



Утвърдил:

Декан

Дата

СОФИЙСКИ УНИВЕРСИТЕТ "СВ. КЛИМЕНТ ОХРИДСКИ"

Факултет: Физически

Специалност: (код и наименование)

--	--	--	--	--	--	--	--	--	--

„Безжични мрежи и устройства“

Магистърска програма: (код и наименование)

Ф	3	Б	2	7	2	1	1	2
---	---	---	---	---	---	---	---	---

„Безжични мрежи и устройства“

УЧЕБНА ПРОГРАМА

Дисциплина:

--	--	--	--

 (код и наименование)

„Сигурност на комуникационните мрежи и системи“

Преподавател: гл. асист. д-р Любосвет Стойчев Стоев

Асистент:

Учебна заетост	Форма	Хорариум
Аудиторна заетост	Лекции	30
	Семинарни упражнения	15
	Практически упражнения	15
Обща аудиторна заетост		60
Извън-аудиторна заетост	Подготовка за контролна работа по време на курса	30
	Подготовка на разширен конспект по една тема от конспекта (до 3-5 страници)	40
	Проучване на литература и електронни издания	20
Обща извън-аудиторна заетост		90
ОБЩА ЗАЕТОСТ		150
Кредити аудиторна заетост		2
Кредити извън-аудиторна заетост		3
ОБЩО ЕКСТ		5

№	Формиране на оценката по дисциплината	% от оценката
1.	Писмен тест по въпроси от конспекта (по жребий);	30
2.	Самостоятелно подготвена в къщи „паметна записка“ (до 3-5 стр. конспектиране) на една тема от конспекта по жребий	30
3.	Контролна работа	30
4.	Окончателен изпит – окончателно събеседване	10

Анотация на учебната дисциплина:

Високата сложност на съвременната инфраструктура прави обществото чувствително от голям брой заплахи. Те са свързани както с рискови техногенни фактори, така и от умишлени въздействия от криминален или терористичен характер. Модерните комуникационни и информационни мрежи пренасят огромен поток от данни и притежават висока степен на автономност, което поставя в зависимост от тяхното безупречно функциониране всички сфери на човешката дейност. Това прави тяхната защита въпрос от първостепенна важност за качеството на живота и сигурността на обществото.

Предложеният курс по „Сигурност на комуникационните мрежи и системи” ще предложи кратък преглед на развитието на методите за защита на информацията и комуникационните мрежи и ще продължи с обзор на съвременната практика в различни области. Слушателите ще бъдат запознати с методите за повишаване на устойчивостта на информационните мрежи в условията на техногенни смущения и аварии, ограничаването на неоторизиран достъп и мониторинга на непозволена дейност.

Предварителни изисквания:

За да се посещават този курс от студентите не се изисква специална подготовка. Желателно е да имат добри познания от общия курс по физика, обща представа за излъчването и разпространението на електромагнитни вълни, да са слушали курса по теория на информацията, както и добри познания по теория на вероятностите и статистика.

Очаквани резултати:

След успешното завършване на курса се очаква всеки студент да може:

- Да разбира и да борави свободно с основни понятия от областта на сигурността и отбраната (научна област 9, направление 9.1 – „национална сигурност“), такива като защита и сигурност на системи и организации, среда за сигурност, риск и показатели на риска
- да е запознат с основните форми на защита на информационните системи и свързаната с тях инфраструктура, такива като физическа защита, криптография и стеганография.
- да е запознат с основните принципи на управлението на риска;
- да може да извършва основен анализ на риска и кризисно планиране за малка организация/ ведомство/ предприятие.

Учебно съдържание**I. Лекции:**

№	Тема:	Хорариум
1	1. Видове заплахи за комуникациите и нужда от защита 2. Комуникации: задачи и ограничения 3 Комуникации: задачи и ограничения 3.1 Видове защита 3.2 Аналогия с компютърната безопасност	10
2	4 Методи за защита 4.1 Криптография 4.2 Стеганография 4.3 Мрежи с регистрирани потребители 4.4 Анонимни мрежи 4.5 Анонимни комуникационни устройства 5 Корпоративна готовност и превенция 5.1 Business impact analysis 5.2 Business continuity management (general) 6 Системи за сравнително сигурни комуникации 6.1 Анонимна мобилна телефония 6.2 Наземни линии 6.3 Анонимен интернет	10

3	7 Комуникационно-информационни мрежи за специални цели: понятие за радиоелектронно разузнаване и борба 7.1 Радиоелектронно разузнаване 7.2 Радиолокация 7.3 Електронно противодействие	10
Общо		30

II. Семинарни упражнения:

№	Тема:	Хорариум
1	<ul style="list-style-type: none"> • Кризисно планиране • Business continuity • Щабна игра “Отговор на заплаха” 	30
Общо		15

Конспект по Сигурност на комуникационните мрежи и системи

1. Понятие за сигурност. Среда за сигурност – йерархия. Корпоративна, национална и международна сигурност.
2. Аспекти на сигурността. Сигурност, безопасност и защита.
3. Сигурност на информацията – аспекти, подходи и решения.
4. Кибер-сигурност. Обзор на кибер-средата
5. Основи на тайнописа. Криптография и стеганография
6. Риск и управление на риска
7. Организация и управление на системите за сигурност.
8. Анализ на информационното пространство.

Библиография

Основна:

- [1] В. И. Громов, Г. А. Васильев „Выживание и безопасность”, Москва 1998.
- [2] В. А. Вартанесян „Радиоелектронная разведка”, ВИ МинОб 1975.
- [3] А. В. Куприянов и А. И. Сахаров „Теоретические основы радиоелектронной борьбы”, Москва 2007.
- [4] ISO 31000: RISK MANAGEMENT.
- [5] US DOD FM 19.30: PHYSICAL SECURITY — WHOLE BUILDING DESIGN GUIDE
- [6] GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION, Brussels, 17.11.2005 COM(2005) 576.

Допълнителна:

- [7] D. S. Alberts, J. J. Garstka and F. P. Stein, NET-CENTRIC WARFARE (Washington DC, DoD 2000) SBN 1-57906-019-6
- [8] J. F. Teugels, ENCYCLOPEDIA OF ACTUARIAL SCIENCE (John Wiley & Sons, 2004) ISBN: 9780470012505.

Дата: май 2013 г.

Съставил: /...../

(гл. асист. д-р Любосвет Стойчев Стоев)