УЧЕБНА ПРОГРАМА

Код: **91-858-23** Дисциплина: **Методика на експертиза на мрежова сигурност**

Ниво: 7. Магистър ECTS кредити: **1.5**

Обучаващо звено: Катедра „Сигурност и безопасност“

Анотация на учебната дисциплина

В курса "Методика на експертиза на мрежова сигурност" се включват познания от областта на общата информатика, компютърните мрежи и комуникации и криптографията. Курсът разглежда хардуерните и софтуерните компоненти на компютърните мрежи, архитектури и протоколи, но акцент се поставя на ключовите концепции за центровете за данни и на различните инфраструктури - паралелно съществуващи мрежи Ethernet, Fibre Channel (SAN) и изчислителните клъстери InfiniBand. Курсът разглежда конвергенцията на локалните мрежи и SAN чрез използване на технологии като FCoE и Data Centre Bridging (DCB) и решения от екосистемата FCoE (комутатори, адаптери, дискови масиви и т.н.). Отделя се внимание на защитата и проблемите на мрежите и стандартните начини за подход и разрешаване на тези проблеми.

Компетентности като очаквани резултати от обучението

Знания: Курсът по “ Методика на експертиза на мрежова сигурност т” осигурява знания в актуалните проблеми на мрежовата сигурност. Курсът предоставя специализирани знания за пълна виртуализация на инфраструктурата и единно управление на мрежата, сървърите, системите за съхранение, платформите за услуги и виртуалните ресурси.

Умения: Курсът изгражда умения за изграждане на програмно реализирана изчислителна инфраструктура, прилагаща концепциите за софтуерно дефинирани мрежи SDN и софтуерно дефинирани системи за съхранение (SDS) Студентите ще придобият умения по конструиране и администриране на компютърни мрежи. Обучаваните ще могат да свързват и да адресират устройствата в една мрежа, да предотвратяват колизии и да осигуряват надеждна защита в мрежата, независимо от нейния мащаб. Ще могат да прилагат съвременни технологии за защита и контрол на трафика в мрежата.

Отношения и нагласи: Интересът към програмно конфигурируемите центрове за данни определено е налице заради стремежа на организациите към създаване на инфраструктура, която е принципно по-гъвкава, по-мащабируема и по-икономична. Усвояването на дисциплината е необходима предпоставка за професионална и личностна реализация на индивида през настоящия век. Всяка компания в голяма степен дължи своя успех на стратегическото използване на мрежите и нагласата към важността на тяхното приложение е очевиден факт в епохата на дигиталната трансформация. Успехът на бизнеса е невъзможен без мрежова сигурност.

Методи за обучение и връзки с други дисциплини

Методи на обучение: Методите за обучение по дисциплината се базират на запознаване на студентите с теоретичен материал и същевременно незабавното му практическо прилагане, за да може те да упражняват и прилагат предлаганите им технологични инструменти и знания, които да превръщат в лични умения за работа като бъдещи експерти по киберсигурност.

Лекции (2 часа на седмица, 7 седмици). Лекциите са от съществена важност за разбиране на основите на компютърните заплахи и начините за справяне с тях. Учебната зала за лекционните занятия да бъде оборудвана с мултимедиен проектор и интернет достъп. За всяко лекционно занятие е разработена Powerpoint презентация, в която има множество примери, за да могат студентите да усвоят по-лесно и трайно теоретичния материал и да го превърнат в практическо умение. Презентацията е достъпна за студентите чрез Google Classroom.

Предварителни изисквания: Предварителни знания и умения по дигитална компетентност.

Осигурявани дисциплини: Дисциплината дава базови познания, необходими за следните дисциплини от учебния план на специалност ИКН: ИТ инфраструктура, Електронен бизнес, Разпределени и облачни изчисления

Проверка на знанията и уменията

Крайно оценяване: Изпит

Методи и форми на оценяване: Защита на курсов проект. Проектът е представяне на възникнал проблем и методи за справяне.

