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: *Приложна криптография*
2. Код на курса: 23.1.4.0.21
3. Вид на курса: *задължителен*
4. Ниво: *магистър*
5. Година на изучаване: *втора*
6. Семестър: *четвърти*
7. Брой кредити: *4*
8. Име на лектора: *гл. ас. д-р Иван Иванов*
9. Резултати от обучението за дисциплината– усвоени знания, умения, компетенции (цели):

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

Основни знания за защита от паразитни информационни излъчвания, защита на електрозахранването и от случайни грешки, политики за обмяна на ключовете, криптографска защита на информационния обмен в комуникационните мрежи, защитени протоколи за обмен на данни, хардуерни защитни стени и системи за откриване/превенция от проникване в мрежата (IDS/IPS), оценка за устойчивост на криптографската защита и др.

Практически умения за ограничаване на достъпа до комуникационно информационните мрежи, прилагане на SHA, криптографски ключове и тяхното управление, криптографска защита на телефонните разговори, сигурност и криптиране в GSM, WLAN сигурност, хардуерни защитни стени и системи за откриване/превенция от проникване в мрежата (IDS/IPS), MS Direct Access – управление на контрол на достъпа до корпоративен интранет, оценка за устойчивост на криптографската защита и др.

Целта на курса е да даде на студентите в систематизиран вид теоретични и практически знания за ограничаване на достъпа до комуникационно информационните мрежи, SHA - сигурни хеширащи алгоритми, криптографски ключове и тяхното управление, криптографска защита на телефонните разговори, сигурност и криптиране в GSM, WLAN сигурност, хардуерни защитни стени и системи за откриване/превенция от проникване в мрежата (IDS/IPS) и др.

10.Начин на преподаване: *лекции и практически упражнения*

11.Предварителни изисквания:

Необходими предварителни знания по дисциплините:

„Интернет комуникации", „Компютърно моделиране и симулиране на мрежи", „Проектиране на потребителски интерфейс"

12. Съдържание на курса (анотация):

Дисциплината съдържа: Ограничаване на достъпа до комуникационно информационните мрежи (КИМ). Защита от паразитни информационни излъчвания. Защита на електрозахранването. Защита от случайни грешки. SHA - Сигурни Хеширащи Алгоритми. Основни принципи, процедури и блокови схеми за реализация. Криптографски ключове и тяхното управление. Политики за обмяна на ключовете. Криптографска защита на телефонните разговори. Методи за засекретяване с преобразуване в честотната и

времевата област. Цифрови методи за шифриране на речевия сигнал. Криптографска защита на информационния обмен в комуникационните мрежи. WLAN сигурност. Видове алгоритми за криптиране. Сигурност и криптиране в GSM. Алгоритми. Основни принципи, процедури и блокови схеми за реализация и др.

13. Библиография(препоръчителна или задължителна литература)

Основна литература:

- 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.
- Stallings W. Cryptography and Network Security: Principles and Practice (6th Edition), Hardcover, pp., 2013.
- Schneier B. Appliet Cryptography Protocols, Algorithms, and Source Code in C, Wiley, pp. 81-221, 2013.
- Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации. КНОРУС. Москва, 2016.
- Фороузан Б. А., Управление ключами шифрования и безопасность сети (2-е изд.), М.: НОУ "Интуит", 2016.

Допълнителна литература:

- Бехроуз А. Ф., Математика криптографии и теория шифрования (2-е изд.), М.: НОУ "Интуит", 2016.
- Stallings W., Brown L., Computer Security: Principles and Practice (3rd Edition), Pearson, July 18, 2014.

14. Методи и критерии на оценяване:

Дисциплината завършва с текуща оценка.

Изисквания при формиране на оценката по шестобалната система

Окончателната оценка по дисциплината се оформя на базата на точкова система като максималния брой точки, който студентите могат да получат е 100. Те се формират от следните дейности:

- *решаване и навременно предаване на задачите за самостоятелна работа – 20 точки;*
- *активно участие в практическите упражнения и защита на протоколи – 20 точки;*
- *пълното писмено развиване на два теоретични въпроси от лекционния материал, по време на текущия контрол – 60 точки.*

Формиране на крайната оценка

Формирането на крайната оценка е на базата на получените през семестъра точки, като съответствието между броя точки и оценката по шестобалната система е дадено в Таблица 1.

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*