МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МИКОЛАЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. О. СУХОМЛИНСЬКОГО
Механіко-математичний факультет

Кафедра інформаційних технологій

ЗАТВЕРДЖУЮ
Проректор із науково-педагогічної роботи
_____ О. А. Кузнецова
27 серпня 2020 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Ступінь бакалавра
Галузь знань 11 Математика та статистика
спеціальність 113 Прикладна математика
освітня програма «Інформатика»

2020 – 2021 навчальний рік

Розробник: Зосімов В'ячеслав Валерійович, завідувач кафедри інформаційних технологій, доктор технічних наук, доцент _____(Зосімов В.В.)

Робоча програма затверджена на засіданні кафедри інформаційних технологій
Протокол № 1 від «26» серпня 2020 р.

Завідувач кафедри _____ (Зосімов В.В.)

«26» серпня 2020 р.

Програму погоджено з гарантом ОП Комп'ютерні науки

Доцент кафедри, к.техн.н._____ (Булгакова О.С.)

Програму погоджено з гарантом ОП Прикладна математика

професор кафедри, д.фіз.-мат.н._____ (Поздєєв В.О.)

Анотація

Програма навчальної дисципліни передбачає вивчення методів роботи із сучасним програмним забезпеченням, системного підходу до розв'язування інженерно-технічних задач з допомогою ПК, пошуку і опрацювання інформації з використанням сучасних технологій. Викладання навчальної дисципліни «Технології захисту інформації» забезпечить такі результати навчання: застосовувати теоретичні, методичні і практичні підходи для розв'язування фахових задач; пошук, відбір та систематизація необхідних даних з використанням інформаційних систем і технологій у прикладних галузях. Після вивчення даної дисципліни студент повинен бути здатним здійснювати розробку та підтримку систем захисту від вірусів, зловмисників, застосовувати методи та прийоми для забезпечення надійної роботи комп'ютерних систем та мереж, використовувати сучасні технології цирового шифрування та електронного підпису.

Ключові слова: кіберзахист, кіберпростір, кібербезпека, шифрування, цифровий підпис, криптоаналіз, стеганографія, соціальний інжиніринг.

Abstract

The program of the discipline involves the study of methods of working with modern software, a systematic approach to solving engineering problems using a PC, search and processing of information using modern technologies. Teaching the discipline "Information Security Technologies" will provide the following learning outcomes: apply theoretical, methodological and practical approaches to solving professional problems; search, selection and systematization of necessary data using information systems and technologies in applied fields. After studying this discipline, the student must be able to develop and maintain protection systems against viruses, attackers, apply methods and techniques to ensure the reliable operation of computer systems and networks, use modern technologies of digital encryption and electronic signature.

Keywords: cybersecurity, cyberspace, cybersecurity, encryption, digital signature, cryptanalysis, steganography, social engineering.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, освітній ступінь</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 3</td><td>Галузь знань
11 Математика та статистика</td><td>Нормативна</td></tr>
<tr><td rowspan="2">Індивідуальне науково-дослідне завдання –</td><td rowspan="4">Спеціальність
113 Прикладна математика</td><td>Рік підготовки:</td></tr>
<tr><td>2ск</td></tr>
<tr><td rowspan="2">Загальна кількість годин 90</td><td>Семестр</td></tr>
<tr><td>1-й</td></tr>
<tr><td rowspan="8">Тижневих годин для денної форми навчання:
аудиторних – 2
самостійної роботи студента - 4</td><td rowspan="8">Ступінь бакалавра</td><td>Лекції</td></tr>
<tr><td>16 год.</td></tr>
<tr><td>Практичні, семінарські</td></tr>
<tr><td></td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>14 год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>60 год.</td></tr>
<tr><td>http://moodle.mdu.edu.ua/course/view.php?id=</td><td>Вид контролю: залік</td></tr>
</table>

Мова навчання – українська.

Примітка.

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить: для денної форми навчання – 30 год. – аудиторні заняття, 90 год. – самостійна робота (30% ~ 70%).

2. Мета, завдання навчальної дисципліни та результати навчання

Мета курсу: ознайомити студентів з теоретичними основами криптографії та криптоаналізу та отриманні навичок практичної роботи з інструментами шифрування даних.

