Державний вищий навчальний заклад
"Прикарпатський національний університет імені Василя Стефаника"

Факультет математики та інформатики

Кафедра інформаційних технологій

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Математичні та алгоритмічні основи криптографічного захисту інформації
(шифр і назва навчальної дисципліни)

Рівень освіти Магістр
(назва рівня вищої освіти)

Галузь знань 12 — Інформаційні технології
(шифр і назва галуза)

Спеціальність(ості) 121 — Інженерія програмного забезпечення
(шифр і назва спеціальності(ей))

Освітня програма Якість та безпека програмного забезпечення
(назва програми)

Затверджено на засіданні
кафедри інформаційних технологій
Протокол №1 від 29.08.2019

Івано-Франківськ — 2019

Зміст

1. Загальна інформація

Назва дисципліни	**Математичні та алгоритмічні основи криптографічного захисту інформації**
Викладач(-і)	Савка І. Я.
Контактний телефон викладача	+380 (342) 59-60-58
E-mail викладача	ivan.savka@pnu.edu.ua
Формат дисципліни	Лекції та лабораторні заняття
Обсяг дисципліни	6 кредитів
Посилання на сайт дистанційного навчання	https://ceeq.pnu.edu.ua
Консультації	Четвер 15^{00}

Дисципліна "Математичні та алгоритмічні основи криптографічного захисту інформації" є складовою освітньо-професійної магістерської програми "Якість та безпека програмного забезпечення" підготовки фахівців зі спеціальності "Інженерія програмного забезпечення", що читається у І семестрі в обсязі 6 кредитів (за Європейською Кредитно-Трансферною Системою ECTS), і розрахована на 60 годин аудиторних занять. З них 30 годин лекцій, 30 годин лабораторних занять і 120 годин самостійної роботи. Дисципліна закінчується екзаменом.

2. Анотація дисципліни

Предметом вивчення дисципліни є криптографія — наука про методи захисту конфіденційності, цілісності і автентичності інформації.

Даний курс знайомить студентів із

- основними фундаментальними поняттями і законами криптографічного захисту інформації для їх використання в сучасних комп'ютерних системах;
- основним математичним апаратом криптографії;
- принципами побудови криптографічних протоколів та їх використання в задачах захисту інформації та даних;
- програмними засобами, які реалізують основні криптографічні протоколи;
- методами та засобами криптографічного захисту даних.

3. Мета і завдання навчальної дисципліни

3.1. **Мета викладання дисципліни.** Метою вивчення навчальної дисципліни "Математичні та алгоритмічні основи криптографічного захисту інформації" є: формування у студентів умінь та компетенцій для забезпечення

реалізації ефективного криптографічного захисту інформації та застосуванню відповідних алгоритмів, методів і засобів криптографічного захисту при розробці сучасних інформаційних систем.

3.2. **Завдання вивчення дисципліни.** Завданням вивчення даного предмету є знайомство з класичними техніками шифрування; алгоритмами сучасних криптосистем та основними засобами криптографічного захисту інформації; формуванню знань, вмінь та практичних навичок ефективного використання та проектування алгоритмів криптографічних перетворень при реалізації захисту програм та даних.

4. Компетентності та результати навчання

Перелік компетентностей:

- ЗК-1. Здатність до абстрактного мислення, аналізу та синтезу.
- СК-1. Здатність аналізувати предметні області, формувати, аналізувати та моделювати вимоги до програмного забезпечення.
- СК-5. Здатність оцінювати ступінь обґрунтованості застосування специфікацій, стандартів, правил і рекомендацій в професійній галузі та дотримуватися їх при реалізації процесів життєвого циклу програмного забезпечення

Перелік результатів навчання:

