
Кількість кредитів - __4__ **Кількість годин** - __120__	вибіркова (обов'язкова, вибіркова)	
Семестр викладання дисципліни	6 (порядковий номер семестру)	_____ (порядковий номер семестру)
Вид контролю:	екзамен (залік, екзамен)	
Розподіл часу:		
- лекції (годин)	16	___
- лабораторні роботи (годин)	_____	___
- практичні заняття (годин)	32	___
- самостійна робота студентів (годин)	42	___
- курсовий проект (годин)	_____	___
- курсова робота (годин)	_____	___
- розрахунково-графічна робота (контрольна робота)	_____	___
- підготовка та складання екзамену (годин)	30	___

4. Очікувані результати навчання з дисципліни

По завершені вивчення дисципліни студенти повинні:

знати: основні загрози для цілісності даних; типи атак на програмне забезпечення; методи шифрування даних, методи кодування даних, методи криптографічного захисту даних; коригуючі коди; стеганографічні методи захисту даних; методи крипто- та стеганоаналізу; програмне забезпечення для кодування та шифрування даних; засоби операційних систем для захисту даних та програм; апаратні та апаратно-програмні рішення для захисту даних

---

[2] Якщо дисципліна викладається декілька семестрів, то на кожний семестр за відповідною формою навчання заповнюється окремий стовпчик таблиці.

[3] Якщо дисципліна на заочній (дистанційній) формі навчання не викладається, то графа "заочна форма навчання" відсутня.

вміти: застосовувати існуючі методи симетричного та асиметричного криптографічного захисту інформації; використовувати хеш-функції; розробляти програмні засоби захисту даних та програм; використовувати інструментальні можливості операційних систем для захисту даних та програм; використовувати інструменти для аудиту безпеки даних та програм; використовувати стандартні пакети програм для захисту даних.

5. Критерії оцінювання результатів навчання Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі екзамену.

Відповідність підсумкової семестрової рейтингової оцінки в балах оцінці за національною шкалою та шкалою ECTS:

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
90-100	Відмінно	A	Відмінно (відмінне виконання лише з незначною кількістю помилок)
82 – 89	Добре	B	Дуже добре (вище середнього рівня з кількома помилками)
75 – 81		C	Добре (в загальному вірне виконання з певною кількістю суттєвих помилок)
67 – 74	Задовільно	D	Задовільно (непогано, але зі значною кількістю недоліків)
60 – 66		E	Достатньо (виконання задовольняє мінімальним критеріям)
35 – 59	Незадовільно	FX	Незадовільно (з можливістю повторного складання)
1 – 34		F	Незадовільно (з обов'язковим повторним курсом)

6. Засоби діагностики результатів навчання тестові завдання.

7. Розподіл дисципліни у годинах за формами організації освітнього процесу та видами навчальних занять[4]

Назва теми лекційного матеріалу	Кількість годин		Назва тем	Кількість годин		Література
	очна	заочна	ЛР, ПР, СЗ, СРС СРС	очна	заочна	
1	2	3	4	5	6	7
Семестр 1.						
Тема 1. Вступ. Основи теорії кодування даних. Кодування мультимедійних даних	2		ПР1. Коригуючі коди СРС. Інформація, міри інформації, коди.	4 5		О. 1-8 Д. 1-5
Тема 2. Поширені методи ефективного кодування даних для комп'ютерних систем загального призначення	2		ПР2. Методи ефективного кодування даних СРС. Методи Лемпела-Зіва	4 5		О. 1-8 Д. 1-5
Тема 3. Методи криптографічного захисту даних. Шифри та їх використання.	2		ПР3. Класичні методи та шифри СРС. Класичні та сучасні методи а алгоритми шифрування даних	4 6		О. 1-8 Д. 1-5
Тема 4. Методи шифрування даних у комп'ютерних системах загального призначення, симетричні та асиметричні схеми шифрування.	2		ПР4. Алгоритми та методи шифрування в комп'ютерних системах СРС. Асиметричні методи шифрування та їх підтримка у бібліотеках мов програмування	4 5		О. 1-8 Д. 1-5
Тема 5. Безпека програм та даних на основі механізмів та політик розмежування прав доступу до даних	2		ПР5. Використання хеш-функцій (на прикладі MD5), оцінка стійкості паролю до зламу СРС. Використання хеш-функцій для захисту програм та даних	4 5		О. 1-11 Д. 1-9
Тема 6. Методи захисту даних та програм на основі алгоритмів приховування інформації в потоках даних	2		ПР6. Методи приховування інформації в потоках даних СРС. Стеганографія	4 5		О. 1-11 Д. 1-9
Тема 7. Методи захисту програм та даних під час виконання, захист носіїв даних.	2		ПР7. Методи захисту виконуваних файлів (програм) від зламу та налагодження СРС. Апаратні та програмні засоби захисту програм та	4 5		О. 1-11 Д. 1-9

[4] Якщо дисципліна викладається декілька семестрів, то теми розбивати посеместрово.

			даних			
Тема 8.Сучасні методи автентифікації та ідентифікації користувачів для захисту даних – цифровий підпис, біометричні методи автентифікації.	2		ПР8. Електронний цифровий підпис на прикладі GnuPG, захист документів та електронної пошти за допомогою цифрових підписів СРС. Інструментальні засоби захисту програм та даних	4 5		О. 1-11 Д. 1-9
			СРС Підготовка до екзамену	30		
Усього за семестр	16			104		
УСЬОГО за дисципліну	16			104		

8. Орієнтовна тематика індивідуальних та/або групових занять

9. Форми поточного та підсумкового контролю усне та письмове опитування, захист практичних робіт, тестові завдання в системі Moodle, екзамен.

