УЧЕБНА ПРОГРАМА

Код: **91-787-23** Дисциплина: **Методика на експертиза за неправомерен достъп в корпоративни информационни системи**

Ниво: 7. Магистър ECTS кредити: **7.5**

Обучаващо звено: Катедра „Обществен ред и сигурност“

Анотация на учебната дисциплина

В курса "Методика на експертиза за неправомерен достъп в корпоративни информационни системи“ се включват познания от областта на общата информатика, компютърните мрежи и комуникации и криптографията. Курсът разглежда рисковете и предизвикателствата за сигурността на кибер системите, критериите за оценка на сигурността и видовете заплахи. Отделя се внимание на кибершпионажа и уеб-базираните атаки, както и на стандартните начини за подход и разрешаване на тези проблеми, като се включват реални примери. Място в учебната дисциплина намира и биометричната сигурност.Компетентности като очаквани резултати от обучението

Компетентности като очаквани резултати от обучението

Знания: Курсът по “Методика на експертиза за неправомерен достъп в корпоративни информационни системи” осигурява знания в актуалните проблеми на компютърната сигурност, както и практически умения за тяхното решаване. Студентите ще придобият специализирани знания за работа със системи за откриване на проникване (IDPS), за справяне с атаки на уеб приложения, фишинг, DoS атаки, SQL Injection, man in the middle, DNS spoofing и спам. Обучаваните ще получат знания за методите за защита на компютърните мрежии адекватно противодействие при атаки.

Умения: Курсът усъвършенства необходимите навици и умения в отговор на повишените изисквания към киберсигурността и средствата за киберзащита. След завършването на курса студентите ще могат успешно да разрешават проблеми в областта на киберсигурността. Чрез различни активни форми на обучение (практически занятия, защита на курсови проекти и дискусии) у обучаемите се формират умения за разбиране на проблемите в сферата на компютърната сигурност. В резултат студентите ще придобият умения и компетентности за справяне с увеличаващия се брой компютърни атаки. Обучаваните ще могат да прилагат съвременни технологии за защита и контрол.

Отношения и нагласи: Приемането на стратегия за дигитална трансформация може да донесе големи ползи за организациите - от повече гъвкавост за служителите до намаляване на разходите и подобряване на ефективността. За да се постигнат тези предимства обаче, трябва да се включва фокус върху киберсигурността. Усвояването на дисциплината е необходима предпоставка за професионална и личностна реализация на индивида през настоящия век. Всяка компания в най-голяма степен дължи своя успех на надеждното и сигурно използване на компютърните технологии и нагласата към важността на тяхното приложение е очевиден факт в епохата на дигиталната трансформация. Постигането и поддържането на ефективна киберсигурност в този нов базиран на облака свят е задача на цялото общество.

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 кибер сигурност. . 1. Лекции (2 часа на седмица, 15 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. 2. Практически занятия (3 часа на седмица, 15 седмици). Практическите занятия са от основно значение за трайно усвояване на умения и практики за идентифициране на видовете атаки и методите за противодействие. По всяка тема от лекционния материал има специално подготвено практическо задание, което студентите изпълняват по време на практическите задания в компютърна зала под тюторството и насоките на преподавателя, който им помага да се справят с възникнали в процеса на работа трудности, неясноти или допуснати грешки.
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. МЕТОДИКА ЗА ИЗГРАЖДАНЕ И ОЦЕНКА НА СРЕДСТВАТА И СИСТЕМИТЕ ЗА ФИЗИЧЕСКА СИГУРНОСТ НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ https://www.dksi.bg/media/1526/metodikapofizi4eskasigurnost2015edited2017.pdf
2. Иван Гайдарски, Метод и модели за разработка на системи за информационна сигурност в организации, 2022, Изд. БАН, https://www.iict.bas.bg/konkursi/2022/IGaidarski/disertatsia.pdf
3. Hamid Jahankhani, Stefan Kendzierskyj, Nishan Chelvachandran, Jaime Ibarra, (2023), Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity, Springer Nature, 450 pages
4. Markus Christen, Bert Gordijn, Michele Loi, (2023), The Ethics of Cybersecurity, Springer Nature, 384 pages
5. David J.P.Fisher, Networking in the 21st century, RockStar Publishing (June 6, 2023), 194 pages, ISBN-13: 978-1944730192, ISBN-10: 1944730192
6. An Ultimate Guide to Cyber Security for Beginners

https://www.simplilearn.com/tutorials/cyber-security-tutorial/cyber-security-for-beginners