- ПР-1. Знати і системно застосовувати методи аналізу та моделювання прикладної області, виявлення інформаційних потреб і збору вихідних даних для проектування програмного забезпечення.
- ПР-2. Обґрунтовувати вибір методів формування вимог до програмної системи, розробляти, аналізувати та систематизувати вимоги.
- ПР-4. Оцінювати і вибирати методи і моделі розробки, впровадження, експлуатації програмних засобів та управління ними на всіх етапах життєвого циклу.
- ПР-6. Аналізувати, оцінювати і вибирати методи, сучасні програмно-апаратні інструментальні та обчислювальні засоби, технології, алгоритмічні та програмні рішення для ефективного виконання конкретних виробничих задач з програмної інженерії.
- ПР-7. Обґрунтовано вибирати парадигми і мови програмування для вирішення прикладних завдань; застосовувати на практиці системні та спеціалізовані засоби, компонентні технології (платформи) та інтегровані середовища розробки програмного забезпечення.
- ПР-8. Проводити аналітичне дослідження параметрів функціонування програмних систем для їх валідації та верифікації, а також проводити аналіз обраних методів, засобів автоматизованого проектування та реалізації програмного забезпечення.

- ПР-9. Знати і застосовувати сучасні професійні стандарти і інші нормативно-правові документи з інженерії програмного забезпечення.

У результаті вивчення навчальної дисципліни студент повинен:

Знати: основні криптографічні алгоритми симетричного та асиметричного шифрування, хешування та цифрового підпису; стандартні криптографічні примітиви та порядок їх застосування; базові стандарти в галузі криптографічного захисту інформації.

Вміти: працювати з технічною літературою і документацією; проектувати алгоритми криптографічних перетворень; розробляти криптографічні системи та криптографічні примітиви; здійснювати загальну оцінку якості криптографічного захисту інформації в інформаційних системах.

5. Організація навчання дисципліни

Обсяг дисципліни	
Вид заняття	Загальна кількість годин
Лекції	28
Практичні	
Лабораторні	32
Самостійна робота	120

Ознаки дисципліни				
Спеціальність, освітня програма	Рівень освіти	Курс (рік навчання)	Семестр	Обов'язкова/ вибіркова
121 — Інженерія програмного забезпечення, Якість та безпека програмного забезпечення	Магістр	1-й	1-й	обов'язкова

Тематика дисципліни						
Назви змістових модулів і тем	Кількість годин					
	вс.	лек.	пр.	лаб.	інд.	сам.
Семестр 1						
Змістовий модуль 1. *Класичні та сучасні симетричні криптосистеми*						
Тема 1. *Вступ. Основні поняття. Шифри перестановки та простої заміни. Криптографічна стійкість шифрів.*	12	2		2		8
Тема 2. *Шифри складної заміни. Шифр одноразового блокноту*	12	2		2		8

Тематика дисципліни						
Назви змістових модулів і тем	Кількість годин					
	вс.	лек.	пр.	лаб.	інд.	сам.
Тема 3. *Сучасні симетричні криптосистеми. Мережі Фейстеля. Опис алгоритму DES.*	12	2		2		8
Всього за модуль:	36	6		6		24
Змістовий модуль 2. *Математичний апарат та його застосування в криптографії*						
Тема 4. *Арифметика. Прості числа. НСД. Розширений алгоритм Евкліда. Конгуренції. Кільце лишків. Модульна арифметика. Функція Ейлера. Теореми Ейлера та Ферма.*	12	2		2		8
Тема 5. *Поля Галуа $GF(p^n)$. Побудова полів Галуа $GF(2^n)$.*	12	2		2		8
Тема 6. *SP-мережі. Симетричний алгоритм блочного шифрування AES.*	12	2		2		8
Всього за модуль:	36	6		6		24
Змістовий модуль 3. *Асиметричні криптосистеми*						
Тема 7. *Криптосистеми з відкритим ключем. Алгоритм шифрування RSA*	12	2		2		8
Тема 8. *Протокол обміну ключами Діффі–Хелмана. Шифр Шаміра*	12	2		2		8
Тема 9. *Схема шифрування Ель–Гамаля*	12	2		2		8
Тема 10. *Еліптична криптографія*	12	2		2		8
Всього за модуль:	48	8		8		32
Змістовий модуль 4. *Криптографічні протоколи та методи криптоаналізу*						
Тема 11. *Хешування. Вимоги до хеш-функцій. Схема Меркеля–Дамгарда. Алгоритми сімейства MD і SHA*	12	2		2		8
Тема 12. *Поняття електронного цифрового підпису (ЕЦП). Схеми використання. Система ЕЦП Ель-Гамаля (EGSA).*	12	2		2		8
Тема 13. *Програмна реалізація ЕЦП алгоритмом Ель-Гамаля.*	10			2		8
Тема 14. *Алгоритми цифрових підписів DSA та ECDSA*	12	2		2		8
Тема 15. *Загальні поняття криптоаналізу.*	14	2		4		8
Всього за модуль:	60	8		12		40
Всього за семестр:	180	28		32		120
Усього годин:	180	28		32		120

