МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА

Факультет математики та інформатики

Кафедра алгебри та геометрії

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАХИСТ ІНФОРМАЦІЇ

Освітня програма: Математика комп'ютерних технологій
Прикладна математика

Спеціальність: 111 Математика
113 Прикладна математика

Галузь знань: 11 Математика та статистика

Затверджено на засіданні кафедри
Протокол № 7 від 29 березня 2022 р.

м. Івано-Франківськ – 2022 рік

ЗМІСТ

1. Загальна інформація
2. Анотація до курсу
3. Мета та цілі курсу
4. Компетентності
5. Результати навчання
6. Організація навчання курсу
7. Система оцінювання курсу
8. Політика курсу
9. Рекомендована література

© Мазуренко Н.І., 2022–2023

1. ЗАГАЛЬНА ІНФОРМАЦІЯ

Назва дисципліни	Захист інформації
Викладач(-і)	Мазуренко Н.І.
Контактний телефон	(0342)596016
E-mail	nataliia.mazurenko@pnu.edu.ua
Формат дисципліни	Лекції та практичні заняття
Обсяг дисципліни	6 кредитів
Консультації	Вівторок, 15^{00}

2. АНОТАЦІЯ ДО КУРСУ

Дисципліна "Захист інформації" є складовою підготовки магістрів з математики (дисципліною за вибором студента) і сприяє фундаменталізації освіти, формуванню науковою світогляду і розвитку системного мислення.

Як навчальна дисципліна «Захист інформації» забезпечує володіння принципами побудови комплексних систем захисту інформації, розробки, дослідження та застосування механізмів захисту інформації; механізмами захисту, які засновані на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення автентичності, цілісності та конфіденційності інформаційних систем та технологій; основами стенографічного захисту інформації та особливостями побудови інфраструктури відкритих ключів.

3. МЕТА ТА ЦІЛІ КУРСУ

Курс забезпечує ознайомлення з принципами побудови та використання програмних та програмно-апаратних засобів для захисту програмного забезпечення та іншої інформації в комп'ютерних системах; вчить використовувати основні принципи побудови систем захисту інформації та застосовувати методи протидії спробам несанкціонованого доступу до неї з боку сторонніх осіб. Також, курс забезпечує набуття знань з математичних основ криптографічного захисту інформації.

Завданням дисципліни є формування у студентів теоретичних знань та вироблення практичних навичок проектування комплесних рішень із захисту інформації.

4. КОМПЕТЕНТНОСТІ

- Здатність до абстрактного мислення, аналізу та синтезу, до застосування теорії у практичних ситуаціях;
- Здатність до пошуку та інтерпретації інформації, засвоєння нових знань, генерування та викладу ідей, зокрема, з застосуванням інформаційних технологій;
- Здатність працювати як автономно, так і у складі наукового, зокрема, інтернаціонального, колективу фахівців з усвідомленням відповідальності за результати роботи;
- Здатність вести дослідницьку діяльність, включаючи оцінку актуальності дослідження, аналіз проблем, вибір способу й методів дослідження, а також оцінку якості результатів.
- Цілісне уявлення про математику, її сучасний стан, виникнення і шляхи розвитку, її місце у системі наукових знань людства;
- Здатність зрозуміти постановку завдання, пов'язаного із застосуванням математичних методів, сформульовану на мові певної предметної галузі;
- Здатність математично формалізувати проблему прикладного характеру, розпізнати стандартні об'єкти і властивості аналізу, звичайних диференціальних рівнянь, рівнянь математичної фізики, дискретної математики, теорії керування, методів оптимізації, алгебри, геометрії;
- Здатність обирати та застосовувати математичні методи для розв’язування практичних задач захисту інформації;
- Уміння ефективно співпрацювати, розподіляти роботу і спілкуватись з колегами в процесі командного виконання дослідницьких та програмних проектів;
- Здатність до побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення та аналізу алгоритмів, оцінювання їх ефективності та складності для адекватного моделювання предметних областей і створення програмних та інформаційних систем;
- Здатність застосовувати основні методи та алгоритми прийняття рішень в умовах наявності нечіткої вхідної інформації, здійснювати аналіз отриманих результатів.

