Силабус навчальної дисципліни
«*ТЕОРЕТИЧНІ ОСНОВИ КРИПТОГРАФІЇ*»

Спеціальність	*125 Кібербезпека*
Освітня програма	*125 Кібербезпека*
Освітній рівень	*Бакалавр*
Статус дисципліни	*Базова*
Мова викладання	*Українська*
Курс / семестр	*3 курс, 5 семестр*
Кількість кредитів ЄКТС	*5*
Розподіл за видами занять та годинами навчання	*Лекції – 24 год.*
	Практичні (семінарські) – …. год.
	Лабораторні – 24 год.
	Самостійна робота – 102 год.
Форма підсумкового контролю	*екзамен*
Кафедра	*Кібербезпеки та інформаційних технологій, м. Харків, пр-т Науки 9-А, 057-702-18-31, http://www.kafcbit.hneu.edu.ua/*
Викладач (-і)	*Мілов Олександр Володимирович, к.т.н., проф.*
Контактна інформація викладача (-ів)	*oleksandr.milov@hneu.net*
Дні занять	*вівторок*
Консультації	*Понеділок 10.10; дистанційні; відповідно до графіку; індивідуальні*

Мета навчальної дисципліни “Теоретичні основи криптографії” є ознайомлення з теоретичними основами криптології, придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації, розуміння суті інформаційних процесів в криптографічних системах, застосування комп'ютерів для вирішення завдань шифрування і дешифрування, розробка і використання математичних і обчислювальних моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення.

Передумови для навчання

Вступ до фаху, Основи програмування

Зміст навчальної дисципліни

Змістовий модуль 1. Види криптографічних перетворень інформації. Сучасні симетричні криптографічні системи

Тема 1. Основні поняття і визначення криптографії. Принципи криптографічного захисту інформації. Історія розвитку криптографії.

Тема 2. Шифрувальні криптографічні перетворення. Односторонні функції. Хеш-функції. Електронний цифровий підпис. Генератори псевдовипадкових послідовностей.

Тема 3. Шифри перестановки. Шифри заміни (підстановки). Шифри гамування.

Тема 4. Композиційні блокові шифри і принципи їх побудови.

Тема 5. Криптоаналіз і види криптоаналітичних атак.

Тема 6. Стандарт шифрування даних DES. Алгоритм криптографічного перетворення даних ГОСТ 28147-89. Стандарт шифрування США нового покоління (AES).

Змістовий модуль 2. Криптографічні системи з відкритим ключем

Тема 7. Алгоритми шифрування з відкритим ключем.

Тема 8. Криптосистема шифрування RSA. Алгоритм цифрового підпису RSA.

Тема 9. Криптосистема Діффі-Хеллмана. Криптосистема Ель Гамаля. Алгоритм цифрового підпису Ель Гамаля (EGSA).

Тема 10. Криптосистема на основі еліптичних кривих.

Тема 11. Алгоритм безпечного хешування (SHA). Односторонні хеш-функції на основі симетричних блокових алгоритмів. Алгоритми шифрування з відкритим ключем.
Тема 12. Алгоритм цифрового підпису DSA.

Матеріально-технічне (програмне) забезпечення дисципліни

Internet, MS Office

Сторінка курсу на платформі Moodle (персональна навчальна система) Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Теоретичні основи криптографії" https://pns.hneu.edu.ua/course/view.php?id=5733	*Посилання:*

Рекомендовані джерела

Основна

1. *Математичні основи криптографії: конспект лекцій / укладачі: В. А. Фільштінський, А. В. Бережний. - Суми: Сумський державний університет, 2011. - 138 с.*

Додаткова

2. *В. Мао. Современная криптография: теория и практика. - СПб.: Вильямс, 2005, Д 85с.*
3. *Аграновский А. В., Хади Р. А. Практическая криптография: алгоритмы и их программирование - М.: СОЛОН-ПРЕСС, 2009*
4. *Бирюков А. А. Информационная безопасность: защита и нападение - М.: ДМК Пресс, 2012*
5. *Вернет, Пэйн. Криптография. Официальное руководство RSA Security. - М.: Бином, 2002,342с.*
6. *Виега Д., Лебланк Д., Ховард М. 19 смертных грехов, угрожающих безопасности программ : Как не допустить типичных ошибок - М.: ДМК Пресс, 2009 v*
7. *Грэм, Кнут, Паташник. Конкретная математика. - М.: Мир, 1998, 145с.*
8. *П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. Программно-аппаратные средства обеспечения информационной безопасности. Теоретические основы компьютерной безопасности. - М.: Радио и связь, 2000, 176с.*
9. *А.А. Малюк, С.В. Пазизин, Н.С. Погожин. Введение в защиту информации в автоматизированных системах. - М.: Горячая Линия - Телеком, 2001, 126с.*
10. *А.А. Молдовян, Н.А. Молдовян, Гуц, Изотов. - Криптография: скоростные шифры. - СПб.: БХВ, 2002, 222 с.*
11. *Ноден, Ките. Алгебраическая алгоритмика. - М.: Мир, 1999, 192с.*

Інформаційні ресурси

12. *www.cyberpol.ru - Комп'ютерна злочинність і способи боротьби.*
13. *www.iso27000.ru - Інформаційний портал, присвячений питанням управління інформаційною безпекою.*
14. *www.itsec.ru - Інтернет-журнал «Інформаційна безпека».*
15. *www.inside-zi.ru - Інформаційно-методичний журнал «Захист інформації. Інсайд».*
16. *www.kaspersky.ru - Лабораторія Касперського.*
17. *www.drweb.com – Лабораторія DrWeb.*
18. *Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни "Теоретичні основи криптографії" https://pns.hneu.edu.ua/course/view.php?id=5733*

Система оцінювання результатів навчання

*Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально*

можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Більш детальна інформація щодо оцінювання наведена в технологічній карті дисципліни.

Накопичування рейтингових балів з навчальної дисципліни *(приклад)*

Види навчальної роботи	**Max кількість балів**
Лекційні заняття	**12**
Захист лабораторних робіт	**24**
Поточні КР	**24**
Екзамен	**40**
Максимальна кількість балів	**100**

Відповідність шкали оцінювання ЄКТС національній системі оцінювання та ХНЕУ ім. С. Кузнеця

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену (іспиту), диференційованого заліку, курсового проекту (роботи), практики, тренінгу	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

Політики навчальної дисципліни

Політика дотримання академічної доброчесності,
Політика щодо пропусків занять,
Політика щодо виконання завдань пізніше встановленого терміну,
тощо

Більш детальну інформацію щодо компетентностей, результатів навчання, методів навчання, форм оцінювання, самостійної роботи наведено у Робочій програмі навчальної дисципліни «Теоретичні основи криптографії», 2020.

Силабус затверджено на засіданні кафедри «31» серпня 2020 р. Протокол № 2