6. Система оцінювання дисципліни

Система оцінювання курсу відбувається згідно з критеріями оцінювання навчальних досягнень студентів, що регламентовані в університеті. Допуск до іспиту становить максимум 50 балів, бал за складання іспиту (підсумковий контроль) становить максимум 50 балів.

При виставленні допуску до іспиту враховуються наступні навчальні досягнення студентів. Передбачена контрольна робота, за яку студенти можуть отримати до 20 балів. За виконання всіх лабораторних робіт та їх захист студент може отримати до 20 балів. За самостійну роботу, поточне опитування під час аудиторних годин і відвідування студенти можуть отримати до 10 балів.

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка ЄКТС	Оцінка за національною шкалою
90 – 100	A	відмінно
80 – 89	B	добре
70 – 79	C	добре
60 – 69	D	задовільно
50 – 59	E	достатньо
1 – 49	FX	незадовільно

7. Політика курсу

Студент, перебуваючи на лабораторних роботах, отримує індивідуальне завдання та самостійно працює над його виконанням. За результатами виконання лабораторної роботи здається звіт, який захищається усно. Це сприяє розвитку навичок самостійної роботи над поставленою задачею та індивідуальному підходу у опануванні курсу із врахуванням можливостей та базового рівня студента.

Академічна доброчесність. Дотримання академічної доброчесності студентами передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання;
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

- академічний плагіат — оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих

текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;
- самоплагіат — оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів; фабрикація - вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;
- фальсифікація — свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;
- списування — виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності: повторне проходження оцінювання (контрольна робота, іспит тощо); повторне проходження відповідного освітнього компонента освітньої програми.

8. Рекомендована література

1. Вербіцький О. В. Вступ до криптології. – Львів: Видавництво НТЛ., 2008. –248 с.
2. Глинчук Л.Я. Криптологія: навч.-метод. посіб. – Луцьк: Вежа-Друк, 2014. – 163 с.
3. Остапов С.Е., Валь Л.О. Основи криптографії. Навчальний посібник. – Чернівці: Книги – XXI, 2008. – 188 с.
4. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації: навчальний посібник. – Харків: Вид. ХНЕУ, 2013. – 476 с.
5. Лахно В. А. Опорний конспект лекцій з дисципліни "Основи криптографічного захисту інформації". – Київ: [Б. в.], 2016. – 172 с.
6. Столлингс В. Криптография и защита сетей: принципы и практики, 2-е изд.: Пер. с англ. – М.: Изд. дом «Вильямс», 2007. – 672 с.
7. Бабаш А.В., Шанкин Г.П. Криптография. – М.: Солон-ПРЕСС, 2007. – 512 с.
8. Ян С. Криптоанализ RSA. – Ижевск: РХД, 2011. – 312 с.

Додаткова література

9. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК Пресс, 2012. – 256 с.
10. Венбо Мао. Современная криптография. Теория и практика. М: Вильямс, 2005. – 768 с.
11. Ємець В., Мельник А., Попович Р. Сучасна криптографія: основні поняття – Л.: БаК. – 2003. –144 с.
12. Задірака В.К., Олексюк О.С. Комп'ютерна криптологія: Підручник. – Київ – Тернопіль: Збруч, 2002. – 504 с.

13. Шнайер Б. Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С. – М.: ”Триумф”, 2001. – 610 с.
14. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]. – Режим доступу:
https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf

Викладач  Савка І.Я.