ЗАТВЕРДЖЕНО
Методичною радою
університету
від 26.02.2020
(протокол №5)

Силабус
навчальної дисципліни
Криптографічні методи перетворення інформації
2023-2024 навчальний рік

Освітня програма «Цифрові технології»
Спеціальність 015 Професійна освіта (Цифрові технології)
Галузь знань 01 Освіта/Педагогіка
Рівень вищої освіти перший

Викладач	Антоненко Олександр Володимирович
Посилання на сайт	
Контактний тел.	
E-mail викладача:	oleksandrantonenkobdpu@gmail.com
Графік консультацій	Понеділок 13:00-14:15

Обсяг курсу на поточний навчальний рік:

Кількість кредитів/ годин	Лекції	Лабораторні заняття	Самостійна робота	звітність
3/90	12	12	66	залік

Семестр: ~~осінній~~/весняний
Мова навчання: українська
Ключові слова: шифрування, алгоритм, криптографія, ключ, цифровий підпис.
Мета та предмет курсу: ознайомлення студентів з основними методами й засобами захисту комп'ютерної інформації, методам і алгоритмам криптографічного захисту (симетричним і асиметричним алгоритмам шифрування, функціям хешування, електронного цифрового підпису, аутентифікації й керування криптографічними ключами).

Компетентності та програмні результати навчання:

Загальні компетентності:

- ЗК 10. Здатність до абстрактного та аналітичного мислення й генерування ідей.
- ЗК 13. Здатність бути критичним і самокритичним при прийнятті обґрунтованих рішень та оцінюванні якості виконуваних робіт.

Фахові компетентності:

- ФК 2. Здатність до організації матеріально-технічного забезпечення технологічного процесу виробництва ІТ-продукту та процесу професійної підготовки з комп’ютерних технологій.
- ФК 7. Здатність до використання ІТ-продуктів та методик професійного навчання.

- ФК 8. Здатність до відновлення метеріально-технічного забезпечення виробничого та освітнього процесів.

Результати навчання:

- ПР 6. Застосовувати відповідне програмне забезпечення виробничого та освітнього призначення.
- ПР 9. Розуміти принципи функціонування матеріально-технічного забезпечення виробничого та освітнього процесів.
- ПР 13. Розв’язувати типові спеціалізовані задачі у виробничому та освітньому процесах.

Зміст курсу:

Змістовій модуль 1. *Вступ. Історія криптографії. Методи криптографічного захисту інформації.*

Тема 1. Вступ. Історія криптографії.

Тема 2. Методи криптографічного захисту інформації.

Змістовій модуль *2. Симетричні та асиметричні алгоритми шифрування*

Тема 3. Симетричні алгоритми шифрування.

Тема 4. Асиметричні алгоритми шифрування.

Змістовій модуль3. *Функції хешування. Електронний цифровий підпис*.

Тема 5. Функції хешування

Тема 6. Електронний цифровий підпис.

Змістовій модуль 4. *Ідентифікація й аутентифікація. Керування криптографічними ключами*

Тема 7. Ідентифікація й аутентифікація.

Тема 8. Керування криптографічними ключами.

Методи навчання:

- методи організації і здійснення навчально-пізнавальної діяльності:
  - пояснення;
  - розповідь;
  - бесіда;
  - ілюстрування;
  - демонстрування;
  - самостійне спостереження;
  - практичні і дослідні роботи;
- методи стимулювання навчальної діяльності:
  - створення ситуації інтересу у процесі викладення;
  - створення ситуації новизни;
  - опора на життєвий досвід студента;
  - стимулювання обов'язку і відповідальності в навчанні;
- методи контролю і самоконтролю у навчанні:
  - індивідуальне опитування, фронтальне опитування, комбіноване опитування;
  - тестовий, самоконтроль і самооцінка.

Політика курсу (особливості проведення навчальних занять): очне, заочне, дистанційне, робота з лабораторним обладнанням.

Технічне й програмне забезпечення/обладнання, наочність: лабораторне обладнання, спеціалізоване програмне забезпечення, вимірювальні прилади.

