

Факултет: ФАКУЛТЕТ ПО ТЕЛЕКОМУНИКАЦИИ И МЕНИДЖМЪНТ

Катедра: ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

Професионално направление: 5.3. КОМУНИКАЦИОННА И КОМПЮТЪРНА ТЕХНИКА

Специалност: ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

Образователно-квалификационна степен: МАГИСТЪР

ОПИСАНИЕ НА ЛЕКЦИОНЕН КУРС

1. Наименование на курса: *Криптографска защита на корпоративни данни*

2. Код на курса: М.01.046.2

3. Вид на курса: *избираема*

4. Ниво: *магистър*

5. Година на изучаване: *втора*

6. Семестър: *четвърти*

7. Брой кредити: 3

8. Име на лектора: *доц. д-р Иван Иванов*

9. Резултати от обучението за дисциплината:

Целта на курса е да даде на студентите в систематизиран вид теоретични и практически знания за основни криптографски алгоритми и различни свери на тяхното приложение.

Студентите, приключили обучението си по дисциплината, трябва да придобият:

Основни знания по спецификата и използването на криптографски алгоритми в областта на приложната криптография.

Практически умения за работа с криптографски алгоритми, както и приложения и протоколи използващи същите.

Компетенции: След успешно приключване на курса студентите трябва да могат:

- След приключване на курса студентите, трябва да са усвоили механизмите за работа и практическа реализация на криптографски алгоритми.

10. Начин на преподаване:

Начинът на преподаване: Лекциите се провеждат чрез запознаване на студентите с предвидения в учебната програма материал. Лекциите са онагледени с графичен и видео материал, с нагледни примери и задачи, които са представени чрез презентации с мултимедиен проектор.

Практическите упражнения се провеждат в лабораториите на катедрата, оборудвани със съвременни компютри и мрежови устройства, като всеки студент работи самостоятелно.

Преди всяко практическо занятие студентите се информират за необходимостта от предварителна подготовка по темата.

11. Предварителни изисквания:

Студентите следва да имат задълбочени познания по инженерна математика и основите на сигурността.

Курсове, ползващи дисциплината са: изходяща дисциплина

12. Съдържание на курса:

Курсът разглежда актуални теми, свързани със работата прилагането на блокови, поточни и асиметрични криптографски алгоритми.

13. Библиография

Основна литература:

1. Иванов И. Основи на криптографията, Издателство ВУТП, 2021.
2. Stallings W., Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, March 5, 2016.
3. Schneier B. Applied Cryptography Protocols, Algorithms, and Source Code in C, Wiley, pp. 81-221, 2013.
4. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации. КНОРУС. Москва, 2016.

5. Фороузан Б. А., Управление ключами шифрования и безопасность сети (2-е изд.), М.: НОУ "Интуит", 2016.

Допълнителна литература:

1. Иванов И. Ръководство за лабораторни упражнения по сигурност и защита на информацията и администриране и защита на комуникационни и компютърни мрежи, изд. център-ВУ КТП, София, 2013, ISBN: 978-954-9332-88-9.
2. Easttom C, Modern Cryptography: Applied Mathematics for Encryption and Information Security, McGraw-Hill Education, October 12, 2015.
3. Hoffstein J, Pipher J, Silverman J, An Introduction to Mathematical Cryptography 2nd Edition, Springer, September 11, 2014.
4. Мэйволд Э. Безопасность сетей. Национальный Открытый Университет "ИНТУИТ", 2016.
5. Бехроуз А. Ф., Математика криптографии и теория шифрования (2-е изд.), М.: НОУ "Интуит", 2016.

14. Методи и критерии на оценяване:

Оценяването на дисциплината се формира по точкова система, като максималният брой точки, които могат да получат студентите е 100 (виж таблица 1). Знанията, уменията и компетентностите се оценяват чрез провеждане на писмени контролни работи за проверка на теоретичното и практическото усвояване на учебния материал, представянето на студентите по време на практическите упражнения, както и способността им за самостоятелно решаване на задачите, поставени в практическите упражнения. Дисциплината завършва с писмен изпит.

Таблица 1.

Брой точки	Оценка по шестобалната система
0 – 20	Слаб 2 (F)
20 – 39	Слаб 2 (FX)
40 – 49	Среден 3,00 (E)
50 – 59	Среден 3,00 (D)
60 – 69	Добър 4,00 (C)
70 – 84	Мн. добър 5,00 (B)
85 – 100	Отличен 6,00 (A)

15. Език на преподаване: български