Завдання вивчення курсу: формування у студентів певних знань та вмінь з теорії криптографії; знайомство з колом задач, що розв'язуються в криптографії та криптоаналізі, застосовувати теоретичні, методичні і практичні підходи для розв'язування фахових задач; пошук, відбір та систематизація необхідних даних з використанням інформаційних систем і технологій у прикладних галузях

Передумови для вивчення дисципліни: для освоєння курсу студенти повинні знати курси програмування, дискретна математика та теорія алгоритмів, вища математика.

Навчальна дисципліна складається з 3-ох кредитів.

Програмні результати навчання:

ПР3 Володіти основними положеннями та методами математичного, комплексного та функціонального аналізу, лінійної алгебри та теорії чисел, аналітичної геометрії, теорії диференціальних рівнянь, зокрема рівнянь у частинних похідних, теорії ймовірностей, математичної статистики та випадкових процесів, чисельними методами.

ПР5 Вміти застосовувати сучасні технології програмування та розроблення програмного забезпечення, програмної реалізації чисельних і символьних алгоритмів.

ПР7 Поєднувати методи математичного та комп'ютерного моделювання з неформальними процедурами експертного аналізу для пошуку оптимальних рішень.

Згідно з вимогами освітньо-професійної програми студент оволодіває такими компетентностями:

І. Загальнопредметні:

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК5. Здатність проведення досліджень на відповідному рівні.

ЗК6. Здатність до абстрактного мислення, аналізу та синтезу.

ІІ. Фахові:

ФК6. Здатність розв'язувати професійні задачі за допомогою комп'ютерної техніки, комп'ютерних мереж та Інтернету, в середовищі сучасних операційних систем, з використанням стандартних офісних додатків.

ФК9. Здатність до проведення математичного і комп'ютерного моделювання, аналізу та обробки даних, обчислювального експерименту, розв'язання формалізованих задач за допомогою спеціалізованих програмних засобів.

ФК14. Здатність сформулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, та обирати метод її розв'язання, що забезпечує потрібні точність і надійність результату

Програма навчальної дисципліни

Кредит 1. Введення до криптографії.

Тема 1. Захист інформації, види атак на інформацію.

Основні загрози інформаційній безпеці. Категорії безпеки інформації в комп'ютерних мережах та інформаційних системах. Методи захисту інформації. Задачі технічного і криптографічного захисту інформації. Моделі симетричної і асиметричної криптосистем.

Тема 2. Загальні відомості про шифри та криптосистеми.
Історія криптографії. Основні поняття криптографії та теорії секретних систем. Перші методи шифрування перестановки та заміни. Одноалфавітні системи шифрування Віженера, Плейфейра та ін. Багато алфавітні системи шифрування: Енігма, Бьюфорта, Віженера. Їх роль у сучасній криптографії.
Тема 3. Шифри заміни та перестановки.
Основи шифрування. Шифри однозначної заміни. Шифр Цезаря. Атбаш. Лозунговий шифр. Полібіанський квадрат. Тюремний шифр. Шифрувальна система Трисемуса. Шифр масонів. Криптоаналіз шифрів однозначної заміни.
Перестановка та підстановка. Прості шифри. Криптоаналітичні атаки та метод підрахунку частот для моно та багатоалфавітних криптосистем.
Кредит 2. **Модульна арифметика**.
Тема 4. Арифметика цілих чисел.
Теорія подільності. Алгоритм Евкліда для знаходження НСД. Розширений алгоритм Евкліда. Лінійні диофантові рівняння.
Тема 5. Операції по-модулю.
Остача від ділення. Система найменших відрахувань по модулю n. Відображення нескінченної кількості елементів множини Z на один елемент множини Zn. Поняття порівняння замість рівності. Властивості операції порівняння.
Тема 6. Адитивна та мультиплікативна інверсії
Операції, обчислення величини, зворотньої заданому числу на множині Zn. Адитивна інверсія (оператор, зворотний додаванню). Мультиплікативна інверсія (оператор, зворотний множенню). Властивості інверсій.
Кредит 3. Алгоритми шифрування.
Тема 7. Закритий та відкритий ключі.
Відмінності симетричного та асиметричного підходу до шифрування. Алгоритми генерації відкритого та закритого ключа. Переваги асиметричного шифрування. Засоби передачі ключів.
Тема 8. Поняття односторонніх функцій
Сутність односторонніх перетворень. Алгоритм генерації закритого ключа в асиметричному шифруванні. Показники безпеки асиметричних алгоритмів. Поняття довжини ключа.
Тема 9. Алгоритм RSA.
Сутність алгоритму асиметричного шифрування RSA. Етапи генерації відкритого та закритого ключа. Шифрування та розшифрування даних за допомогою алгоритму RSA. Інтеграція результатів роботи асиметричних алгоритмів в процес симетричного шифрування.
Тема 10. Хеш-функції та цифрові підписи
Аутентифікація повідомлень. Вимоги до хеш-фукнцій. Галузь застосування хеш-функцій. Прості хеш-функції. Застосування ланцюгів зашифрованих блоків. Хеш-функція MD5. Логіка виконання функції MD5. Вимоги до цифрових підписів. Пряма та арбітражний цифрові підписи. Галузь застосування цифрових підписів. Стандарт цифрового підпису DSS. Основні компоненти групи користувачів. Алгоритм перевірки підпису.

