



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

Спеціальність	125 Кібербезпека
Освітня програма	Кібербезпека
Освітній рівень	Бакалавр
Статус дисципліни	Обов'язкова
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) – немає 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	Згідно діючого розкладу занять
Консультації	Відповідно до графіку
<p><b>Мета</b> 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.</p>	
<p><b>Передумови для навчання</b> Математичний аналіз, лінійна алгебра, теорія ймовірностей і математична статистика, дискретна математика, програмування</p>	
<p><b>Зміст навчальної дисципліни</b></p> <p><b>Змістовий модуль 1. Безпека і захист даних</b></p> <p>Тема 1. Механізми і політики розподіл прав доступу</p> <p>Тема 2. Механізми шифрування. Симетричні та несиметричні криптосистеми</p> <p>Тема 3. Протоколи автентифікації. Цифрові підписи</p> <p>Тема 4. Комплексні системи захисту даних</p> <p>Тема 5. Основні види атак на програмне забезпечення. Основи криптоаналізу</p> <p>Тема 6. Основи цифрової стеганографії</p> <p><b>Змістовий модуль 2. Безпека в програмному забезпеченні</b></p> <p>Тема 7. Основи технології відкритих ключів (PKI)</p> <p>Тема 8. Захист програмного забезпечення в Інтернет-технологіях</p> <p>Тема 9. Захист персональних даних</p> <p>Тема 10. Основні принципи захисту програмного забезпечення</p>	



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

*Internet, MS Office*

**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**

<b>Види навчальної роботи</b>	<b>Мах кількість балів</b>
Лекційні заняття	<b>12</b>
Захист лабораторних робіт	<b>24</b>
Поточні КР	<b>24</b>
Екзамен	<b>40</b>
<b>Максимальна кількість балів</b>	<b>100</b>

**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 «*Основи криптографічного захисту*», <http://www.repository.hneu.edu.ua/handle/123456789/24048>.**