Програма підготовки бакалаврів у галузі знань 12 – "Інформаційні технології" зі спеціальності 121 –"Інженерія програмного забезпечення"

"Безпека програм та даних"

120 год. / 4 кредити ЕКТС
(15 год. лекцій, 30 год. лабораторних занять)

Навчальний контент

5-й семестр

Модуль 1. Захист інформації, криптографія і криптоаналіз.

Змістовий модуль 1.1 Введення у захист інформації. Шифри. Алгоритми.

Тема 1. Основні концепції захисту інформації.
Тема 2. Криптографія і криптоаналіз, потокові і блокові шифри.

Змістовий модуль 1.2 Введення у захист інформації. Шифри. Алгоритми.

Тема 3. Сучасні алгоритми симетричного шифрування.
Тема 4. Принципи побудови криптосистем з відкритим ключем.

Модуль 2. Коди та протоколи і програмування систем безпеки.

Змістовий модуль 2.1 Коди. Цифрові підписи та протоколи.

Тема 5. Коди автентичності повідомлень та функції хешування.
Тема 6. Цифрові підписи та протоколи автентифікації.

Змістовий модуль 2.2 Програмна реалізація ПЗ та аналіз безпеки.

Тема 7. Програмна реалізація криптографічних алгоритмів, безпека прикладних програм.
Тема 8. Моделювання загроз ПЗ, методи безпечної реалізації ПЗ.
Тема 9. Методи і засоби аналізу безпеки ПЗ.

Програма підготовки бакалаврів у галузі знань 12 – "Інформаційні технології" зі спеціальності 121 –"Інженерія програмного забезпечення"

"Безпека програм та даних"

120 год. / 4 кредити ЕКТС
(15 год. лекцій, 30 год. лабораторних занять)

Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
5-й семестр		
1	Програмування процедур роботи зі стеками.	7
2	Програмування процедур роботи з чергами.	7
3	Програмування процедур роботи зі списками.	8
4	Програмування процедур роботи з деревами.	8
Разом		**30**

Програма підготовки бакалаврів у галузі знань 12 – "Інформаційні технології" зі спеціальності 121 –"Інженерія програмного забезпечення"

"Безпека програм та даних"

120 год. / 4 кредити ЕКТС
(15 год. лекцій, 30 год. лабораторних занять)

Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин
5-й семестр		
1	Моделі загроз безпеки програмного забезпечення	6
2	Формальні методи доказу правильності програм і їх специфікації	6
3	Конфіденційні обчислення	6
4	Самотестуючи і само корегуючи програми	6
5	Захист програм і забуванне моделювання на RAM-маши-	6

	нах	
6	Кріптопрограмування за допомогою використання інкрементальних алгоритмів	6
7	Захист програм від автоматічної генерації інструментальними засобами програмних закладок	6
8	Методи ідентифікації програм	6
9	Методи і засоби захисту програм від комп'ютерних вірусів	6
10	Методи захисту програмного забезпечення від дослідження коду	7
11	Методи і засоби забезпечення цілісності та достовірності використовуваного програмного коду	7
12	Підходи до захисту програм від несанкціонованого копіювання	7
Разом		75

Програма підготовки бакалаврів у галузі знань 12 – "Інформаційні технології" зі спеціальності 121 –"Інженерія програмного забезпечення"

"Безпека програм та даних"

120 год. / 4 кредити ЕКТС
(15 год. лекцій, 30 год. лабораторних занять)

Завдання для поточного та підсумкового контролю

5-й семестр

Контрольні питання до 1-го модуля

1. Які основні концепції захисту інформації?
2. Що таке криптографія?
3. Що таке стеганографія?
4. Яке бувають шифри?
5. Який алгоритм симетричного шифрування?
6. Який алгоритм несиметричного шифрування?
7. Що таке системи з відкритим ключем?
8. Що таке системи симетричного шифрування?
9. Які принципи побудови криптосистем вважаються сучасними?
10. Які використовують шифри?
11. Що таке криптоаналіз?

Контрольні питання до 2-го модуля

1. Що таке коди?
2. Які методи автентифікації ви знаєте?
3. Що таке функції хешування?
4. Що таке цифрові підписи?
5. Що таке протоколи автентифікації?
6. Опишіть криптографічний алгоритм?
7. Як програмно реалізуються криптографічні алгоритми?
8. Що таке безпека прикладних програм?
9. Що таке моделювання загроз ПЗ?
10. Де використовують методи безпечної реалізації ПЗ?
11. Які методи аналізу безпеки ПЗ ви знаєте?
12. Які засоби аналізу безпеки ПЗ ви знаєте?