3. Структура навчальної дисципліни

Назви кредитів і тем	Кількість годин					
	усього	у тому числі				
		л	П	лаб	інд	ср
1	2	3	4	5	6	7
Кредит 1. Введення до криптографії.						
Тема 1. Захист інформації, види атак на інформацію.	8	1				7

Тема 2. Загальні відомості про шифри та криптосистеми.	10	1				9
Тема 3. Шифри заміни та перестановки.	12	2		2		8
Усього	30	4		2		24
Кредит 2. Модульна арифметика.						
Тема 4. Арифметика цілих чисел.	9	1		2		6
Тема 5. Операції по-модулю.	11	1		2		8
Тема 6. Адитивна та мультиплікативна інверсії	10	2		2		6
Усього	30	4		6		20
Кредит 3. Алгоритми шифрування						
Тема 7. Закритий та відкритий ключі.	6	2		2		2
Тема 8. Поняття односторонніх функцій	6	2		2		2
Тема 9. Алгоритм RSA.	6	2		2		2
Тема 10. Хеш-функції та цифрові підписи	12	2				10
Усього	30	8		6		17
Усього годин:	90	16		14		60

4. Теми лекційних занять

N з/п	Назва теми	Кількість годин
Кредит 1. Введення до криптографії		
1	**Тема 1.** Захист інформації, види атак на інформацію.	1
2	**Тема 2.** Загальні відомості про шифри та криптосистеми.	1
3	**Тема 3**. Шифри заміни та перестановки.	2
Кредит 2. Модульна арифметика.		
4	**Тема 4.** Арифметика цілих чисел.	1
5	**Тема 5**. Операції по-модулю.	1
6	**Тема 6**. Адитивна та мультиплікативна інверсії	2
Кредит 3. Алгоритми шифрування		
7	**Тема 7.** Закритий та відкритий ключі.	2
8	**Тема 8.** Поняття односторонніх функцій	2
9	**Тема 9**. Алгоритм RSA.	2
10	**Тема 10.** Принципи роботи хешування. Цифрові підписи.	2
	Всього	**16**

5. Теми лабораторних занять

N з/п	Назва теми	Кількість годин
Кредит 1. Введення до криптографії		
1	Тема 3. Шифри однозначної заміни. Шифр Цезаря. Атбаш. Лозунговий шифр. Полібіанський квадрат. Тюремний шифр	2
Кредит 2. Модульна арифметика.		
2	Тема 4. Алгоритм Евкліда для знаходження НСД	2
3	Тема 5. Операції по-модулю.	2
4	Тема 6. Адитивна інверсія (оператор, зворотний додаванню).	2
Кредит 3. Алгоритми шифрування		
5	Тема 7. Алгоритми генерації відкритого та закритого ключа.	2
6	Тема 8. Алгоритм генерації закритого ключа в асиметричному шифруванні.	2
7	Тема 9. Алгоритм RSA.	2

