ЦЕНТЪР ПО ИКОНОМИЧЕСКИ И УПРАВЛЕНСКИ НАУКИ

# УЧЕБНА ПРОГРАМА

Утвърждавам:
Декан:

CS536

# ИНФОРМАЦИОННА СИГУРНОСТ В ИНТЕРНЕТ

Приета: Протокол № 17 от 29.09.2021 г.

Лектор: доц. д-р Веселина Жечева

## АНОТАЦИЯ

Дисциплината има за цел да систематизира и обобщи знанията на студентите относно информационната сигурност в Интернет среда. Разглеждат се основните видове заплахи и уязвимости от страна на сървъра и клиента, както и съответните защити. Дисциплината завършва със защита на курсова работа и изпит.

## ОСНОВНИ ЦЕЛИ

Основна цел на дисциплината е да формира знания и умения у студентите за анализ и оценка на проблемите, свързани с информационната сигурност в Интернет.

След обучението си по информационна сигурност в Интернет, студентът ще:

- познава основните проблеми, свързани със сигурността в Интернет;
- анализира текущите заплахите и уязвимостите в системите, работещи в Интернет среда;
- избира подходящи средства за защита на компютри и мрежи, свързани с Интернет.

## ПРЕДПОСТАВКИ

Дисциплината е заключителна в областта на информационните технологии и изисква предварителна подготовка на студентите по дисциплината Информационна сигурност, Програмиране, Операционни системи, Компютърни мрежи и комуникации.

## СТАТУТ И СТРУКТУРА

| специалност | статут | Кредити | задочно обучение | | | | дистанционно обучение | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | л | с | У | общ | Л | с | У | Общ |
| Съдебни икономически експертизи | | 6 | 30 | | | 30 | | | | |
| | | | | | | | | | | |

## СЪДЪРЖАНИЕ НА КУРСА

Тема 1. Заплахи и уязвимости. Случайни и злонамерени заплахи. Злонамерен софтуер. Социално инженерство. Атаки и методи за превенция. Аспекти на сигурността на информацията.

Тема 2. Планиране на политиката за сигурност. Видове политики за сигурност. Специфични правила. Реакции при нарушаване.

Тема 3. Криптография и защита на данните в Интернет среда. Сертификати и ключове. Цифрови подписи. Инфраструктура (Public Key Infrastructure). Сигурност на транзакциите. Протоколи.

Тема 4. Уязвимости от страна на клиента (Web браузъра). Бисквитки - същност и рискове, свързани с тях. Web маяци (Web beacons). Зарибяване (phishing). Шпионски софтуер (spyware). Реклами (adware). Вируси. Червеи. Заплахи, свързани с изнудвания.

Тема 5. Сигурност на Web сървъра. Защитни стени. Демилитаризирана зона (DMZ) и бастион хост. Атаки, предизвикващи отказ на услуга. DNS измами.

Тема 6. Системи за откриване на нарушения. Типове системи за откриване на пробивите. Мрежово-базирани системи. Хост-базирани системи. Хибридни системи. Основни компоненти и методи на действие.

Тема 7. Kerberos ключове. Запознаване с Kerberos. Протоколът на Kerberos. Базата данни на Kerberos. Защита при Интернет търговия и разплащания. Основни въпроси. Цифров кеш. Кредитни карти.

## СЕМИНАРНИ УПРАЖНЕНИЯ

Тема 1. Заплахи и уязвимости. Вируси. Шпионски софтуер и реклами. Методи на защита.

Тема 2. Защитни стени. Екраниращи рутери. Демилитаризирана зона. Бастион хост. Отделена подмрежа. Прокси. Избор на решения.

Тема 3. Публичен ключ. Жизнен цикъл - генериране, прилагане, криптиране, предаване, проверка, декриптиране. Процеси. Протоколи.

Тема 4. Системи за откриване на нарушения. Honeypots. Видове. Оценка. Използване. Следене на процесите в системата.