5. РЕЗУЛЬТАТИ НАВЧАННЯ

- демонструвати знання й розуміння основних концепцій, принципів, теорій фундаментальної та прикладної математики і використовувати їх на практиці, а також гуманітарних дисциплін підготовки фахівця (**Р1**);
- володіти основними положеннями та методами математичного, комплексного та функціонального аналізу, алгебри і теорії чисел та аналітичної геометрії, теорії ймовірностей, математичної статистики та випадкових процесів. (**Р2**);
- знати де виникають задачі захисту інформації і основні принципи ефективної формалізації таких задач (**Р3**);
- самостійно працювати над дослідницькою темою, обґрунтовувати і створювати програмну реалізацію розроблених методів. (**Р4**);
- уміти розробляти математичні моделі об'єктів і процесів, які досліджуються, використовуючи процедури формального уявлення про систему та результати дослідження реальних природничих та соціально-економічних процесів. (**Р5**);
- уміти розробляти нові і удосконалювати існуючі моделі та алгоритми захисту інформації. (**Р7**);
- знати способи захисту інформації та найпростіші методи шифрування. Знати функціональні можливості застосування сучасних пакетів програмної реалізації криптографічних перетворень та криптографічних бібліотек (**Р23**);
- уміти проводити наукові дослідження, грамотно викладати і представляти опрацьований матеріал і власні результати, в тому числі і з сучасними можливостями візуалізації, створювати комп'ютерну реалізацію розроблених методів (**Р25**).

6. ОРГАНІЗАЦІЯ НАВЧАННЯ КУРСУ

Обсяг курсу	
Вид заняття	Загальна кількість годин
Лекції	30
Практичні	30
Самостійна робота	120

Ознаки курсу				
Спеціальність, освітня програма	Рівень освіти	Курс (рік навчання)	Семестр	Нормативна/ вибіркова
111 математика Математика комп'ютерних технологій	Магістр	2ий	3ій	вибіркова
113 прикладна математика				

Тематика курсу					
Тема	Форма заняття	Література	Завдання, год	Вага оцінки	Термін виконання
Складові «Інформаційної безпеки». Огляд безпеки системи	лекція практ	[1–3, 5, 8]	**2** год лекційні **2** год практ. роб. **6** год сам. роб.	3	1ий тиждень
Методи та пристрої забезпечення захисту і безпеки	сам. роб. практ	[1, 3]	**2** год практ. роб. **8** год сам. роб.		2ий тиждень
Захист, доступ та автентифікація. Шифрування файлів	лекція практ	[1, 2, 7]	**2** год лекційні **2** год практ. роб. **6** год сам. роб.	3	3ій тиждень
Моделі захисту інформації	лекція практ	[1, 3, 7, 8]	**2** год лекційні **2** год практ. роб. **6** год сам. роб.	3	4ий тиждень
Відновлення даних	лекція практ	[1, 6, 7]	**2** год лекційні **2** год практ. роб. **6** год сам. роб.	3	5ий тиждень
Антивірусний захист	сам. роб. практ	[1, 3, 6, 7]	**2** год практ. роб. **18** год сам. роб.	3	6ий тиждень
Шифрування даних	лекція практ	[1, 3, 4, 8]	**2** год лекційні **2** год практ. роб. **6** год сам. роб.	3	7ий тиждень
Основні види атак, принципи криптоаналізу	лекція практ	[8-9]	**2** год лекційні **4** год практ. роб. **6** год сам. роб.	3	8ий тиждень
Алгоритми з секретним ключем	лекція практ	[8-9]	**2** год лекційні **6** год практ. роб. **6** год сам. роб.	6	9ий тиждень
Алгоритми з відкритим ключем	лекція	[8-9]	**2** год лекційні	6	10ий

