

Факултет: ФАКУЛТЕТ ПО ТЕЛЕКОМУНИКАЦИИ И МЕНИДЖМЪНТ

Катедра: ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

Професионално направление: 5.3.КОМУНИКАЦИОННА И КОМПЮТЪРНА ТЕХНИКА

Специалност: КОМПЮТЪРНО АДМИНИСТРИРАНЕ НА СОФТУЕРНИ ПРИЛОЖЕНИЯ

Образователно-квалификационна степен: ПРОФЕСИОНАЛЕН БАКАЛАВЪР

ОПИСАНИЕ НА ЛЕКЦИОНЕН КУРС

1. Наименование на курса: ЗАЩИТНИ СТЕНИ

2. Код на курса: P.16.035.1

3. Вид на курса: задължителен

4. Ниво: професионален бакалавър

5. Година на изучаване: трета

6. Семестър: пети

7. Брой кредити: 4,5

8. Име на лектора: доц. д-р инж. Ирина Топалова

9. Резултати от обучението за дисциплината: Студентите да се запознаят с теоретичните и практическите аспекти на съвременни видове заплахи за сигурността на мрежата, със съвременните методи и технически средства за смекчаване на заплахите, видовете защитни стени и тяхното практическо приложение. В курса се разглеждат въпроси, свързани с идеологията и проектирането на защитни стени при имплементирането им в мрежовата структура. Студентите, приключили обучението си по дисциплината, трябва да придобият:

Основни знания за видовете технически средства за откриване на атаки, видовете защитни стени и техните функционални възможности.

Практически умения за прилагане на усвоените функционалности на съвременни технически средства за откриване и предотвратяване на атаки в реални системи за защита, както и за имплементиране на защитни стени в комуникационните системи.

Компетенции: След успешно приключване на курса *студентите трябва да могат:*

- да познават съвременните методи и инструменти за смекчаване на заплахите, както и на инструментите за одит на сигурността на мрежата;

- да използват локални и сървър базирани автоматизирани функции за сигурност в мрежови устройства;

- да познават видовете и технологиите на защитни стени;

- да проектират, конфигурират и тестват видовете VPN тунели ;

- да конфигурират технически средства за адаптивна защита на мрежи – ASA – (Adaptive Security Appliance) и Hillstone.

- да работят със софтуер за менажиране на защитни стени (Device Manager), ASA Security Device Manager (ASDM);

10. Начин на преподаване: Лекциите се провеждат по класическия начин като студентите се запознават последователно с предвидения материал. Твърденията се илюстрират с примери, които максимално улесняват работата на студентите в упражненията. Лекциите са богато илюстрирани с графичен материал, който се представя чрез презентации с мултимедиен проектор и допълнения с примери. Практическите упражнения се провеждат в компютърните лаборатории на катедрата, оборудвани с необходимите мрежови устройства и софтуерни пакети за симулация.

11. Предварителни изисквания: Познания по „Мрежи и протоколи 1” и „Мрежи и протоколи 2”, „Балансиране на мрежово натоварване“, включени в учебния план на специалността.

12. Съдържание на курса: Придобиване на познания за функционалните особености на съвременните технически средства за откриване на атаки, за технологиите в защитните стени и за подходящото им интегриране в мрежовата структура на комуникационни системи, с цел осигуряване на надеждна защита. В практически аспект, курсът включва основните елементи и конкретните реализации на различни технически средства за откриване на атаки и за проектиране на защитни стени в съвременните комуникационни мрежи.

13. Библиография

Основна литература:

1. Omar Santos, Jazib Frahim, Cisco ASA Security Contexts, 2015, Cisco Press.
2. Cisco IOS XR Fundamentals by Dawit Birhanu, Mark Ghattas, Syed Natif Nawaz, Mobeen Tahir, Chapter 5. Cisco IOS XR Monitoring and Operations, 2017.
3. Joseph Muniz, Nadhem AlFardan, Gary McIntyre, Overview of Security Operations Center Technologies, 2015, Cisco Press.
4. Sean Wilkins, Cisco ASA Access Lists Concepts and Configuration, 2013, Cisco Press.
5. Hillstone E-2000 Series Next-Generation Firewall, User Manuel, www.hillstonenet.com, 2018.

Допълнителна литература:

1. Monitoring and Troubleshooting With Cisco Prime LAN Management Solution 4.1, Copyright © 2011 Cisco Systems, Inc. All rights reserved.
2. <https://www.capterra.com/network-monitoring-software/>, 2018.
3. <http://sectools.org/sploits.html>, 2018.
4. Rowayda, A. Sadeq; M Sami, Soliman; Hagar, S Elsayed, Effective anomaly intrusion detection system based on neural network with indicator variable and rough set reduction. International Journal of Computer Science Issues, 2014.
5. Keerthi Latha, Learn About Intrusion Detection and Prevention, © 2016 by Juniper Networks, Inc. All rights reserved, 2016.

14. Методи и критерии на оценяване: Формирането на крайната оценката е на базата на получените през семестъра точки, като съответствието между броя точки и оценката по шестобалната система е представено в Таблица 1. На обявената дата за дооформяне на крайната оценка студентите развиват писмено един или два въпроса от конспекта по дисциплината и решават зададен казус в практическа задача.

Таблица 1.

Брой точки	Оценка по шестобалната система
0 – 10	Слаб 2 (F)
11 – 20	Слаб 2 2 (FX)
21 – 26	Среден 3.00 (E)
27 – 31	Среден 3.00 (D)
32 – 40	Добър 4.00 (C)
41 – 48	Мн. добър 5.00 (B)
над 49 точки	Отличен 6.00 (A)

15. Език на преподаване: български