

Факултет: ФАКУЛТЕТЪТ ПО ТЕЛЕКОМУНИКАЦИИ И МЕНИДЖМЪНТ
Катедра: ИНФОРМАЦИОННИ ТЕХНОЛОГИИ
Професионално направление: 5.3. КОМУНИКАЦИОННА И КОМПЮТЪРНА ТЕХНИКА
Специалност: КОМПЮТЪРНО АДМИНИСТРИРАНЕ НА СОФТУЕЪРНИ ПРИЛОЖЕНИЯ
Образователно-квалификационна степен: ПРОФЕСИОНАЛЕН БАКАЛАВЪР

ОПИСАНИЕ НА ЛЕКЦИОНЕН КУРС

1. Наименование на курса: *ОСНОВИ НА КРИПТОГРАФИЯТА*
2. Код на курса: P.18.026.1
3. Вид на курса: задължителен
4. Ниво: бакалавър
5. Година на изучаване: втора
6. Семестър: 4
7. Брой кредити: 4,5
8. Име на лектора: доц. д-р инж. Иван Иванов
9. Резултати от обучението за дисциплината – усвоени знания, умения, компетенции (цели):
Целта на дисциплината основи на криптографията е да се даде на студентите в систематизиран вид основни (фундаментални) познания в областта на криптографията.
10. Начин на преподаване: лекции и практически упражнения
11. Предварителни изисквания (пред-условни или съусловни дисциплини):
Студентите следва да имат задълбочени познания в областта на за технологията на прилагане на криптографските алгоритми на ниво бит, както и възможностите за тяхното имплементиране в различни приложения и крайни устройства. От съществено значение са знанията придобити по дисциплините Инженерна математика, Основи на сигурността, Кибер заплахи и кибер кризи и Обектно-ориентирано програмиране.
12. Съдържание на курса (анотация):
В дисциплината се разглеждат актуални теми, свързани с историята на криптографията, както и основните криптографски процедури и схеми на която база лежат всички съвременни алгоритми. Направена е класификация на криптографските алгоритми, както са разгледани по-известните във всяко едно направление – симетрични, асиметрични и поточни.
13. Библиография (препоръчителна или задължителна литература)
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. Бабаи 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:

За оценка на студентите се използва точкова система. Оценяват се знания, умения и компетентност чрез провеждане на писмени контролни работи за проверка на теоретичната и практическата усвояемост на учебния материал, представянето на студентите по време на практическите упражнения, както и умението им за самостоятелно решаване на задачите поставени на практическите упражнения. Дисциплината завършва с писмен изпит.

Тежест на оценяването:

15. Език на преподаване: български