Тема 5. Възстановяване и резервно копиране. Процедури за резервно копиране и възстановяване. Тестване. Документиране.

## КУРСОВА ЗАДАЧА

Курсовата задача се задава на всеки студент и съдържа задачи по анализ и оценка на текущите заплахи и защити за избрана от студента и консултирана от преподавателя тема. Всеки студент защитава курсовата си задача и получава оценка, характеризираща нивото на усвояване на учебния материал.

## МЕТОДИ ЗА ОЦЕНЯВАНЕ

> Всеки студент разработва самостоятелна курсова задача, представляваща изследване на конкретен проблем в областта на защитата на корпоративните мрежи. Задачата включва самостоятелна разработка на определена тема от тематиката на дисциплината. Оценяват се реализацията и защитата на разработката - **до 30 т.** Критериите за оценяване на разработката са: оригиналност, задълбоченост на изследването, сложност на темата, представяне на разработката.

> За представяне на собствени идеи - **до 10 т.**

> За присъствия и участие в упражненията се получават **до 6 т.**

Изпитът е писмен и представлява тест с отворени въпроси, който се оценява с максимално **54 т.** Крайната оценка е комплексна и включва в себе текущ контрол на семинарните упражнения, оценка от курсовата работа и оценка от писмения изпит. За оформяне на оценката студентът набира точки, чиито максимална стойност е 100. Общата оценка се определя от сумата на точките през семестъра и от изпитната процедура:

36-50т. - Среден (3); 51-65 т. - Добър (4); 66-80 т.-Мн. Добър(5); 81-100 т.-Отличен (6).

Студентът трябва да има минимум 14 точки от контрола през семестъра и минимум 22 точки от изпитната процедура, за да му се формира положителна комплексна оценка.

## ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА


1. Ларс Кландер, Защита от хакери, СофтПрес, София, 1999, ISBN 954-685-055-1, (българско издание).
2. Анонимус, Максимална защита, Книги 1&2, ИнфоДАР, София, 2001, ISBN 954-761-070- 8, (българско издание).
3. Майк Шима, Брадли Джонсън, Анти-хакер, СофтПрес ООД, 2005, ISBN 954-685-324-0, (българско издание).
4. Пол Улфе, Чарли Скот, Майк Ъруин, Анти-спам, СофтПрес ООД, 2005, ISBN 954-685- 328-3, (българско издание).
5. Швета Базин, Основи на мрежовата сигурност, Дуо дизайн ООД, 2004, ISBN 954-8396- 21-1, (българско издание).
6. Ашок Any, Администриране и защита на Apache Server, Дуо дизайн ООД, 2004, ISBN 954-8396-19-X, (българско издание).
7. Харприт Гангули, JAVA сигурност, Дуо дизайн ООД, 2004, ISBN 954-8396-24-6, (българско издание).

8. Рупендра Джийт Санду, Оцеляване при бедствия и аварии, Дуо дизайн ООД, 2004, ISBN 954-8396-20-3, (българско издание).
9. Сурби Малхотра, Microsoft .NET Framework сигурност, Дуо дизайн ООД, 2005, ISBN 954- 8396-25-4, (българско издание).
10. Базин Ш., Основи на мрежовата сигурност, Duo Design, 2004.
11. Притам В. В., Защитни стени и сигурност в Интернет, Duo Design, 2005.
12. Семерджиев Ц., Сигурност и защита на информацията, Класика и Стил, 2007.
13. Уелс К., Сигурност на Ajax приложения, ЗеСТ Прес, 2009.
14. http://www.nlcv.bas.bg
15. http://www.cybercrime.bg/bg
16. http://www.sans.org
17. http://www.nist.gov
18. http://www.securityfocus.com/
19. http://www.cert.org/
20. http://www.nsa.gov/
21. http://searchsecurity.techtarget.com/