МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний автомобільно-дорожній університет

Потік – **ЗМІ** **«ЗАТВЕРДЖУЮ»**

2017 – 2018 навчальний рік Декан Механічного факультету

професор _____ Кириченко І.Г.

«20» грудня 2017 року

РОБОЧА ПРОГРАМА

навчальної дисципліни **«Технології захисту інформації»**
(назва навчальної дисципліни згідно навчального плану)

підготовки **бакалавра**
(назва освітньо-кваліфікаційного рівня)

галузі знань **12 «Інформаційні технології»**
(шифр і назва галузі знань)

напряму підготовки **122 «Комп'ютерні науки»**
(шифр і назва напряму підготовки)

кваліфікація **3121 «Фахівець з інформаційних технологій»**
(шифр і назва кваліфікації для бакалавра, спеціальності - для магістра)

(шифр за ОПП № **3.12)**
(за ОПП чи № навчального плану)

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	Характеристика навчальної дисципліни
	денна форма навчання
Кількість кредитів - 4 **Кількість годин - 120**	**нормативна, обов'язкова** (нормативна, за вибором ВНЗ, за вибором студента)
Семестр викладання дисципліни	**6**
Вид контролю:	залік
Розподіл часу:	
- лекції (годин)	**32**
- практичні, семінарські (годин)	-
- лабораторні роботи (годин)	**32**
- самостійна робота студентів (годин)	**56**
- курсовий проект (годин)	-
- курсова робота (годин)	-
- розрахунково-графічна робота (контрольна робота)	-

2. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальний тиждень	Назва теми лекційного матеріалу	Кількість годин		Назва ПР, ЛР, СЗ, СРС	Кількість годин		Література
		очна	заочна		очна	заочна	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Розділ 1. Безпека і захист даних							
1 - 2	Тема 1. Огляд безпеки системи. Механізми і політика розмежування прав доступу	4		Злом моноалфавітного підстановлювального шифру методом частотної атаки	ЛР – 4, СРС - 4		1–7, 12-15
3 - 4	Тема 2. Методи та пристрої забезпечення захисту і безпеки	4		Одноразові блокноти. Симет-річні методи шифрування	ЛР – 4, СРС - 4		1–7, 12-15
5 - 6	Тема 3. Захист, доступ та аутентифікація. Моделі захисту. Захист пам’яті	4		Метод шифрування з відкритим ключем RSA	ЛР – 4, СРС - 8		1–7, 12-15
7 - 8	Тема 4. Шифрування даних. Управління відновленням. Комп’ютерна стеганография	4		Скрита передача інформації в JPEG зображеннях. Робота у S-Tools	ЛР – 4, СРС - 8		1–7, 12-15
9 - 10	Тема 5. Основні напрямки розвитку сучасної криптографії. Механізми та протоколи управлін-ня ключами в ІВК інформаційної системи	4		Використання хеш-функцій на прикладі MD5. Оцінка стійкості паролю до злому	ЛР – 4, СРС - 8		1–7, 12-15
Разом за Розділом 1.		20			ЛР – 20 СРС - 32		
Розділ 2. Мережева безпека							
11	Тема 6. Основні види атак, принципи криптоаналізу. Основи криптографії	2		Введення в методи криптографії і кріптоаналіза (частина 1)	ЛР – 2, СРС - 4		1–10, 12-15
12	Тема 7. Алгоритм з секретним ключем. Алгоритм з відкритим ключем.	2		Введення в методи криптографії і кріптоаналіза (частина 1)	ЛР – 2, СРС - 4		1–10, 12-15
13 - 14	Тема 8. Протоколи аутентифікації. Питання безпеки та брандмауери.	4		Запис і читання інформації для пластикових карток з магнітною стрічкою	ЛР – 4, СРС - 8		1–10, 12-15
15 - 16	Тема 9. Цифрові підписи. Використання паролів і механізмів контролю за доступом.	4		Шифрування з відкритим ключем і електронна цифрова підпис на GPG	ЛР – 4, СРС - 8		1–10, 12-15
Разом за Розділом 2.		12			ЛР – 12, СРС - 24		
УСЬОГО		32			ЛР – 32, СРС - 56		

3. ЗАСОБИ ДІАГНОСТИКИ УСПІШНОСТІ НАВЧАННЯ

Засобами діагностики з дисципліни є тестовий контроль з використанням ПК та виконання самостійних контрольних завдань на лабораторних заняттях.

