Syllabus

Донбаська державна машинобудівна академія Факультет «Машинобудування» Кафедра «Автоматизація виробничих процесів»	«ІНФОРМАЦІЙНА БЕЗПЕКА В КОМП'ЮТЕРНИХ МЕРЕЖАХ» для студентів з галузі знань 12 Інформаційні технології, за спеціальністю 123 Комп'ютерна інженерія м. Краматорськ, ДДМА, вул. Академічна, 72 (2-й корпус ДДМА) Semester: [4], Year: [2020-2021]

Instructor information

Name	к.ф.-м. н., доцент **Костіков Олександр Анатолійович**
Contact Info	alexkst63@gmail.com
Office location	ДДМА, (2-й корпус, а.2206)
Office hours	понеділок - п'ятниця з 9.00 по 14.00

Course Description

Навчальна дисципліна «Інформаційна безпека в комп'ютерних мережах» є невід'ємною частиною циклу комп'ютерних дисциплін, необхідних працівникам підприємств незалежно від форми власності та організаційно-правової форми господарювання.

Метою викладання дисципліни «Інформаційна безпека в комп'ютерних мережах» є навчання сучасним технологіям в області інформаційних систем, створення та експлуатації систем захисту інформації.

Основні завдання вивчення дисципліни:

- засвоєння знань по нормативно-правовим основам організації інформаційної безпеки, вивчення стандартів і керівних документів щодо захисту інформаційних систем;
- ознайомлення з основними загрозами інформаційній безпеці, правилами їх виявлення, аналізу та визначення вимог до різних рівнів забезпечення інформаційної безпеки;
- ознайомлення з загрозами інформаційній безпеці, створюваними комп'ютерними вірусами, вивчення особливостей цих загроз та характерних рис комп'ютерних вірусів.

- вивчення особливостей забезпечення інформаційної безпеки в комп'ютерних мережах і специфіки засобів захисту комп'ютерних мереж;
- вивчення змісту і механізмів реалізації сервісів безпеки «ідентифікація» і «аутентифікація»;
- ознайомлення з основними прийомами захисту корпоративних мереж при використанні Internet.

Передумови: комп'ютерна техніка та програмування, комп'ютерні мережі, розподілені комп'ютерні системи та мережі.

Мова викладання: українська.

Learning Objectives

Випускник магістратури має опанувати здатностями:

«Запам'ятовування, знання»	Знання нормативно-правових актів забезпечення інформаційної безпеки. Знання існуючих видів загроз інформаційним системам та методів забезпечення інформаційної безпеки. Знання криптографічних методів захисту інформації.
«Розуміння»	Критично осмислювати проблеми в сфері інформаційної безпеки.
«Уміння та застосування знань»	Вміти організовувати безпечну роботу в Інтернеті. Вміти проектувати і класифікувати захищені комп'ютерні системи. Здатність застосовувати положення правових актів для забезпечення інформаційної безпеки. Здатність визначати загрози безпеці програм та даних.
«Аналіз» та «синтез»	Аналізувати основні підходи, теорії та концепції навчальної дисципліни з урахуванням існуючих міжпредметних зв'язків. Мати уявлення про математичні моделі інформаційної безпеки.
«Оцінювання» та «створення (творчість)»	Створення комплексної системи захисту інформації.
«Комунікація»	Вибирати та відслідковувати найновіші досягнення в області інформаційної безпеки, взаємокорисно спілкуючись із колегами. Зрозуміло і недвозначно доносити власні висновки, а також знання та пояснення, що їх обґрунтовують, до фахівців і нефахівців, зокрема до осіб, з якими працюють.
«Автономія та відповідальність»	Усвідомлювати відповідальність за розвиток професійного знання і практик, оцінку стратегічного розвитку колективу. Усвідомлювати необхідність подальшого навчання, вивчення, аналізу, узагальнення та поширення передового досвіду з інформаційної безпеки, систематично підвищувати свою професійну кваліфікацію.

Learning Outcomes

Під час навчання магістрант має здобути наступні програмні компетентності:

Інтегральна

Здатність розв'язувати складні задачі і проблеми в галузі інформаційних технологій або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.

Загальні

Творчість та інновації:

Здатність до абстрактного мислення, аналізу та синтезу.

Здатність проведення досліджень на відповідному рівні.

Здатність до пошуку, опрацювання та аналізу інформації з різних джерел.

Здатність до генерації нових ідей і варіантів розв'язання задач, комбінування та експериментування, оригінальності, конструктивності, економічності та простих рішень.

Здатність здійснення безпечної діяльності.

Інформаційні технології: здатність до використання інформаційних і комунікаційних технологій.

Спеціальні (фахові)

Знання та розуміння математичних моделей інформаційної безпеки та методів оцінювання захищеності комп'ютерних мережевих систем.