Система оцінювання та вимоги:

1. Поточний контроль

- звіт з лабораторної роботи;

- звіт з самостійної роботи;
- індивідуальне завдання;
- індивідуальне опитування;
- фронтальне опитування;
- комбіноване опитування;

2. Залік

Критерії оцінювання завдань змістових модулів

Максимальна кількість балів разом із самостійною роботою за кожну тему становить 25 балів. Система нарахування балів подана в таблиці. Контроль включає оцінювання знань, умінь та навичок.

Завдання оцінюється 10-ма балами, якщо відповідь правильна, повна, з достатнім теоретичним обґрунтуванням, позначена елементами творчості; має місце аргументація особистої позиції, правильно оформлена лабораторна робота.

Оцінка "8-9 бали": відповідь правильна, логічна, обґрунтована, але без елементів власних суджень, правильно оформлена лабораторна робота..

Оцінка "6-7 бали": в цілому завдання виконано правильно, повністю, проте мають місце окремі неточності, або розв'язання не містить належного теоретичного обґрунтування, правильно оформлена лабораторна робота..

Оцінка "4-5 бали": відповідь неповна, поверхова, характеризується відсутністю самостійного аналізу, правильно оформлена лабораторна робота..

Оцінка "2-3 бал": відповідь елементарна, фрагментарна, що зумовлено нечітким уявленням про предмет питання, правильно оформлена лабораторна робота..

Оцінка "1 бал": тільки правильно оформлена лабораторна робота.

Оцінка "0 балів": неправильна відповідь або її відсутність, лабораторна робота не оформлена.

Система рейтингових (вагових) балів та критерії оцінювання

Лабораторні роботи. Ваговий бал – 10, в тому числі підготовка протоколу – 2 бали, виконання роботи – 4 бали, захист роботи – 4 бали.

*0..2 підготовка протоколу :*2 – якісна підготовка, акуратно оформлений протокол лабораторної роботи; 1 - наявність недоліків у оформленні протоколу лабораторної роботи; 0 – грубі помилки при оформленні протоколу лабораторної роботи, протокол відсутній

0..4 виконання роботи, захист роботи: 4 – акуратне та правильне виконання роботи, логічна та послідовна відповідь при захисті лабораторної роботи; 3 – наявність незначних недоліків у відповідях при виконанні, захисті лабораторної роботи; 2-1 – наявність недоліків у виконанні, у відповідях при захисті лабораторної роботи, протоколі; 0 –відсутність виконання роботи, грубі помилки при інтерпретації результатів розрахунку, студент неспроможний захистити роботу.

Штрафні бали.

Несвоєчасний захист лабораторної роботи, незадовільний вхідний контроль – (1..5) балів

Заохочувальні бали.

Участь у модернізації лабораторних робіт, удосконаленні дидактичних матеріалів 5..15 балів Інформаційний пошук та підготовка реферату з наданої викладачем теми 5..10 балів

Список рекомендованих джерел

Основні

Антоненко О.В. Криптографічні методи перетворення інформації / О.В. Антоненко - Навчальний посібник + CD для студентів вищих педагогічних навчальних закладів напряму

підготовки 6.010104 Професійна освіта (Комп'ютерні технології). – Бердянськ, 2015. – 177 с.

Бабаш, А.В. Криптография. / А.В. Бабаш, Г.П. Шанкин. — М.: Солон-Р, 2002. — 512 с.: іл.

Левин, М. Криптография: руководство пользователя. / М Левин. — М.: Познав. книга плюс, 2001. — 320 с.: іл.

Столлингс, В. Криптография и защита сетей: принципы и практика: пер. с англ / В Столлингс. — 2-е видання. — М.: Вильямс, 2001. — 672 с.: іл.

Допоміжні

Алферов А.П., Зубов А.Ю. и др. Основы криптографии: Учеб. пособие, 2-е изд., испр. и доп. М.: Гелиос АРВ, 2002.- 480 с.: ил.

Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные коды на языке С. 1996.

Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. М.: "Горячая линия - Телеком", 2001.

Ємець А.В., Мельник В.В., Попович П.А. Сучасна криптографія. Основні поняття. Львів, 2003 р. – 156 С.

1.