10. Інструменти, обладнання та програмне забезпечення Debian GNU Linux, ОС Windows, GnuPG, C++, C#, Java, Python 3, GNU Octave/Scilab/Scicos/NSP.

11. Рекомендовані джерела інформації

1. Базова література

Базова

1. Технології захисту інформації : навч. посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2013. – 476 с.
2. Жураковский Ю.П., Полторак В.П. Теорія інформації кодування: Підручник. - Київ : Вища школа, 2001. - 255 с.
3. Теорія інформації та кодування : навч. посібник / В.Л. Кожевников, А.В. Кожевников. – Дніпродзержинськ : Національний гірничий університет, 2012. – 108 с.
4. Захист інформації в автоматизованих системах управління : навч. посібник / Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
5. Основы стеганографии. / А.В. Аграновский, П.Н. Девянин, А.В. Черемушкин, Р.А. Хади. – Ростов на Дону, 2003. – 117 с.
6. Основы криптографии. / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – Гелиос АРВ, 2002. – 480 с.
7. Белоногов В. А. Теория кодирования: учебное пособие. / В.А. Белоногов. – Екатеринбург : УГТУ-УПИ, 2002 . – 111 с.
8. Бородин Л.Ф. Введение в теорию помехоустойчивого кодирования. / П.Ф. Бородин. – М.: Советское радио, 1968. – 407 с.
9. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. / В.Е. Козлов. – Горячая линия – Телеком, 2002. – 336 с.

7. Розподіл дисципліни у годинах за формами організації освітнього процесу та видами навчальних занять[4]

Назва теми лекційного матеріалу	Кількість годин		Назва тем	Кількість годин		Література
	очна	заочна	ЛР, ПР, СЗ, СРС СРС	очна	заочна	
1	2	3	4	5	6	7
Семестр 1.						
Тема 1. Вступ. Основи теорії кодування даних. Кодування мультимедійних даних	2		ПР1. Коригуючі коди СРС. Інформація, міри інформації, коди.	4 5		О. 1-8 Д. 1-5
Тема 2. Поширені методи ефективного кодування даних для комп'ютерних систем загального призначення	2		ПР2. Методи ефективного кодування даних СРС. Методи Лемпела-Зіва	4 5		О. 1-8 Д. 1-5
Тема 3. Методи криптографічного захисту даних. Шифри та їх використання.	2		ПР3. Класичні методи та шифри СРС. Класичні та сучасні методи а алгоритми шифрування даних	4 6		О. 1-8 Д. 1-5
Тема 4. Методи шифрування даних у комп'ютерних системах загального призначення, симетричні та асиметричні схеми шифрування.	2		ПР4. Алгоритми та методи шифрування в комп'ютерних системах СРС. Асиметричні методи шифрування та їх підтримка у бібліотеках мов програмування	4 5		О. 1-8 Д. 1-5
Тема 5. Безпека програм та даних на основі механізмів та політик розмежування прав доступу до даних	2		ПР5. Використання хеш-функцій (на прикладі MD5), оцінка стійкості паролю до зламу СРС. Використання хеш-функцій для захисту програм та даних	4 5		О. 1-11 Д. 1-9
Тема 6. Методи захисту даних та програм на основі алгоритмів приховування інформації в потоках даних	2		ПР6. Методи приховування інформації в потоках даних СРС. Стеганографія	4 5		О. 1-11 Д. 1-9
Тема 7. Методи захисту програм та даних під час виконання, захист носіїв даних.	2		ПР7. Методи захисту виконуваних файлів (програм) від зламу та налагодження СРС. Апаратні та програмні засоби захисту програм та	4 5		О. 1-11 Д. 1-9

[4] Якщо дисципліна викладається декілька семестрів, то теми розбивати посеместрово.

Розроблено та внесено: _ кафедрою комп'ютерних технологій та мехатроніки__
(повне найменування кафедри)

Розробник (и) програми: _асистент _____ Мнушка Оксана Василівна_
(підпис) (ПІБ розробників)

Обговорено та рекомендовано до затвердження на засіданні кафедри Протокол № _18_ від " _27_ " _червня 2019 р.
(номер) (та дата протоколу)

Завідувач кафедри __д.т.н., проф._ _____ _Ніконов Олег Якович_
(науковий ступінь, вчене звання) (підпис) (ПІБ завідувача кафедри)

Погоджено
Декан _____ Механічного факультету_____
(повна назва факультету, де читається дисципліна)
__д.т.н., проф. _____ _Кириченко Ігор Георгійович__
(наук. ступінь, вчене звання) (підпис) (ПІБ декана)
" " _____ 20___ року
(день) (місяць) (рік)

Примітки:
Робоча програма навчальної дисципліни розробляється відповідною кафедрою у 2-х екземплярах на 5 років і затверджується до 30 серпня: 1 екземпляр – у навчальний відділ; 2-екземпляр залишається на кафедрі.

Форма в редакції ХНАДУ відповідно до листа МОН України за №1/9-434 від 09 липня 2018 року затверджена Методичною радою ХНАДУ 26 вересня 2018 року протокол№1