Додаткові спеціальні

Здатність обробляти і інтерпретувати інформацію з застосуванням інтелектуальних систем обробки даних.

Формулювання програмних результатів навчання представлені нижче.

Програмні результати навчання

- Уміння адекватно обирати математичні моделі інформаційної безпеки та оцінювати захищеність комп'ютерних мережевих систем на основі різних метрик.
- Уміння обробляти та інтерпретувати інформацію з застосуванням інтелектуальних систем управління і обробки даних.

Learning Resources

Базова

1. Куприянов А.И. Основы защиты информации: учеб. пособие для стул. высш. учеб. заведений А.И. Куприянов. А.В. Сахаров. В.А. Шевцов.— М.: Издательский центр «Академия». 2006.— 256 с. - 3 екз.

2. Цирлов В.Л. Основы информационной безопасности автоматизированых систем. Краткий курс.— М.: Феникс. 2008.— 174 с. - 3 екз.

3. Белов Е.Б. и др. Основы информационной безопасности. Учебное пособие для вузов.— М.: Горячая линия-Телеком. 2006.— 544 с. - 3 екз.

4. Бармен. Скотт. Разработка правил информационной безопасности.: Пер. с англ.— М.: Издательский дом «Вильяме». 2002.— 20S с. - 3 екз.

5. Домарев В.В. Безопасность информационных технологий. Системный подход.- К.: ООО «ТИД «ДС». 2004.- 992 с. - 3 екз.

6. Конеев И.Р.. Беляев А.В. Информационная безопасность предприятия.— СПб.: БХВ-Петербург. 2003.— 752 с. - 3 екз.

7. Лужецький В.А.. Войтович О.П.. Кожухівський А.Д. Основи інформаційної безпеки. Посібник.— Черкаси: ЧДТУ. 2008.— 243 с - 3 екз.

8. Малюк А.А. Информационная безопасность: концептуальные и методологические основы зашиты информации. Учеб. пособие для вузов.— М.: Горячая линия-Телеком. 2004.— 280 с. - 3 екз.

9. Про інформацію. Закон України від 2 жовтня 1992 р. № 2657—XII. -7 экз.

10. Про науково-технічну інформацію. Закон України від 25 червня 1993 р. № 3322-XII.. - 7 экз.

Методичне забезпечення

11. Інформаційна безпека в комп'ютерних мережах. Конспект лекцій (для студентів спеціальності 123 «Комп'ютерна інженерія»). – Краматорск: ДДМА, 2019.

12. Методичні вказівки до компьютерного практикуму дисципліни "Інформаційна безпека в комп'ютерних мережах" (для студентів спеціальності 123 «Комп'ютерна інженерія»). – Краматорськ: ДДМА, 2019.

Web-ресурси

1. http://www.nbuv.gov.ua/node/208.
2. http://jml.iiau.edu.ua/hidex.php/ZI article view/3504.
3. https://er.nau.edu.ua.handleNAU325S3.

Assessments and Grading Policies

Перелік обов'язкових контрольних точок для оцінювання знань та вмінь

Вид заняття або контрольного заходу	Балів за одно заняття або контрольний захід		За семестр			До 1-й атестації	
			кількість занять або контрольних заходів	сума балів		кількість занять або контрольних заходів	сума балів
	min	max					
Поточний контроль	8	15	4	**32**	**60**	1	15
Модульний контроль	11,5	20	2	**23**	**40**		
Всього за семестр (С)				**55**	**100**		
Іспит(Е)				**55**	**100**		
Всього(С+Е)*0.5				**55**	**100**		

Критерії оцінювання сформованості програмних результатів навчання під час підсумкового контролю

Сума балів за всі види навчальної діяльності	Оцінка за національною шкалою
	для екзамену, курсового проекту (роботи), практики
90 – 100	відмінно
74-89	добре
60-73	задовільно
0-69	незадовільно

Типові недоліки, які зменшують рівень досягнення програмного результату навчання
75-89% - студент припускається суттєвих помилок в обранні методів та формул розв'язку задач
60-74% - студент некоректно формулює назви методів, формул, приводить не чіткі пояснення до розв'язку задач
менше 60% - студент не може обґрунтувати свій розв'язок посиланням на відповідний метод або відповідну формулу розв'язку
75-89% - студент припускається певних логічних помилок при розв'язку задач на заняттях та під час захисту індивідуальних завдань, відчуває певні складності у поясненні окремих моментів розв'язку задач
60-74% - студент припускається істотних логічних помилок при розв'язку задач на заняттях та під час захисту індивідуальних завдань, відчуває істотні складності при поясненні окремих моментів розв'язку задач
менше 60% - студент не здатний продемонструвати володіння логікою та аргументацією при розв'язку задач на заняттях та під час захисту індивідуальних завдань, не здатний пояснити розв'язання задач
75-89% - студент припускається певних помилок у стандартних методичних підходах до розв'язку та відчуває ускладнення при їх модифікації за зміни вихідних умов задач
60-74% - студент відчуває ускладнення при модифікації стандартних методичних підходів до розв'язку за зміни вихідних умов задач, виникають ускладнення при самостійному контролі отриманих результатів
менше 60% - студент нездатний самостійно здійснювати розв'язок задач, контролювати отриманий результат, робити перевірку

