

Факултет: ФАКУЛТЕТ ПО ТЕЛЕКОМУНИКАЦИИ И МЕНИДЖМЪНТ

Катедра: ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

Професионално направление: 5.3. КОМУНИКАЦИОННА И КОМПЮТЪРНА ТЕХНИКА

Специалност: КИБЕРСИГУРНОСТ НА ВИСОКИТЕ ТЕХНОЛОГИИ

Образователно-квалификационна степен: ПРОФЕСИОНАЛЕН БАКАЛАВЪР

ОПИСАНИЕ НА ЛЕКЦИОНЕН КУРС

1. Наименование на курса: *КИБЕР ЗАПЛАХИ И КИБЕР КРИЗИ*

2. Код на курса: P.18.019.1

3. Вид на курса: *задължителен*

4. Ниво: *професионален бакалавър*

5. Година на изучаване: *втора*

6. Семестър: *трети*

7. Брой кредити: 6

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

9. Резултати от обучението за дисциплината:

Целта на курса е да даде на студентите в систематизиран вид основни познания в областта на Киберзаплахите и киберкризите. Студентите, приключили обучението си по дисциплината, трябва да придобият основни знания относно:

- Видовете киберзаплахи;
- Механизми за споделяне на информация при киберинцидент;
- Предотвратяване и справяне с киберкризи;
- Противодействие на киберзаплахи;
- Действия при национален и международен план при киберинцидент.

Практическите умения, които студентите следва да придобият и развият по време на курса са свързани с характеристиките и противодействието на киберзаплахите и управлението на киберкризи.

Компетенции: След приключване на курса студентите, успешно завършили обучението, трябва да са усвоили частично теоретичните и практическите възможности за действия при кибер заплахи и кибер кризи.

10. Начин на преподаване:

Обучението по дисциплината *“Кибер заплахи и кибер кризи”* се извършва през трети семестър съгласно действащия учебен план чрез лекции, групирани по два учебни часа седмично в продължение на 15 седмици и практически упражнения, групирани по два учебни часа седмично в продължение на 15 седмици.

По време на лекциите студентите изграждат теоретичните си знания като участват в семинарните упражнения и самостоятелното изготвяне на план за реакция при киберзаплахи, киберинциденти и киберкриза. Лекциите са илюстрирани с графичен материал, който се представя чрез презентации с мултимедияен проектор и се допълват с примери и задачи. Семинарните упражнения се провеждат в лаборатория на катедрата, оборудвана с компютри.

11. Предварителни изисквания:

Студентите следва да имат предварителни знания по Основи на сигурността и стандарти за информационна сигурност, Мрежи и протоколи и Е-мениджмънт при кризите.

Курсове, ползващи дисциплината са: Защита на информацията при Е-търговия, Защита на безжичните комуникации, Е-мениджмънт при кризи, Политики за киберсигурност, Хакерски атаки и инструменти, Въведение в облачните технологии, Технически системи за сигурност, Наказателно-правни аспекти на киберсигурността, Защита на класифицираната информация, Сигурност на електронните карти за разплащане.

12. Съдържание на курса:

Учебната програма по дисциплината представя технология на киберзаплахите, изследване на кибер инциденти и управление на киберкризи във връзка със спецификата на специалността. В *Раздел първи* на учебната програма са представени основни понятия и се

дефинира проблемна област. Представят се методи за идентифициране на заплахи, определяне на вида и източника на заплахата, правят се анализи на заплахите, разглеждат се актуални проблеми и предизвикателства при кибер тероризма и киберкултурата в информационните мрежи и системи.

Раздел втори разглежда механизми за защита на критична инфраструктура, механизми за защита на SCADA системи, кибер инциденти чрез мобилни устройства и методи за докладване на инциденти.

В *Раздел пети* се разглеждат кризисни етапи и Екипи за реагиране при компютърни инциденти. Обръща се внимание и на регулацията в България за действие при инциденти, закона за киберсикурност и националната стратегия за киберсигурност. Отделя се внимание и на международните дейности при киберкризи и действията на експертния център в областта на кибернетичната сигурност в Европа. Изучават се методи за тестване за уязвимости в компютърните системи и мрежи, изготвяне на препоръки за защита и поддържането и актуализирането на информационни системи.

13. Библиография

ОСНОВНА ЛИТЕРАТУРА

1. The Red Book. A Roadmap for Systems Security Research, SysSec Consortium, September, 2013, <http://www.red-book.eu>.
2. Национална стратегия за киберсигурност.
3. Закон за киберсигурност.
4. Европейския регламент за защита на личните данни.
5. Материали на Агенция на Европейския съюз за мрежова и информационна сигурност (ENISA).

ДОПЪЛНИТЕЛНА ЛИТЕРАТУРА

1. Computer Security Fundamentals (Pearson IT Cybersecurity Curriculum (ITCC) 3rd Edition.
2. Computer Network Security and Cyber Ethics, 4th Edition.
3. Cyber-security of SCADA and Other Industrial Control Systems, Springer International Publishing AG
4. The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities (Wiley Finance).

1.

14. Методи и критерии на оценяване:

Дисциплината завършва с текуща оценка.

Изисквания при формиране на оценката по шестобалната система

Тежест на оценяването: 50% от теста и 50% от писмената разработка.

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)

Формиране на крайната оценка

Въз основа на показани знания от теста и писмената разработка.

Отличен (6) – за добро познаване на информационните източници, задълбочено овладени ключови и допълнителни знания и умения, осмислено и правилно разбиране на материята, умения за решаване на сложни задачи, собствено мислене и аргументиране на решенията.

Мн. добър (5) – за много добре овладени ключови и допълнителни знания, осмислено и правилно разбиране на материята, умения за прилагане на наученото при сложни казуси и задачи.

Добър (4) – за овладени ключови и допълнителни знания за решаване на казуси и задачи, но без да може да ги развие до самостоятелно мислене.

Среден (3) – за усвоени ключови знания и решения на типови задачи.

Тестовите по дисциплината се състоят от 75 затворени въпроса, като въпросите имат пет възможни отговора, от които само един е верен.

15. Език на преподаване: *български*