8	Тема 10. Аутентифікація повідомлень. Хеш-функція MD5	2
	Всього	**14**

6. Самостійна робота

N з/п	Назва теми	Кількість годин
Кредит 1. Введення до криптографії		
1	Тема 1. Категорії безпеки інформації в комп'ютерних мережах та інформаційних системах. Задачі технічного і криптографічного захисту інформації.	7
2	Тема 2. Багато алфавітні системи шифрування: Енігма, Бьюфорта, Віженера. Їх роль у сучасній криптографії.	9
3	Тема 3. Шифрувальна система Трисемуса. Шифр масонів. Криптоаналіз шифрів однозначної заміни. Криптоаналітичні атаки та метод підрахунку частот для моно та багатоалфавітних криптосистем.	8
Кредит 2. Модульна арифметика.		
4	Тема 4. Арифметика цілих чисел. Розширений алгоритм Евкліда.	6
5	Тема 5. Операції по-модулю. Поняття порівняння замість рівності. Властивості операції порівняння.	8
6	Тема 6. Мультиплікативна інверсія (оператор, зворотний множенню). Властивості інверсій.	6
Кредит 3. Алгоритми шифрування		
7	Тема 7. Переваги асиметричного шифрування. Засоби передачі ключів.	2
8	Тема 8. Показники безпеки асиметричних алгоритмів.	2
9	Тема 9. Алгоритм RSA. Інтеграція результатів роботи асиметричних алгоритмів в процес симетричного шифрування.	2
10	Тема 10. Галузь застосування хеш-функцій. Прості хеш-функції. Застосування ланцюгів зашифрованих блоків. Основні компоненти групи користувачів. Алгоритм перевірки підпису.	10
	Всього	**60**

7. Форми роботи та критерії оцінювання

Рейтинговий контроль знань студентів здійснюється за 100-бальною шкалою:

Шкала оцінювання: національна та ECTS

ОЦІНКА ЄКТС	СУМА БАЛІВ	ОЦІНКА ЗА НАЦІОНАЛЬНОЮ ШКАЛОЮ	
		екзамен	залік
A	90-100	5 (відмінно)	5/відм./зараховано
B	80-89	4 (добре)	4/добре/ зараховано
C	65-79		
D	55-64	3 (задовільно)	3/задов./ зараховано
E	50-54		
FX	35-49	2 (незадовільно)	Не зараховано

Форми поточного та підсумкового контролю. Комплексна діагностика знань, умінь і навичок студентів із дисципліни здійснюється на основі результатів проведення поточного й підсумкового контролю знань (КР). Поточне оцінювання (індивідуальне, групове і фронтальне опитування, самостійна робота, самоконтроль). Завданням поточного контролю є систематична перевірка розуміння та засвоєння програмового матеріалу, виконання практичних, лабораторних робіт, уміння самостійно опрацьовувати тексти, складання конспекту рекомендованої літератури, написання і захист реферату, здатності публічно чи письмово представляти певний матеріал.

Завданням підсумкового контролю (КР, залік) є перевірка глибини засвоєння студентом програмового матеріалу модуля.

Критерії оцінювання відповідей на практичних заняттях:

Студенту виставляється відмінно, якщо студент здатний самостійно здійснювати основні види навчальної діяльності. Знання студента є глибокими, міцними, узагальненими; студент вміє застосовувати знання творчо, його навчальна діяльність позначена вмінням самостійно оцінювати різноманітні життєві ситуації, явища, факти, виявляти і відстоювати особисту позицію.

Студенту виставляється дуже добре, якщо студент знає істотні ознаки понять, явищ, закономірностей, зв'язків між ними, а також самостійно застосовує знання в нестандартних ситуаціях, володіє розумовими операціями, вміє робити висновки, виправляти допущені помилки. Відповідь повна, правильна, логічна, обґрунтована.

Студенту виставляється добре, якщо студент знає ознаки понять, явищ, закономірностей, зв'язків між ними на середньому рівні, а також самостійно застосовує знання в стандартних ситуаціях, володіє розумовими операціями, вміє робити висновки, виправляти допущені помилки. Відповідь повна, правильна, логічна, обґрунтована.

Студенту виставляється достатньо, якщо відповідь студента при відтворенні навчального матеріалу елементарна, зумовлюється початковими уявленнями про предмет вивчення. Студент відтворює основний навчальний матеріал, здатний виконувати завдання за зразком, володіє елементарними вміннями навчальної діяльності.