Характеристика змісту засобів оцінювання

№	Назва і короткий зміст контрольного заходу	Характеристика змісту засобів оцінювання
1.	Контроль поточної роботи на практичних заняттях	• самостійне виконання завдань на практичних заняттях з використанням відповідного програмного забезпечення; • стандартизовані тести • задачі, що вимагають використання вмінь аналізу, синтезу, аналізу через синтез
2.	Модульні контрольні роботи	• Теоретичні питання з тематики лекцій; • задачі, що вимагають використання вмінь аналізу, синтезу, аналізу через синтез
Підсумковий контроль		• стандартизовані тести • Теоретичні питання з тематики лекцій • задачі, що вимагають використання вмінь аналізу, синтезу, аналізу через синтез

Course Schedule

Графік навчального процесу та контролю знань і перездач з дисципліни для студентів повного курсу навчання

на 1 семестр види занять		Всього	Навчальні тижні (денна/заочна форма)																	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Аудиторні	Лекції	**36 / 8**	2/2	2/-	2/-	2/-	2/2	2/-	2/-	2/-	2/-	2/-	2/-	2/2	2/-	2/-	2/-	2/-	2/-	2/2
	Практичні	**36 / 4**	2/2	2/-	2/-	2/-	2/-	2/-	2/-	2/-	2/-	2/-	2/-	2/2	2/-	2/-	2/-	2/-	2/-	2/-
	Лабораторні																			
	Індивідуальні																			
	Поточ. контр.						+					+				+			+	
	Контр.роб.(ТО)																			
	Модул. контр												M1							M2
	Захист курсов																			
	Захист лабор.																			
	Консультації																			
	Атестації										A1									
	Всього	**72 / 12**	4/4	4/-	4/-	4/-	4/2	4/-	4/-	4/-	4/-	4/-	4/-	4/4	4/-	4/-	4/-	4/-	4/-	4/2
Самостійні	Курс. проект.																			
	Підгот. до зан	**93 / 153**	5/8	5/9	5/8	5/9	5/8	5/9	5/8	5/9	5/8	5/9	5/8	5/9	5/8	5/9	5/8	6/9	6/8	6/9
	Розрах.-граф.																			
	Екскурсії																			
	Всього	**93 / 153**	5/8	5/9	5/8	5/9	5/8	5/9	5/8	5/9	5/8	5/9	5/8	5/9	5/8	5/9	5/8	6/9	6/8	6/9
Навчальне навантаження студентів		**165/165**	**9/12**	**9/9**	**9/8**	**9/9**	**9/10**	**9/9**	**9/8**	**9/9**	**9/8**	**9/9**	**9/8**	**9/13**	**9/8**	**9/9**	**9/8**	**10/9**	**10/8**	**10/9**

Підсумковий контроль – іспит.

