

# ЗАЩИТА НА ИНФОРМАЦИЯТА

доц. д-р Георги Павлов, Университетско издателство “Стопанство”, София, 2010

Увод.....	7
<b>Първа глава</b>	
<b>АНАЛИЗ НА ИНФОРМАЦИОННАТА СИГУРНОСТ.....</b>	<b>9</b>
1.. Определение за информационна сигурност (ИС).....	9
2.. Основни понятия, свързани с ИС.....	11
3.. Защита на информацията в информационните системи .....	14
4.. Обзорни въпроси и задачи за самостоятелна работа .....	29
<b>Втора глава</b>	
<b>КРИТЕРИИ И СТАНДАРТИ ЗА ИНФОРМАЦИОННА СИГУРНОСТ.....</b>	<b>30</b>
1.. Критерии за оценка на надеждни компютърни системи в САЩ (Оранжева книга на МО на САЩ).....	30
2.. Критерии за оценка на информационната сигурност в ЕС .....	41
3.. Защита от нерегламентиран достъп в системите на Руската федерация (РФ) .....	42
4.. Обзорни въпроси и задачи за самостоятелна работа .....	43
<b>Трета глава</b>	
<b>СИСТЕМА ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ (СУИС) .....</b>	<b>44</b>
1.. Необходимост от осигуряване на информационна сигурност .....	44
2.. История на стандартите за информационна сигурност .....	47
3.. Разработване и внедряване на Система за управление на информационната сигурност (СУИС), Стандарти 180/IEC 17799 и 27001 .....	51
4.. Обзорни въпроси и задачи за самостоятелна работа .....	60
<b>Четвърта глава</b>	
<b>СЪЩНОСТ НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ .....</b>	<b>61</b>
1.. Основни понятия, свързани с класифицирането на информация .....	61
2.. Области за класификация на информация във връзка с националната сигурност .....	62
3.. Видове класифицирана информация и нива на класификация .....	69
4.. Обзорни въпроси и задачи за самостоятелна работа .....	70
<b>Пета глава</b>	
<b>ДОКУМЕНТАЛНА СИГУРНОСТ .....</b>	<b>71</b>
1. Основни понятия.....	71
2. Процедура за класифициране на информацията .....	72
3. Процедура по маркиране на класифицирана информация .....	74
4. Регистриране на КИ - Уникален регистрационен номер.....	76
5. Регистратури за класифицирана информация.....	80
6. Обзорни въпроси и задачи за самостоятелна работа .....	84
<b>Шеста глава</b>	
<b>ВИДОВЕ ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ.....</b>	<b>85</b>
1. Видове защита на КИ .....	85
2. Същност на криптографската сигурност и сертифициране .....	86
3. Същност на сигурността на АИС и/или мрежи, в които се обработва класифицирана информация. Разработка и процедура за сертифициране.....	88
4. Същност на индустриалната сигурност. Важни моменти в реализацията й.....	102

5. Обзорни въпроси и задачи за самостоятелна работа.....	103
--	-----

### Седма глава

<b>ПРИЛОЖНА КРИПТОГРАФИЯ</b> .....	104
------------------------------------	-----

1. Същност на криптографията.....	104
2. Традиционна криптография. Исторически анализ.....	106
3. Обзорни въпроси и задачи за самостоятелна работа .....	112

### Осма глава

<b>БЛОКОВИ КРИПТОАЛГОРИТМИ</b> .....	113
--------------------------------------	-----

1. Криптоалгоритми със секретен ключ.....	113
2. Схеми за реализация и криптоанализ на DES(DATA Encryption Standard) .....	114
3. Тройна (TRIPLE) DEA, IDEA и AES.....	118
4. Обзорни въпроси и задачи за самостоятелна работа .....	127

### Девета глава

<b>КРИПТОГРАФИЯ С ПУБЛИЧНИ КЛЮЧОВЕ</b> .....	128
--	-----

1. Криптография с публични ключове. Алгоритъм K8A.....	128
2. Алгоритъм на Ал Гамал (Al Gamal) .....	131
3. Организации в областта на криптографията .....	133
4. Обзорни въпроси и задачи за самостоятелна работа .....	136

### Десета глава

<b>СИГУРНОСТ НА УДОСТОВЕРЯВАНЕТО</b> .....	137
--	-----

1. Удостоверяване - същност, алгоритми и протоколи.....	137
2. Удостоверяване, базирано на разпределени секретни ключове (протоколи Challenge-Response) .....	144
3. Алгоритъм на Дифи и Хе споразумение за ключове	
4. Удостоверяване с център	
5. Удостоверяване с използване	
6. Удостоверяване KERBER	
7. Обзорни въпроси и задачи	

### Единадесета глава

#### **ЦИФРОВИ СЕРТИФИКАТИ**

1. Основни понятия..... —	
2. Алгоритми със секретен ключ	
3. Подписи с публични ключове	
4. Алгоритми MD - Message	
5. Политика в областта на ■	
6. Обзорни въпроси и задачи	

Терминологичен речник-

Приложения.....

Литература.....—