Студенту виставляється мінімальний задовільно, якщо відповідь студента при відтворенні навчального матеріалу елементарна, зумовлюється початковими уявленнями про предмет вивчення. Студент відтворює основний навчальний матеріал.

Кількість балів у кінці **семестру** повинна складати від 150 до 300 балів (за 3 кредити), тобто сума балів за виконання усіх завдань.

Відповідний **розподіл балів, які отримують студенти** за 3 крд

Поточне оцінювання та самостійна робота										КР	Накопичувальні бали/ Сума
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10		
30	35	35	30	30	40	20	30	30	20	100	300/100*

***Примітка.** Коефіцієнт для іспиту – 0,6. Іспит оцінюється в 40 б.

8. Засоби дігностики

Засобами діагностики та методами демонстрування результатів навчання є: завдання до лабораторних занять, завдання для самостійної та індивідуальної роботи, презентації результатів досліджень, тестові завдання, контрольні роботи.

9. Методи навчання

Усний виклад матеріалу: наукова розповідь, спрямована на аналіз фактичного матеріалу; пояснення − вербальний метод навчання, за допомогою якого розкривається сутність певного явища, закону, процесу; проблемне навчання, робота з підручником та додатковими джерелами.

Лекційні заняття призначені для теоретичного осмислення і узагальнення складних розділів курсу, які освітлюються, в основному, на проблемному рівні та у формі діалогічно-проблемних лекцій.

Лабораторні заняття є аудиторними, проводяться по наперед відомих темах у вигляді активних форми проведення занять. Вони призначені для закріплення і глибшого вивчення певних аспектів лекційного матеріалу на практиці.

Самостійна робота є позааудиторною і призначена для самостійного ознайомлення студента з певними розділами курсу за рекомендованими педагогом матеріалами і підготовки до виконання індивідуальних завдань по курсу.

Поточний рейтинг-контроль проводиться викладачем в процесі проведення всіх видів занять. Проміжний рейтинг-контроль призначений для практичної комплексної оцінки освоєння розділів курсу і здійснюється шляхом підготовки студентами відповідей на поставлені питання.

10. Рекомендована література

Базова

1. Анин Б.Ю. Защита компьютерной информации. СПб.: БХВ-Санкт-Петербург, 2015. 384 с.
2. Технології захисту інформації : навчальний посібник. С. Е. Остапов, С. П. Євсеєв, О. Г. Король. Х. : Вид. ХНЕУ, 2015. 476 с. (Укр. мов.)

Допоміжна

1. Бабаш, А. В. История криптографии. Часть I. А.В. Бабаш, Г.П. Шанкин. М.: Гелиос АРВ, 2016. 240 с.
2. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа. Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2015. 376 с.
3. Бабенко, Л.К. Современные интеллектуальные пластиковые карты. Л.К. Бабенко. - М.: Гелиос АРВ, 2015. 921 с.
4. Болотов, А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. А.А. Болотов, С.Б. Гашков, А.Б. Фролов. М.: КомКнига, 2013. 306 с.
5. Бузов, Геннадий Алексеевич Защита информации ограниченного доступа от утечки по техническим каналам. Бузов Геннадий Алексеевич. М.: Горячая линия - Телеком, 2016. 186 с.
6. Вельшенбах, М. Криптография на Си и C++ в действии. Учебное пособие. М. Вельшенбах. М.: Триумф, 2014. 462 с.
7. Тарнавський, Ю. А. Технології захисту інформації [Електронний ресурс] : підручник для студентів спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах». Ю. А. Тарнавський ; КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с
8. Методичні вказівки до лабораторних робіт з дисципліни «Технології захисту інформації» для студентів напряму підготовки «Комп'ютерні науки» усіх форм навчання / уклад.: Г. В. Неласа, Г. Л. Козіна. Запоріжжя: ЗНТУ, 2016. 52 с.

9. Дронюк І. М. Технології захисту інформації на матеріальних носіях Монографія. Львів : Видавництво Львівської політехніки, 2017. 200 с

11. Інформаційні ресурси

1. http://learncryptography.com
2. http://php.net/