	практ		**6** год практ. роб. **6** год сам. роб.		тиждень
Протоколи автентифікації. Потокові шифри	лекція практ	[8-9]	**2** год лекційні **4** год практ. роб. **6** год сам. роб.	6	11ий тиждень
Хешування. Цифрові підписи. Розподіл таємниці	лекція практ	[8-9]	**2** год лекційні **4** год практ. роб. **6** год сам. роб.	6	12ий тиждень
Сума балів за виконані лабораторні роботи				45	
Тематичний контроль	контрольна робота	[1–9]	Підготовка до к. р., **6** год. с. р. Індивід. завдання, **2** ауд. год.	20	13ий тиждень
Практикум з захисту інформації	сам. роб.	[1–9]	Індивідуальні завдання, **20** год. с. р.	15	7ий – 14ий тижні
Тематичний контроль	тест	[1–9]	Підгот. до тесту, **8** год. с. р.	20	15ий тиждень
Підсумковий контроль	екзамен			**100**	

7. СИСТЕМА ОЦІНЮВАННЯ КУРСУ

Загальна система оцінювання	Підсумкова оцінка з дисципліни у є сумою оцінок за кожен з таких видів робіт: практичні завдання, самостійна робота (практикум та опрацювання окремих тем), тематичний контроль (контрольна робота і тест). Підсумкова оцінка визначається відповідно до поданої нижче таблиці оцінювання за різними шкалами (100-бальна, ECTS, національна).
Авдиторна робота	Максимальна оцінка за правильно виконану та захищену практичну роботу становить 3 бали.
Самостійна робота	Практикум містить по 5 завдань у кожному з 25 варіантів. Максимальна оцінка за виконання і захист завдань практикуму становить 3 бали за кожне завдання.
Тематичний контроль	Кожен варіант контрольної роботи містить 7 завдань на застосування методів захисту інформації. Максимальна оцінка становить 20 балів. Тест містить від 15 до 30 завдань закритого типу на розуміння основних понять, методів та засобів захисту інформації. Максимальна оцінка за тест становить 20 балів.

ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ECTS</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>для екзамену, курсового проекту (роботи), практики</td><td>для заліку</td></tr>
<tr><td>90 – 100</td><td>A</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>80 – 89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>70 – 79</td><td>C</td></tr>
<tr><td>60 – 69</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>50 – 59</td><td>E</td></tr>
<tr><td>26 – 49</td><td>FX</td><td>незадовільно з можливістю повторного складання</td><td>не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-25</td><td>F</td><td>незадовільно з обов’язковим повторним вивченням дисципліни</td><td>не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

8. ПОЛІТИКА КУРСУ

Усі види навчальної роботи слід виконувати вчасно, щоб зберігати загальний темп курсу, котрий сприяє ефективному засвоєнню матеріалу без шкоди здоров’ю. Наслідками пропущених занять без поважних причин, зазвичай, стають додаткові завдання для самостійної роботи.

При проходженні курсу вітаються комунікативність, активність, креативність, самостійність. Плагіат та інші види академічної недоброчесності не принесуть користі, тому є недоречними.

9. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.
2. Ленков С. В. Методы и средства защиты информации. В 2-х томах / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко.Т.II. Информационная безопасность. – К. : Арий, 2008. – 344 с.
3. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и Техника, 2004. – 384 с.
4. Калянов Георгий Николаевич CASE: Структурный системный анализ: (Автоматизация и применение) .-М.:ЛОРИ,1996 .-243с.
5. Карпенко Станіслав Григорович, Іванов Євген Олександрович Основи інформаційних систем і технологій: Навч. посібник/Міжрегіон. академія управлін. персоналом .-Київ, 2002 .-263с.

6. Новак В.О., Симоненко Ю.Г., Бондар В.П., Матвєєв В.В. Інформаційні системи в менеджменті: Підручник для студ. вищ. навч. закл. К.:Каравела, 2008 .- 615с.
7. Смирнова Г.Н. Проектирование электронных систем документооборота: Учеб.пособие.- М.:ФОРУМ-ИНФРА-М,2004 .-118с.
8. Вербіцький О. В. Вступ до криптології. - Львів: ВНТЛ, 1998. - 248с.
9. Бабенко Т.В., Гулак Г.М., Сушко С.О., Фомичова Л.Я. Криптологія у прикладах, тестах і задачах: навч. посібник / Д.: Національний гірничий університет, 2013. - 318 с.

Викладач Мазуренко Н. І.