ИЛИЩЕ ПО ТЕЛЕКОМУНИКАЦИИ И ПОЩИ

Факултет: ФАКУЛТЕТ ПО ТЕЛЕКОМУНИКАЦИИ И МЕНИДЖМЪНТ
Катедра: ОБЩО ИНЖЕНЕРСТВО
Професионално направление: 5.13. ОБЩО ИНЖЕНЕРСТВО
Специалност: ДИГИТАЛНО ПРЕДПРИЕМАЧЕСТВО И ВИСОКИ ТЕХНОЛОГИИ
Образователно-квалификационна степен: БАКАЛАВЪР

ОПИСАНИЕ НА ЛЕКЦИОНЕН КУРС

1.Наименование на курса: *КИБЕРСИГУРНОСТ НА ВИСОКИТЕ ТЕХНОЛОГИИ*
2.Код на курса: В.45.067.3
3. Вид на курса: *факултативен*
4. Ниво: *бакалавър*
5. Година на изучаване: *четвърта*
6. Семестър: *седми*
7. Брой кредити: *3*
8. Име на лектора: *доц. д-р инж. Иван Динков Иванов*
9. Резултати от обучението за дисциплината:

Целта на курса е да даде на студентите общ поглед и да формира базови знания, необходими за провеждане на задълбоченото изучаване на аспектите на киберсигурността на високите технологии.

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

Основни знания за сигурността и защитата на информацията, нормативно правна база за защита на информацията, организационни мерки и технически системи и средства за защита на информацията, антивирусна защита на данните в компютърните мрежи, базови процедури и класификация на криптографските алгоритми, криптографски алгоритми, технологии за мрежова сигурност и кибератаки.

Практически умения за работа с конфигуриране и работа с F-Secure Client Security Premium, F-Secure Policy Manager, реализиране и изследване на субституционни и транспозиционни криптографаски процедури, DES, AES и RSA криптографаски алгоритъм, реализиране и изследване на тестове за проникване в локална мрежа.

Компетенции: След приключване на курса, студентите трябва да са усвоили основните понятия в областта на киберсигурността.

10. Начин на преподаване:

Лекциите се провеждат чрез запознаване на студентите последователно с предвидения в учебния план материал. Лекциите са илюстрирани с графичен и видео материал, с нагледни примери и задачи, който се представя чрез презентации с мултимедиен проектор.

Практическите упражнения се провеждат в лабораториите на катедрата, оборудвани със съвременни компютри, като всеки студент работи самостоятелно. Преди всяко практическо занятие студентите са информирани за необходимостта от предварителна подготовка по съответната тема.

11. Предварителни изисквания:

Студентите следва да притежават познания по „Основи на информационните технологии“ и „Основи на програмирането“ и др. дисциплини от предходни семестри.

Курсове, ползващи дисциплината са всички дисциплини в оставащите семестри изискващи знания и умения в областта на киберсигурността.

12. Съдържание на курса:

В дисциплината се засягат основните правни, технически и организационни аспекти за защита на информацията в днешния дигитален свят, даващи възможност на студентите да се справят с бъдещи казуси и разработки в областта на киберсигурността.

13. Библиография

Основна литература:

1. **Nancy R. Mead, Carol C. Woody.** Cyber Security Engineering, ISBN-13: 978-0-134-18980-2, 2017.
2. **Пролетарский А.В., Сурово А.М., Смирнова Е.В., Руденков Н.А.** Технологии защиты информации в компьютерных сетях (2-е изд.) 2016.
3. **Dr. Erdal Ozkaya.** Cybersecurity: The Beginner's Guide, Packt Publishing (May 27, 2019).
4. **Charles J. Brooks,** Christopher Grow, Philip Craig, Donald Short. Cybersecurity Essentials 1st Edition, Sybex, 2018.

5. **Zach Codings,** Computer Programming And Cyber Security for Beginners, Independently published (December 4, 2019).

Допълнителна литература:

1. **Brian Walker,** Cyber Security: Comprehensive Beginners Guide to Learn the Basics and Effective Methods of Cyber Security, Independently published (June 20, 2019).
2. **Elijah Lewis,** Ethical Hacking: A Comprehensive Beginner's Guide to Learn About the Effective Strategies of Ethical Hacking, Independently published (January 11, 2020).
3. **Elijah Lewis,** Cybersecurity: A Comprehensive Beginner's Guide to learn the Realms of Cybersecurity from A-Z, Independently published (January 11, 2020).

14. Методи и критерии на оценяване:

Дисциплината завършва с *текуща оценка.* Отчита се индивидуалната и екипна работа на студента по време на упражненията и положените онлайн тестове.

1. Изисквания при формиране на оценката по шестобалната система

30% от крайната оценка се формира от резултатите от текущите електронни тестове, 20% се формира от изпълнението на практическите упражнения и 50% от финалния тест. Текущите тестове и финалният тест са електронни и са публикувани в системата за електронно обучение на ВУТП. Те включват отворени и затворени въпроси. Част от въпросите са свързани с решаване на казуси, с цел проверка на творческото прилагане на придобитите знания.

2. Формиране на крайната оценка

Формирането на оценка в курса на обучение на всеки от посочените етапи, съобразно получени точки и подредбата им 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*