



Силабус курсу

Програмно-апаратні засоби захисту інформації

Освітньо-професійна програма «Комп'ютерна інженерія»

Ступінь вищої освіти – магістр

Спеціальність: 123 «Комп'ютерна інженерія»

Рік навчання: 1, Семестр: 1

Кількість кредитів: 5, Мова викладання: українська

Керівник курсу

ППП

к.т.н., доцент Леся Дубчак

Контактна інформація dlo@wunu.edu.ua

Опис дисципліни

Дисципліни "Програмно-апаратні засоби захисту інформації" передбачає отримання студентами навиків та знань щодо захисту інформації в комп'ютерних системах

Структура курсу

№п/п	Тема	Результати навчання	Завдання
1	Задачі криптографії	Засвоїти основні поняття та положення комп'ютерної криптографії, принципи та історія розвитку криптографічного захисту інформації.	Опитування
2	Історія розвитку засобів захисту інформації	Засвоїти прості алгоритми захисту інформації.	Опитування
3	Сучасні симетричні криптосистеми	Опанувати поняття симетричних криптоалгоритмів, процес шифрування та дешифрування алгоритму DES та IDEA	Опитування

4	Арифметика асиметричних криптосистем, генерація ключів	Засвоїти поняття асиметричних криптоалгоритмів та їх математичні основи.	Тести
5	Криптосистема RSA	Вивчити процес шифрування та дешифрування криптоалгоритму RSA	Опитування
6	Криптосистеми Рабіна та Ель-Гамалія	Засвоїти процес шифрування та дешифрування криптоалгоритмів Рабіна та Ель-Гамалія	Опитування
7	Алгоритми електронного цифрового підпису	Вивчити основні поняття електронного цифрового підпису, способи його реалізації та сфери застосування	Опитування
8	Криптографічні протоколи	Засвоїти поняття криптографічного протоколу, вивчити протоколи обміну ключем, жеребу по телефону, розподілу таємниці	Опитування
9	Класичні та сучасні методи криптоаналізу	Ознайомитись з поняттям криптоаналізу, частотного аналізу, методом зустрічі посередині, методом «парадоксу днів народження» та сучасними атаками на реалізацію та засоби захисту від них.	Опитування
10	Засоби захисту фінансових даних	Засвоїти процес Internet-банкінг, роботу POSтерміналів, банкоматів та методи захисту фінансових даних.	Опитування
11	Сучасні апаратні засоби захисту інформації	Ознайомитися з засобами аутентифікації користувача, протидії несанкціонованому доступу та засобом захисту інформації «Ельбрус».	Опитування
12	Політика безпеки інформації. Законодавча база захисту інформації в Україні.	Засвоїти поняття політики безпеки, нормативно-правового та організаційного забезпечення безпеки, комунікаційнотехнічного забезпечення та програмного забезпечення	Тести

Літературні джерела

1. Бурячок В.Л. Інформаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толупа. – К.: ДУТ, 2015. – 288 с.
2. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
3. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт.

4. Закон України «Про державну таємницю» від 21.01.1994 // Відомості Верховної Ради України, 1994, № 16. – Ст. 93.
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2005 р.
6. Закон України «Про інформацію» // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.
7. Остапов С.Е. Кібербезпека: сучасні технології захисту / С.Е. Остапов, С.П. Євсєєв, О.Г. Король. – К.: Новий світ-2000, 2020. – 678 с. 17. Хорошко В. О. Проектування комплексних систем захисту інформації./ В.О. Хорошко. – Львів: Видавництво Львівської політехніки, 2020. – 317 с.

Політика оцінювання

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3 (підсумкова оцінка за КПЗ)	Заліковий модуль 4 (екзамен)	Разом
20%	20%	20%	40%	100%
1. Усне опитування під час занять (6 тем по 10 балів = 60 балів) 2. Письмова робота = 40 балів	1. Усне опитування під час занять (6 тем по 10 балів = 60 балів) 2. Письмова робота = 40 балів	1. Написання та захист КПЗ = 80 балів 2. Виконання завдань під час тренінгу = 20 балів	1. Тестові завдання = 50 балів 2. Практичне завдання = 50 балів	

Шкала оцінювання:

За шкалою ЗУНУ	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75–84		C (добре)
65–74	задовільно	D (задовільно)
60–64		E (достатньо)
35–59	незадовільно	FX (незадовільно з можливістю повторного складання)

