СОФИЙСКИ УНИВЕРСИТЕТ "СВ. КЛИМЕНТ ОХРИДСКИ"
ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА

УЧЕБНА ПРОГРАМА

ОКС „бакалавър”

Избираема дисциплина

Утвърдил: ……
/декан/

Утвърдена с решение на ФС с протокол:
№ ……..… от ……..…….

редовна форма на обучение										
Специалност:	*(код и наименование)*									
Софтуерно инженерство, Компютърни науки, Информационни системи, Информатика, Приложна математика, Анализ на данни										

Дисциплина:	*(код и наименование)*	**Ж**	**6**	**3**	**1**
Въведение в мрежовата сигурност					
Fundamentals of Network Security					

Учебната програма е разработена и предложена за утвърждаване от катедра:	
Информационни Технологии (ИТ)	
от:	Георги Георгиев

Преподавателските екипи се утвърждават ежегодно от Факултетен съвет.

Заетост и кредити		
	Обща заетост:	**150**
	Кредити:	**5**
Учебна заетост	***Форма***	***Хорариум***
Аудиторна заетост	Лекции	30
	Семинарни упражнения	0
	Практически упражнения (хоспитиране)	30
	Обща аудиторна заетост:	*60*
	Кредити аудиторна заетост:	*2*
Извънаудиторна заетост	Подготовка на домашни работи (малки проекти)	
	Контролни работи и подготовка за тях	20
	Учебен проект	
	Самосотятелна работа в библиотека или с интернет ресурси	20
	Доклад/Презентация	
	Друг вид извънаудиторна заетост	
	Подготовка за изпит	50
	Обща извънаудиторна заетост:	*90*
	Кредити извънаудиторна заетост:	*3*

Предвидена форма на оценяване:	И

И - изпит, КИ - комбинирано изпитване; ТО - текущо оценяване

Формиране на оценката по дисциплината		
№	***Показател***	***%***
	Контролни работи	
	Участие в час	
	Домашни работи	
	Учебен проект (разработване и защита)	
	Тестова проверка	33
	Текуща самостоятелна работа/контролна работа	
	Демострационни занятия	
	Участие в тематични дискусии	
	Решаване на казуси	
	Изпит - практика (решаване на задачи)	
	Изпит - теория (финален тест в края на курса)	67

Анотация на учебната дисциплина
Курсът въвежда студентите в света на киберсигурността - запознава ги с базовите представи за мрежова сигурност, за идентифициране на уязвими места по отношение на сигурността и на възможни атаки, за реагиране при атаки и възстановяване след инциденти в сигурността. Този курс дава на студентите практически поглед върху някои от тактиките, техниките и процедурите, които обикновено се използват по време на тест за проникване. Включени са реални упражнения за придобиване на сериозен практически опит по отношение на защита на данни, сървъри и мрежи. Курсът е предназначен за професионална подготовка на мрежови администратори и администратори по сигурността.

Предварителни изисквания
От кандидатите за този курс се изисква да имат базови компютърни умения. Необходимо е и свободно ползване на технически английски език.

Очаквани резултати
След успешно преминат курс на обучение студентите ще могат:
· да защитават личния си дигитален живот;
· ще получат представа за най-големите предизвикателства пред сигурността, пред които са изправени компаниите, правителствата и образователните институции;
· ще усвоят основни стратегии за документиране и докладване на резултатите от тестовете за сигурност;
· ще могат да планират и изпълняват основен одит за сигурността на бизнес компании или организации.

