Національний університет водного господарства та природокористування

Опис навчальної дисципліни

1. Код:*113.*
2. Назва:*Захист інформації.*
3. Тип:*вибірковий.*
4. Рівень вищої освіти: *I (бакалаврський).*
5. Рік навчання, коли пропонується дисципліна:*4.*
6. Семестр, коли вивчається дисципліна:*VII.*
7. Кількість встановлених кредитів ЄКТС*:3.*
8.Прізвище, ініціали лектора/лекторів, науковий ступінь, посада:*Рощенюк А.М., ст.викладач кафедри прикладної математики.*
9. Результати навчання: *після вивчення дисципліни студент повинен бути здатним:*

- *знатиструктуру та функції сучасних систем захисту інформації, математичні та алгоритмічні основи криптографії, алгоритми кодування та стискання файлів;*
- *програмувати з використаннях сучасних захисних криптографічних елементів в середовищі С++;*
- *проектувати та створювати надійні реалізації криптографічних алгоритмів, систем та протоколів;*
- *планувати та реалізовувати комплекс профілактичних антивірусних заходів, попереджувати та виявляти випадки несанкціонованого проникнення в локальні мережі.*

10. Форми організації занять:*навчальне заняття, самостійна робота, практична підготовка, контрольні заходи;*
11.

- **Дисципліни, що передують вивченню даної дисципліни:***Програмування, Прикладне програмне забезпечення.*
- **Дисципліни, що вивчаються супутньо із зазначеною дисципліною:***Адміністрування комп'ютерних мереж.*

12. Зміст курсу:*Вступ до криптографії та криптоаналізу. Коди та їх призначення. Коротка історія криптології. Елементи криптоаналізу. Характеристика повідомлень, випробування шифрів, відкриття машинного шифра.*
Елементарна криптографія. Шифри простої заміни. Поліграмні та поліалфавітні шифри. Шифри перестановки. Шифрування блоками. Дешифрування ітераціями.
Криптосистеми з відкритим ключем. Концепція відкритих систем. Система RSA, її опис, коректність, надійність. Система Рабіна. Ідентифікація за допомогою симетричної криптосистеми, на основі цифрового підпису.
Безпека комп'ютерних та мережевих систем. Комп'ютерні віруси і троянські програми. Правові і соціальні питання захисту інформації;
13. Рекомендовані навчальні видання:

1. *Шеннон К. Теория связи в секретных системах. / Работы по теории информации и кибернетике. – М.: ИЛ, 1963. – 829 с.*
2. *Вербіцький О.В. Вступ до криптології. – Л.: Видавництво науково-технічної літератури, 1998. – 247 с.*

Національний університет водного господарства та природокористування

3. *Введение в криптографію: монографія. /Подобщ. ред. В.В.Ященко. –М.: МЦНМО: ЧеРо, 1998. – 271 с.*
4. *Молдовян Р.А., Молдовян Н.А., Советов Б.Я. Криптография. –СПб: Лань, 2000. – 224 с.*
5. *Столлингс В. Криптография и защитасетей: принципы и практика. – М.: Изд. домВильямс, 2001. – 672 с.*
6. *Проскурин В.Г., Крутов С.В., Мацкевич И.В. Защита в операционных системах. – М.: Радио и связь, 2000. – 168 с.*

14. Заплановані види навчальної діяльності та методи викладання:

28 години лекцій, 14 години лабораторних робіт.

Методи: елементи проблемної лекції, індивідуальні завдання, використання мультимедійних засобів;

15. Форми та критерії оцінювання:

Оцінювання здійснюється за 100-бальною шкалою.

Підсумковий контроль (20 балів): ***залік*** *в кінці VII семестру.*

Поточний контроль (80 балів): тестування, опитування;

16. Мова викладання:*українська.*

Завідувач кафедри *Мартинюк П.М., д.т.н., доцент*

Національний університет водного господарства та природокористування

Національний університет
водного господарства
та природокористування

П Е Р Е К Л А Д А Н Г Л І Й С Ь К О Ю

DESCRIPTION OF THE EDUCATIONAL SUBJECT

1. Code: 113.
2. Title: Information security.
3. Type: selective.
4. Higher education level: the first (Bachelor's degree).
5. Year of study when the discipline is offered: 4.
6. Semester when the discipline is studied: VII.
7. Number of established ECTS credits: 3.
8. Name, initials of the lecturer / lecturers, scientific degree, position: Roshcheniuk A.M., senior lecturer of the department of applied mathematics.
9. Results of studies: after having studied the discipline the student must be able:
• to know the structure and functions of modern information security systems, mathematical and algorithmic fundamentals of cryptography, algorithms for encoding and compressing files;
• to program using modern security cryptographic elements in the C ++ environment;
• to design and create reliable implementations of cryptographic algorithms, systems and protocols;
• to plan and implement a set of preventive antivirus measures;
• to prevent and detect cases of illegal access to local networks.
10. Forms of organizing classes: training classes, independent work, practical training, control measures;
11 • Disciplines preceding the study of the specified discipline: Programming, Applications software.
• **Disciplines studied in conjunction with the specified discipline:** Administration of computer networks.
12. Course contents: Introduction to cryptography and cryptanalysis. Codes and their use. A brief history of cryptology. Elements of cryptanalysis. Characteristics of messages, test of ciphers, opening machine cipher.
Elementary cryptography. Simple replacement ciphers. Polygram and polyphonic ciphers. Ciphers of permutation. Block encryption. Iteration decryption.
Public key cryptosystems. Concept of open systems. RSA system, its description, correctness, reliability. Rabin's system. Identification by means of a symmetric cryptosystem, based on a digital signature.
Security of computer and network systems. Computer viruses and Trojan programs. Legal and social issues of information security.
13. Recommended educational editions:
1. Shannon K. Communications theory in secret systems. / Works on the information and cybernetics theory. – Moscow: IL, 1963. – 829 p.
2. Verbitskyi O.V. Introduction to cryptology. – L.: Publishing house of scientific and technical literature, 1998. – 247 p.
3. Introduction to cryptography: a monograph. / gener. ed. by V.V.Yashchenko. – M.: MTsNMO: CheRo, 1998. – 271 p.
4. Moldovian R.A., Moldovian N.A., Sovetov B.Ya. Cryptography – SPb.: Lan', 2000. – 224 p.
5. Stollings V. Cryptography and protection of networks: principles and practice. – M .: Publ. house Williams, 2001. – 672 p.
6. Proskuryn V.G., Krutov S.V., Matskevych I.V. Security in operating systems. – M .: Radio and communication, 2000. – 168 p.
14. Planned types of educational activities and teaching methods:

Національний університет
водного господарства
та природокористування

lectures – 28 hours, laboratory works – 14 hours.
Methods of teaching: problem lecture elements, individual tasks, using multimedia presentations.

15. Forms and assessment criteria:

The assessment is carried out on a 100-point scale.
Final control (20 points): **test** at the end of the 7th semester.
Current control (80 points): testing, questioning.

16. Language of teaching: Ukrainian.

Head of the department,
Doctor of Engineering, associate professor P.M. Martyniuk

Переклад виконав П.І.Мігірін

Національний університет
водного господарства
та природокористування