4. РЕКОМЕНДОВАНА ЛІТЕРАТУРА ТА ІНФОРМАЦІЙНІ РЕСУРСИ

Базова

1. К. Шеннон. Математическая теория связи. Работы по теории информации и кибернетике / Пер. С.Карпова. - М.: ИИЛ, 1963. – 830 с.
2. К. Шеннон. Теория связи в секретных системах // Работы по теории информации и кибернетике. - М., ИЛ, 1963. - с. 333-369.
3. В.А. Хорошко. Методы и средства защиты информации. / В.А. Хорошко, А.А. Чекотков. – К.: Юніор, 2003. - 479 с.
4. Столингс В. Криптография и защита сетей: принципы и практика. 3-е издание./ –М: Издательский дом «Вильямс», 2001. – 672 с.
5. В.В. Домарев. Безопасность информационных технологий. Методология создания систем защиты. — К.: ООО “ДС”, 2005. - 688 с.
6. Цымбал В.П. Задачник по теории информации и кодирования. - Киев: Издательское объединение “Вища школа”, 2000. – 268 с.
7. С.В. Кавчук. Сборник примеров и задач по теории информации. Руководство для практических занятий на базе Mathcad 6.0 Plus. - Таганрог: Изд-во ТРТУ, 2002. – 154 с.

Допоміжна

8. https://uk.wikipedia.org/wiki/Комплексна_система_захисту_інформації.
9. Харин Ю. С. и др. Математические основы криптологии: Учеб. пособие / Ю. С.Харин, В. И. Берник, Г. В. Матвеев. — Мн.: БГУ, 2001. - 319 с.
10. В. Зима, А. Молдован, Н. Молдован. Безопасность глобальных сетевых технологий. - СПБ: БХВ-Петербург, 2003. - 368 с.
11. В. Дьяконов, И.Абраменкова. MATLAB. Обработка сигналов и изображений. Специальный справочник. Питер. 2002. – 412 с.

Інформаційні ресурси

12. https://uk.wikipedia.org/wiki/Захист_інформації.
13. Технології захисту інформації [Електронний ресурс, URL: http://umm.pstu.edu/handle/123456789/7947] : методичні вказівки до самостійного вивчення дисципліни «Технології захисту інформації» для студентів напряму підготовки 6.050101 «Комп'ютерні науки» всіх форм навчання / уклад. С. В. Альошин. – Маріуполь : ПДТУ, 2015. – 37 с.
14. Ахрамович В. М. Навчальна програма дисципліни «Технології захисту інформації» (для спеціалістів) [Електронний ресурс, URL: http://library.iapm.edu.ua/metod_disc/pdf/4086up.pdf]. — К.: ДП «Вид. дім «Персонал», 2012. — 16 с.

15. Єгоров А.О. Методичні вказівки до виконання лабораторних робіт з дисципліни «Технології захисту інформації» [Текст], [Електронний ресурс, URL: http://repository.dnu.dp.ua:1100/upload] / А.О. Єгоров, Н.О. Соколова – Д.: НМетАУ, 2014. – 85 с.

Розробник робочої програми: ___доцент___ _____ _Тиричева О.А.
(вчене звання) (підпис) (ПІБ розробника)

Робочу програму схвалено на засіданні кафедри _КТ та мехатроніки_____
(повна назва кафедри)

Протокол №_5_ від ___19 грудня___2017 р.
(номер) (дата прийняття) (рік)

Завідуючий кафедрою __професор_____ _____ __Клец Д.М._
(вчене звання) (підпис) (ПІБ завідувача кафедри)