Факултет: ФАКУЛТЕТ ПО ТЕЛЕКОМУНИКАЦИИ И МЕНИДЖМЪНТ
Катедра: ОБЩО ИНЖЕНЕРСТВО
Професионално направление: 5.13. ОБЩО ИНЖЕНЕРСТВО
Специалност: ДИГИТАЛНО ПРЕДПРИЕМАЧЕСТВО И ВИСОКИ ТЕХНОЛОГИИ
Образователно-квалификационна степен: БАКАЛАВЪР

ОПИСАНИЕ НА ЛЕКЦИОНЕН КУРС

1. Наименование на курса: *СИСТЕМИ ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ*
2. Код на курса: *B.45.124.1*
3. Вид на курса: *задължителен*
4. Ниво: *бакалавър*
5. Година на изучаване: *четвърта*
6. Семестър: *осми*
7. Брой кредити: 3
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 теоретични и практически знания за стандартите и структурата на система за управление на информационната сигурност, зони на сигурност и видове защитни стени, листи за достъп и управление на политиките на защитните стени, основни мониторинг инструменти, защита на достъпа на защитните стени в мрежата, както и следваща генерация защитни стени (Next Generation FWs) и др.

Студентите, приключили обучението си по дисциплината, трябва да придобият:

Основни знания за видовете атаки и тяхното предотвратяване, видовете защитни стени, тяхната работа, администриране и възможност за мониторинг на мрежата видовете прокси, моделите за реализация, IPS/IDS и др.

Практически умения за работа и администриране на защитни стени, системите за предотвратяване на атаки и прокси, и най-добри практики за откриване и отстраняване на проблеми свързани със сигурността в мрежата и др.

Компетенции: След приключване на курса студентите, трябва да са усвоили:

- трябва да притежават умения за базови конфигурации на защитни стени;
- прилагане на най-добри практики за отстраняване на проблеми свързани със сигурността в мрежата.
- трябва да притежават умения за конфигуриране на IPS/IDS и прокси;
- прилагане на най-добри практики за предотвратяване и отстраняване на атаки.

10. Начин на преподаване:

Методът на преподаване е „учене на база опит", като материалът се поднася в семинарна форма, под формата на делови игри и казуси. Използването на групов динамичен процес позволява студентите да усвоят основните понятия, свързани с дисциплината и да формира и конкретни умения.

Обучението е индивидуализирано, а обучаемият се приема за активен самоорганизращ се индивид. Активното учене се постига чрез действие (правене), интеракция, мултимедийни, виртуални и интерактивни платформи, посредством които студентите самостоятелното достигат до знанията и ги прилагат в конкретни практико-приложни казуси.

11. Предварителни изисквания:

Студентите следва да имат задълбочени познания по следните дисциплини: Киберсигурност на високите технологии, Информационна и технологична сигурност при противодействие на фалшиви новини, Мрежови технологии.

Курсове, ползващи дисциплината са Дипломни работи

12. Съдържание на курса:

В дисциплината се разглеждат актуални теми, свързани със стандартите и структурата на система за управление на информационната сигурност, зони на сигурност и видове защитни стени, листи за достъп и управление на политиките на защитните стени, основни мониторинг инструменти, защита на достъпа на защитните стени в мрежата, както и следваща генерация защитни стени

Цялото обучение е структурирано под формата на теоретичен материал, казуси, ролеви и ситуационни игри и тестови задачи.

13. Библиография

Основна литература:

1. Система за управление на информационната сигурност ISO 27001.

2. David Kim, Michael G. Solomon, Fundamentals of Information Systems Security, ISBN-13: 978-1284220735, Jones & Bartlett Learning; 4th edition (December 24, 2021).

3. Jason Andress, Foundations of Information Security: A Straightforward Introduction, ISBN-13: 978-1718500044, No Starch Press (October 7, 2019).

4. Douglas J. Landoll, Information Security Policies, Procedures, and Standards, ISBN-13: 978-0367669966, Auerbach Publications; 1st edition (September 30, 2020).

5. Mark Dye, Rick McDonald, Antoon Rufi, Network Fundamentals: CCNA Exploration Companion Guide, Published Dec 30, 2011 by Cisco Press, ISBN-10: 1-58713-348-2, ISBN-13: 978-1-58713-348-0, 560 p.

6. Dye M., McDonald R., Rufi A., Network Fundamentals CCNA Exploration Companion.

Допълнителна литература:

1. David Kim, Michael G. Solomon, Fundamentals of Information Systems Security, ISBN-13: 978-1284116458, Jones & Bartlett Learning; 3rd edition (October 26, 2016).

2. Richard Bejtlich, The Practice of Network Security Monitoring: Understanding Incident Detection and Response, No Starch Press; 1st edition (July 15, 2013), ISBN-13: 978-1593275099.

3. Charlie Kaufman, Radia Perlman, Network Security: Private Communications in a Public World (Prentice Hall Series in Computer Networking and Distributed Systems), Addison-Wesley Professional; 3rd edition (September 25, 2022), ISBN-13 : 978-0136643609.

4. J. Michael Stewart, Network Security, Firewalls and Vpns Bundle. (Jones & Bartlett Learning Information Systems Security & Assurance), Jones & Bartlett Learning; 2nd edition (August 10, 2017), ISBN-13 : 978-1284159684.

5. J. Michael Stewart and Denise Kinsey, Network Security, Firewalls, and VPNs (Issa), Jones & Bartlett Learning; 3rd edition (October 29, 2020), ISBN-13: 978-1284183658.

14. Методи и критерии на оценяване:

Дисциплината завършва с *изпит.* Постигането на поставената цел на обучението се контролира през семестъра чрез текущ контрол под формата на индивидуални и екипни задания, тест по време на лекционните занятия. Оценката се формира чрез точкова скала, като се взема предвид участието в практическите занятия, и индивидуалната работа на студента през семестъра.

1. Изисквания при формиране на оценката по шестобалната система

Една част от оценка по дисциплината се оформя на базата на точкова система като максималният брой точки, който студентите могат да получат е 100 (таблица 1).

Окончателната оценка се формира от теоретичен тест по време на изпитната сесия и резултати от изпълнените в хода на груповия динамичен процес казуси и делови игри, като под внимание се взема и активността на студентите по време на самия обучителен процес през семестъра.

Тежест на оценяването:

- ✓ Оценяване в процеса на обучение – самостоятелна работа, проучвания, казуси и делови игри, групов динамичен процес – носи 50% тежест в крайната оценка;
- ✓ Теоретичен изпитен онлайн тест от 20 въпроса с продължителност 40 минути – носи 50% тежест в крайната оценка. Оценяването на теста е съобразно следните критерии: до 50% верни отговори – Слаб 2; до 70% верни отговори – Среден 3; до 80% верни отговори – Добър 4; до 90% верни отговори – Много добър 5 и над 91% - Отличен 6).

2. Формиране на крайната оценка

Формирането на крайната оценка (КО) е на базата на получените резултати от изпитния тест в хода на обучението и груповия динамичен процес (ТК) и резултата от теоретичния тест (ТТ), като съответствието между броя точки и оценката по шестобалната система е дадено в *Таблица 1*.

$$КО = 0,5\ ТТ + 0,5\ ТК$$

Усвоените знания от студентите, изразени в проценти, се оценяват по шестобалната система, както следва:

До 50%	Слаб (2)
51% – 70%	Среден (3)
71% – 80%	Добър (4)
81% – 90%	Мн. добър (5)
Над 90%	Отличен (6)

15. Език на преподаване: *Български/Английски*