Учебно съдържание		
№	***Тема***	***Хорариум л./с.упр./пр.***
	Лекции	

1	**Модул 0**: Въведение	2
2	**Модул 1**: Подготовка за обезопасяване на активи	2
3	**Модул 2**: Разбиране на слоевете за сигурност. Внедряване на базови линии за сигурност (Secure Computing Baselines)	2
4	**Модул 3**: Защита на информация чрез контрол на достъпа и удостоверяване	2
5	**Модул 4**: Използване на криптография за защита на информацията	3
6	**Модул 5**: Използване на PKI за защита на информация	3
7	**Модул 6**: Защита на интернет приложения и компоненти	2
8	**Модул 7**: Внедряване на сигурност за електронна поща и чат системи	2
9	**Модул 8**: Управление на сигурността за директорийни услуги и DNS	2
10	**Модул 9**: Защита при предаването на данни	2
11	**Модул 10**: Внедряване и наблюдение на сигурността за мрежовия периметър (DMZ)	2
12	**Модул 11**: Управление на оперативната сигурност	2
13	**Модул 12**: Осигуряване на непрекъснатостта на бизнеса	2
14	**Модул 13**: Реагиране при инциденти, свързани със сигурността	2
	Практически упражнения	
1	Лаб 1: Проучвателна фаза: Сканиране с NMAP, Оценка на уязвимостта с OpenVAS	1
2	Лаб 2: Троянски кон за отдалечен достъп (RAT) с помощта на Reverse TCP Meterpreter	2
3	Лаб 3: Ескалиране на привилегии и инсталиране на Backdoor	2
4	Лаб 4: Събиране на информация с шпионски софтуер Spyware Screen Captures и Keyloggers	1
5	Лаб 5: Социално инженерство: Събиране на идентификационни данни и отдалечен достъп чрез фишинг имейли	1
6	Лаб 6: Атака чрез SQL инжектиране на уеб приложение	2
7	Лаб 7: Cross-site Scripting (XSS) атака срещу уеб приложение	1

8	Лаб 8: Атаки за отказ на услуга (DoS): SYN/FIN/RST Flood, Smurf атака и SlowLoris	2
9	Лаб 9: Криптографско хеширане и симетрично криптиране	2
10	Лаб 10: Асиметрично криптиране: RSA, цифрови подписи, Diffie-Hellman	2
11	Лаб 11: Инфраструктура с публични ключове: Сертифициращи организации, цифрови сертификати	2
12	Лаб 12: Конфигуриране на Stateful Packet Filter с помощта на iptables	2
13	Лаб 13: Атака с онлайн речник (Dictionary Attack) срещу уеб страница за логване	2
14	Лаб 14: Откриване и предотвратяване на проникване с помощта на Suricata	2
15	Лаб 15: Packet Sniffing и Relay Attack	2
16	Лаб 16: Отравяне на DNS кеш	2
17	Лаб 17: Man In The Middle Attack с помощта на ARP Spoofing	2
18	Лаб 18: Разбиране на атаките с препълване на буфер в уязвимо приложение	2
19	Лаб 19: Провеждане на офлайн атаки към пароли	2

Конспект за изпит	
№	***Въпрос***
1	Подготовка за обезопасяване на активи
2	Разбиране на слоевете за сигурност. Внедряване на базови линии за сигурност (Secure Computing Baselines)
3	Защита на информация чрез контрол на достъпа и удостоверяване
4	Използване на криптография за защита на информацията
5	Използване на PKI за защита на информация
6	Защита на интернет приложения и компоненти
7	Внедряване на сигурност за електронна поща и чат системи
8	Управление на сигурността за директорийни услуги и DNS
9	Защита при предаването на данни
10	Внедряване и наблюдение на сигурността за мрежовия периметър (DMZ)
11	Управление на оперативната сигурност

12	Осигуряване на непрекъснатостта на бизнеса
13	Реагиране при инциденти, свързани със сигурността

Библиография
Основна
1. http://rsmt.it.fmi.uni-sofia.bg/fns
Допълнителна
1. Computer Security Fundamentals. Dr. Chuck Easttom, Fourth Edition, Pearson (2020) 1120 p.
2. Elementary Information Security. 3rd Edition. Richard Smith, PhD. Jones & Bartlett Learning
3. Security Fundamentals. Crystal Panek. Sybex (2020) 402 p.

Дата: 24.06.2024 г. **Съставил:** Георги Георгиев

СПРАВКА ПРЕПОДАВАТЕЛСКИ ЕКИПИ

Софтуерно инженерство, Компютърни науки, Информационни системи, Информатика

Въведение в мрежовата сигурност; Ж631

уч. година	титуляр	асистент	пояснение
2024/2025	Георги Георгиев	Кристиян Младенов	НОВА ИД 2+ курс, Р/зимен сем.