Код: 1-д „Информационно осигуряване и сигурност”

ECTS кредити: 7/5	Седмичен хорариум: 2+0+2
Форма за оценяване: Изпит/Текуща оценка	Форма на контрол: Изпит - тест / Текуща оценка - тестове

Водещо звено:

Катедра: *КОМПЮТЪРНИ НАУКИ И ТЕХНОЛОГИИ*
ФАКУЛТЕТ ПО ИЗЧИСЛИТЕЛНА ТЕХНИКА И АВТОМАТИЗАЦИЯ

Лектор: доц. д-р инж. Х.Вълчанов, доц.д-р инж. В.Алексиева

Катедра: *КОМПЮТЪРНИ НАУКИ И ТЕХНОЛОГИИ*

тел. 052 383 278, 439

e-mail: hristo@tu-varna.bg, valeksieva@tu-varna.bg

Анотация:

Основната цел на дисциплината е да осигури на студентите знания и умения в областта на технологиите и средствата за прилагане на техники за сигурност и защита на информационните системи. Разглеждат се въпроси, свързани с осигуряването на конфиденциалност, цялостност и наличност на информацията. Обръща се внимание на принципите на компютърната и мрежова сигурност, оценка на риска, концепциите на довереност. Анализират се съвременни мрежови модели и решения от позиция на мрежова и информационна сигурност за постигане на оптимално съотношение на модулност, устойчивост, гъвкавост, сигурност и лесно управление. Разглеждат се видове атаки и злонамерен код срещу информационната сигурност, както и техники и средства за тяхното блокиране- системи за разпознаване и предпазване от атаки. Представени са техники за защита на бази данни и Web приложения.

Основни раздели на съдържанието:

- Концепции за риск, заплахи, уязвимости и атаки. Международни стандарти за сигурност.
- Автентикация, оторизация и акаунтинг (AAA). Контрол на достъпа.
- Принципи на сигурността при проектирането. Модел на най-малките привилегии и изолация.
- Сигурност от тип край-до-край. Защита в дълбочина. Валидиране на данните.
- Създаване на сигурен код.
- Заплахи и атаки срещу сигурността. Зловреден софтуер (malware, spyware, botnets, rootkits).
- Модел на Web сигурност. Сигурност на браузъри.
- Управление на сесии и автентикация. Протокол HHTPS. XSS. CSRF.
- Сигурност от страната на клиента. Сигурност на cookies. Сигурност при plug-in.
- Уязвимости на приложенията с бази данни. SQL инжектиране.
- Сигурност от страна на сървъра. Web Application Firewall.
- Организация на архиви. Модели. Принципи.
- Мрежови атаки. Типове атаки - Denial of Service (DoS), Distributed DoS, „Социален инженеринг” и Phishing.
- Архитектури на сигурни мрежи. Сигурност при комуникационни канали и маршрутизиращи протоколи. Secure DNS. Изолация.
- Сигурност при облачни инфраструктури.

Форма на изнасяне на учебното съдържание:
Лекции- включват общо 15 теми.
Лабораторни упражнения – провеждат се в специализирана компютърна лаборатория, като се дава възможност на студентите да приложат на практика получените знания. Провеждат се контролни работи по учебния материал.