Структура дисципліни

Назва модулю та теми
Модуль 1. Поняття та методи забезпечення інформаційної безпеки
Тема 1.1. Інформаційна безпека та рівні її забезпечення *Поняття інформаційної безпеки. Складові інформаційної безпеки. Нормативно-правові основи інформаційної безпеки в Україні. Сервіси безпеки в комп'ютерних мережах. Механізми безпеки.*
Тема 1.2. Загрози інформаційної безпеки та методи запобігання цим загрозам *Класифікація загроз інформаційної безпеки.Канали несанкціонованого доступу до інформації.*
Тема 1.3. Комп'ютерні віруси та захист від них. *Віруси як загроза інформаційної безпеки.Характерні риси комп'ютерних вірусів.Характеристика «вірусрподібних програм». Антивірусні програми, їх класифікація та особливості роботи.*
Тема 1.4. Інформаційна безпека комп'ютерних мереж. *Програмно-апаратні засоби забезпечення ІБ(інформаційної безпеки) в комп'ютерних мережах. Протоколи аутентифікації при вилученому доступі. Захист віртуальних локальних мереж. Організація ІБ мережі за допомогою брандмауерів та фаєрволів.ІБ при роботі в мережі Інтернет. Технологія захисту мережі - IPSec.*
Тема 1.5. Ідентифікація, автеніфікація та права розмежування доступу *Прості паролі. оцінка стійкості пароля. Модифікація механізму простих паролів. Список паролів. Механізм "рукостискань". Багатофакторна автентикація (Multiway authentication).Біометрична автентикація. Рекомендації по вибору механізмів автентикації.*
Тема 1.6. Криптографічні методи захисту інформації. *Основні визначення в області криптографії. 3.2. Класифікація криптографічних систем. Шифр Цезаря. Шифр Шенона. Криптоалгоритм DES (Схема. Особливості шифрування по алгоритму DES. Модифікації алгоритму DES).Цифровий підпис (Digital signature). AES. ГОСТ 28147-89. ANUBIS. Асиметричні криптосистеми. RSA.*
Тема 1.7. Протоколи автеніфікації. *Класифікація протоколів автентикації в комп'ютерних системах та мережах. Протоколи автентикації суб'єктів на основі симетричних криптосистем. Протоколи автентикації суб'єктів на основі асиметричних криптосистем. Протокол автентикації повідомлень на основі симетричних криптосистем. Загальна схема. Протоколи автентикації повідомлень на основі асиметричних криптосистем. Протокол відкритих угод.*
Модуль 2. Створення, введення в дію та супроводження захищених систем
Тема 2.1. Створення комплексної системи захисту інформації *Порядок проведення робіт зі створення комплексної системи захисту інформації Вимоги до комплексної системи захисту інформації та політика безпеки Розроблення технічного завдання на створення комплексної системи захисту інформації*
Тема 2.2. Кваліфікаційний аналіз засобів і систем захисту інформації *Вимоги до кваліфікаційною аналізу Організація державної експертизи Сертифікація засобів технічного захисту інформації*
Тема 2.3. Супроводження комплексної системи захисту інформації *Загальні положення. Завдання та функції служби захисту інформації. Права й обов'язки служби захисту інформації. Взаємодія служби захисту інформації з іншими підрозділами та із зовнішніми організаціями*

Course Policies

- **Attendance & Participation**: у разі відсутності під час заняття студент не повинен його опрацьовувати, у разі відсутності під час контролю, студент має здати контроль під час перездач.
- **Academic Integrity & Collaboration**: звертаючись за допомогою під час опрацювання індивідуальних контрольних робіт, студент має вміти самостійно представляти отримані результати.
- **Late-work/Make-up work policy**: здача індівідуального завдання із запізненням означає зниження оцінки. Оцінка є обернено пропорційною терміну запізнення
- **Statement on student wellness**: у разі хвороби студента запізнена здача індивідуального завдання не впливає на оцінювання.
- **Mobile Devices**: можливе використання мобільних додатків для візуалізації об'єктів, для розрахунків під час аудиторних занять та сам. роботи. Про можливість залучення певних мобільних додатків під час контролю оговорюється окремо із представленням додатку.
- **Evaluation criterion:** Оцінка за результатами вивчення частини курсу(модуль) визначається як сумарна оцінка за тестування модуля, проводить лектор, та розрахункову (самостійну) роботу студента, контроль здійснює асистент.

Оцінювання виконання завдань тестових та самостійних робіт проводиться наступним чином:

1. Максимальна оцінка по кожному завданню (максимально можлива оцінка вказана в карточці з завданням) може бути отримана, коли студент виконав завдання вірно в повному обсязі з поясненнями.
2. У випадку, коли студент виконав завдання з помилками або без пояснень, то оцінка буде нижчою за максимальну.
3. Коли студент не виконав завдання, або допустив суттєві помилки при розв'язку, то оцінка може бути рівною 0 балів за таке завдання.
4. Для того, щоб тест за модулем та самостійна робота вважалася виконаним необхідно набрати мінімально позитивну кількість балів, у кожного з них є своя мінімальна оцінка, в більшості випадків це 30 балів для тесту та 25 для самостійної роботи.

Тобто мінімальна позитивна оцінка за модулем 55 балів, але коли тест, або самостійна робота не складені на мінімально позитивну оцінка модуля буде меншою за 55 балів. Наприклад: тест 40б, а СР 20б, в сумі 60 балів, але мінімальна позитивна оцінка за СР 25 балів, тому оцінка за модулем буде складати 54 бали.

Course analysis

Якість викладання дисциплін контролюється анонімним он-лайн-опитуванням студентів. Вивчається думка здобувачів вищої освіти відносно якості викладання дисциплін.

Необхідно оцінити вказані якості за шкалою: 1 бал – якість відсутня; 2 бали – якість проявляється зрідка; 3 бали – якість проявляється на достатньому рівні; 4 бали – проявляється часто; 5 балів – якість проявляється практично завжди.

Анкета є анонімною. Відповіді використовуються в узагальненому вигляді.

https://docs.google.com/forms/d/1CCKuROPuWcME7DPc9fivhSann5wv9mJj_M4LdiCL3ek/edit?usp=sharing