



**Силабус навчальної дисципліни**  
**«ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ»**

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, <a href="http://www.kafcbit.hneu.edu.ua/">http://www.kafcbit.hneu.edu.ua/</a>
Викладач (-і)	Мілов Олександр Володимирович, к.т.н., проф.
Контактна інформація викладача (-ів)	<a href="mailto:oleksandr.milov@hneu.net">oleksandr.milov@hneu.net</a>
Дні занять	вівторок
Консультації	Понеділок 10.10; дистанційні; відповідно до графіку; індивідуальні

**Мета** навчальної дисципліни “Основи криптографічного захисту” – 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*

Математичний аналіз, лінійна алгебра, теорія ймовірностей і математична статистика, дискретна математика, програмування

**Зміст навчальної дисципліни**

**Змістовий модуль 1. Традиційне шифрування**

Тема 1. Вступ до криптографічних методів захисту.

Тема 2. Традиційне шифрування: класичні методи.

Тема 3. Традиційне шифрування: сучасні методи.

Тема 4. Диференціальний і лінійний криптоаналіз.

Тема 5. Традиційне шифрування: алгоритми "потрійний" DES".

Тема 6. Традиційне шифрування і конфіденційність.

**Змістовий модуль 2. Сучасні методи шифрування**

Тема 7. Розподіл ключів.

Тема 8. Криптографія з відкритим ключем.

Тема 9. Алгоритм RSA.

Тема 10. Управління ключами.

Тема 11. Криптографія з використанням еліптичних кривих.

Тема 12. Цифрові підписи і протоколи аутентифікації.



**Матеріально-технічне (програмне) забезпечення дисципліни**

*Internet, MS Office*

Сторінка курсу на платформі Moodle (персональна навчальна система)

Посилання:  
Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною «Основи криптографічного захисту»

<https://pns.hneu.edu.ua/course/view.php?id=4923>

**Рекомендовані джерела**

*Базова*

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

**Система оцінювання результатів навчання**

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімумально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімумально 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	Мах кількість балів
Лекційні заняття	12
Захист лабораторних робіт	24
Поточні КР	24
Екзамен	40
<b>Максимальна кількість балів</b>	<b>100</b>



<b>Відповідність шкали оцінювання ЄКТС національній системі оцінювання та ХНЕУ ім. С. Кузнеця</b>			
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		
60 – 63	E	задовільно	не зараховано
35 – 59	FX	незадовільно	
1 – 34	F		
<b>Політики навчальної дисципліни</b> <i>Політика дотримання академічної доброчесності, Політика щодо пропусків занять, Політика щодо виконання завдань пізніше встановленого терміну, тощо</i>			
<i>Більш детальну інформацію щодо компетентностей, результатів навчання, методів навчання, форм оцінювання, самостійної роботи наведено у Робочій програмі навчальної дисципліни «Вступ до фаху», 2020.</i>			

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