Критерии за оценяване: Критерии за оценяване на проекта:
Функционална и логическа завършеност
Сложност на проблема/атаката
Адекватно решение

Компоненти и тяхната тежест в крайната оценка: Функционална и логическа завършеност (пълнота): - 20 точки
Сложност на проблема/атаката - 20 точки
Адекватно решение - 20 точки
от 60 до 51 точки - Отличен (6) A
от 50 до 41 точки - Мн. добър (5) B
от 40 до 36 точки - Добър (4) C
от 35 до 30 точки - Добър (4) D
от 29 до 21 точки - Среден (3) E
от 20 до 16 точки - Слаб (2) FX
под 16 точки - слаб (2) F

Учебни материали и ресурси за самоподготовка

Основна литература:

1. Larae Jorel, 5G CORE NETWORK 2023: A Complete Introduction, Fundamentals and Applications to 5G Wireless Networks, Kindle Edition, 2023

2. B. A. Ayomaya, Data Center for Beginners: A beginner's guide towards understanding Data Center Design, 2023, Kindle Edition

2. Kurose, J., K. Ross. Computer Networking: A Top-Down Approach. Pearson, 8th Edition, 2023

3. Dordal P. Introduction to Computer Networks, Release 3.0.1, 2023

http://intronetworks.cs.luc.edu/current/ComputerNetworks.pdf

4. Sean, Michael Kerner, How Use of Chaos Engineering is Improving System Reliability, Feb 2023

https://www.datacenterknowledge.com/devops/how-use-chaos-engineering-improving-system-reliability

5. Уолъс К. CCNP Routing and Switching Route 300-101: Официално ръководство за сертифициране - том 1, Алекс Софт, 2022

6. D.K. Academy. Компютърни мрежи - наръчник на системния администратор , изд. Асеневци,2018

Допълнителна литература:

1. 10 Best Computer Networking Books for Beginners & Experts

https://www.networkstraining.com/best-computer-networks-textbooks/

1. Hoffman H. Ethical Hacking Bible: Cybersecurity, Cryptography, Network Security, Wireless Technology and Wireless Hacking with Kali Linux | 7 books in 1: 10, Kindle edition, 2023

2. Nastase R. Computer Networking: Your Guide in Computer Networking and Routing Protocols for Passing the CCNA Paperback,Independently published, 2023

Речник (ключови думи)

ИТ инфраструктура, IT infrastructure, компютърни мрежи, computer networks, OSI, TCP/IP, SMTP, POP, FTP, мрежови протоколи, колизия, WI-FI, networking, ping, tracert, IPv4, IPv6, Cisco, data centers, InfiniBand, SAN, FCoE, DCB, Redfish, GitHub и др.

Съдържание на учебната дисциплина по тематични единици за редовна / задочна форма на обучение

№	Тема	Основни въпроси	Лекции	Сем. упр.	Пр. зан.	Изв. аудит.	Осигуряване
1.	Компютърни мрежи. Еталонни модели. Мрежови протоколи.	Въведение. Основни компоненти. Видове сървъри (File, Application, Mail, DB), (Mainframe, RAID, Cluster, Virtual). Клиенти. OSI модел. Модел TCP/IP. Сравняване на TCP/IP и OSI. IPv4. IPv6	2			48	мултимедиен проектор интернет
2.	LAN, Backbone, MAN, WAN. Локални мрежи. Ethernet мрежи. Безжични локални мрежи.	Елементи в локалната мрежа (AP, switches, routers). Типове локални мрежи. Wireless стандарти. Сигурност. Конфигуриране на пароли за достъп до маршрутизатор и комутатор. Конфигуриране на RIP v1. Конфигуриране на RIP v2.	2			46	мултимедиен проектор интернет
3.	Виртуализация. Облачни технологии. Cloud computing.	Виртуализация и интеграция на ресурси.Видове облаци. Защита.	2			4	мултимедиен проектор интернет
4.	Центровете за данни. Ethernet, Fibre Channel (SAN) и изчислителните клъстери InfiniBand.	Конвергенцията на локалните мрежи и SAN чрез използване на технологии като FCoE и Data Centre Bridging (DCB) и решения от екосистемата FcoE	2			4	мултимедиен проектор интернет
5.	Заплахи в мрежова среда.	Излагане на информация пред неоторизиран достъп; изтичане на информация; загуба на информация; уязвимост към кибератаки; разкриване на поверителна информация; Insider атака.	4			8	мултимедиен проектор интернет
6.	Мрежова защита.	Managed switch с филтри; статична ARP таблица; команди – ping –r; traceroute; DNSSEC (криптографска защита).	3			6	мултимедиен проектор интернет
	Общо часове		15			30	

Разработил програмата: проф. д-р Теодора Иванова Бакърджиева

Учебната програма е приета от Съвета на катедра Обществен ред и сигурност с протокол № 7/28.03.2024 г.
Учебната програма е утвърдена от Факултетния съвет на Юридически факултет с протокол № 9 /04.04.2024 г. и заповед № 76/05.4.2024 г. на декана на факултета.