5. CCNP Routing and Switching Route 300-101: Официално ръководство за сертифициране - том 1, изд. Алекс Софт, 2022, 696 стр.
6. Трой Макмилан, CCNA Security учебно ръководство, , изд. Алекс Софт, 2022, 528 стр.
7. Cisco CyberOps Associate, Cisco Press, 2023, ISBN: 9780136807834

Допълнителна литература:

1. 10 Fundamental Cybersecurity Lessons for Beginners

https://blog.barkly.com/10-fundamental-cybersecurity-lessons-for-beginners

2. Ethical hacking, 2023

https://www.tutorialspoint.com/ethical_hacking/

3. The Best Internet Security for 2023

https://www.techradar.com/news/best-internet-security-suites

Речник (ключови думи)

ИТ сигурност, криптиране, шифриране, Cyber Security, Phishing, Ransomware, Biometrics 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.	Рискове и предизвикателства за сигурността на кибер системите. Критерии за оценка на сигурността. ARP Poisoning . DNS Spoofing.	Мрежови скенери, скенери за слаби страни, разбивачи на пароли, мрежови анализатори (sniffers), подмяна на обекти, модификация на данни или информация. Възможност за промяна на чужд мрежов трафик (MITM man in the middle). Атака върху network и application слоеве от OSI модела. TCP Kill – прекратяване на TCP връзка. SYN Flood - блокиране на услуга	4			12	мултимедиен проектор интернет
2.	Неоторизиран достъп чрез пароли и вредни програми.	Spyware, Adware, Malware, Trojan, Rootkit, Backdoor, Key loggers, Phishing, Browser Hijack, Dialers .	2		2	14	мултимедиен проектор интернет
3.	Малуер.	Атаки срещу електронна поща - входни и изходни кутии. Спам. Уеб-базирани атаки Атаки на уеб приложения. Фишинг. DoS атаки SQL Injection, man in the middle и DNS spoofing	2		2	14	мултимедиен проектор интернет
4.	Сигурност и IoT. Системи за откриване на проникване (IDPS).	Заплахи и препоръки за защита на IoT системи. Класификация на системите IDS. Методи за откриване, използвани от IDS. Сравнение на IDS със защитни стени. Предимства и недостатъци на IDPS	2		2	14	мултимедиен проектор интернет
5.	Заплахи в Cloud Computing.	Излагане на информация пред неоторизиран достъп; изтичане на информация; загуба на информация; уязвимост към кибератаки; разкриване на поверителна информация; Insider атака.	4		4	12	мултимедиен проектор интернет
6.	Контрол и регламентиране на достъпа до данните.	Защита от разрушаване: антивирусна защита, контрол за автентичност на данните и програмите, защита от хардуерни и софтуерни грешки, защита от грешки на персонала Криптографска защита на данните.	4		4	12	мултимедиен проектор интернет
7.	Архивиране на данни (Backup).	Пълно резервно копие на твърдия диск. Частично резервно копиране, само на избрани директории (папки). Инкрементно - резервно копиране на файлове, които са били изменени след последното резервно копиране.	2		2	12	мултимедиен проектор интернет

	Защита на паролите.	Честа смяна на паролите. Ограничаване броя за въвеждане на паролите. Минимална дължина на паролите. Log out на потребителите. Система с две или повече пароли.					
8.	Мрежова защита.	Managed switch с филтри; статична ARP таблица; команди – ping –r; traceroute; DNSSEC (криптографска защита).	2		4	10	мултимедиен проектор интернет
9.	Защита при облачни технологии.	Силна автентификация; DDoS атаки; Криптиране на данни; DNS (DNSSEC).	2		5	10	мултимедиен проектор интернет
10.	Крипто вируси.	Ransom. RoT: Ransomware of Things. Jackware. Jackware и IoT. Защита.	2		4	10	мултимедиен проектор интернет
11.	Критична инфраструктура.	SCADA системи. Сигурност при SCADA системите. Уязвимост на HMI. Zero day експлойти. PLC уязвимости. Социално инженерство. Препоръки за защита на SCADA системи.	2		5	14	мултимедиен проектор интернет
12.	Биометрия. Биометрична сигурност.	Биометрични системи. Биометрични модалности. Проекти – Soli, CIR, Auth0, EarEcho и др.	2		7	14	мултимедиен проектор интернет
	Общо часове		30		45	150	

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.