

**ИКОНОМИЧЕСКИ УНИВЕРСИТЕТ - ВАРНА**  
**ФАКУЛТЕТ „ИНФОРМАТИКА“**  
**КАТЕДРА „ИНФОРМАТИКА“**

---

---

Приета от ФС (протокол № 8 / 05.03.2020 г.)

Приета от КС (протокол № 7 / 28.02.2020 г.)

**УТВЪРЖДАВАМ:**

**Декан:**

**(проф. д-р Владимир Сълов)**

**У Ч Е Б Н А   П Р О Г Р А М А**

ПО ДИСЦИПЛИНАТА: “КРИПТОГРАФИЯ И ЗАЩИТА НА ДАННИТЕ”;

ЗА СПЕЦ: „Информатика и компютърни науки“; ОКС „бакалавър“

КУРС НА ОБУЧЕНИЕ: 3; СЕМЕСТЪР: 6;

ОБЩА СТУДЕНТСКА ЗАЕТОСТ: 150 ч.; в т.ч. аудиторна 60 ч.

КРЕДИТИ: 5

**РАЗПРЕДЕЛЕНИЕ НА СТУДЕНТСКАТА ЗАЕТОСТ СЪГЛАСНО УЧЕБНИЯ ПЛАН**

<i>ВИД УЧЕБНИ ЗАНЯТИЯ</i>	<i>ОБЩО(часове)</i>	<i>СЕДМИЧНА НАТОВАРЕНОСТ (часове)</i>
АУДИТОРНА ЗАЕТОСТ:		
т. ч.		
• ЛЕКЦИИ	30	2
• УПРАЖНЕНИЯ (семинарни занятия/ лабораторни упражнения)	30	2
ИЗВЪНАУДИТОРНА ЗАЕТОСТ	90	-

Изготвили програмата:

1. ....  
(проф. д-р Владимир Сълов)
2. ....  
(гл. ас. д-р Деян Михайлов)
3. ....  
(гл. ас. д-р Бонимир Пенчев)

Ръководител катедра: .....  
„Информатика“ (проф. д-р Юлиан Василев)

## I. АНОТАЦИЯ

Дисциплината „Криптография и защита на данните” предоставя основни теоретични знания в областта на кодирането и криптографията и тяхното приложение в компютърните системи. Разглеждат се аспектите на защитата на информацията и основните математически методи за постигането и. Излагат се някои класически и съвременни форми на криптографска защита.

Придобитите знания и умения могат да се прилагат за определяне на необходимите мерки за защита на информацията при обработка и предаване на данни и тяхната имплементация в компютърните системи и мрежи, както и да бъдат основа за допълнително самостоятелно постигане на ново знание.

Дисциплината дава възможност на студентите да задълбочат получените фундаментални знания в областта на дискретната математика, алгебрата, теорията на вероятностите, програмирането, компютърните мрежи и да формират нови умения за интеграция на методите и средствата за криптиране в различни компютърни системи.

## II. ТЕМАТИЧНО СЪДЪРЖАНИЕ

No. по ред	НАИМЕНОВАНИЕ НА ТЕМИТЕ И ПОДТЕМИТЕ	БРОЙ ЧАСОВЕ		
		Л	СЗ	ЛУ
<b>Тема 1. Теоретични основи на криптографията и защитата на данните</b>		<b>8</b>	<b>8</b>	
1.1	Понятие за информационна сигурност и защита на данните. Атаки срещу информационната сигурност и противодействие. Механизми за безопасност. Правна регламентация.	2	2	
1.2	Модулна аритметика. Основни понятия и алгоритми.	2	2	
1.3	Класически субституционни и транспозиционни шифри. Криптоанализ.	2	2	
1.4	Теоретико-информационна устойчивост на шифрите.	2	2	
<b>Тема 2. Съвременни шифри</b>		<b>10</b>	<b>10</b>	
2.1	Съвременни симетрични шифри	2	2	
2.2	Съвременни асиметрични шифри	2	2	
2.3	Интегритет на данните. Криптографски хеш-функции.	2	2	
2.4	Електронен подпис	2	2	
2.5	Елиптични криви.	2	2	
<b>Тема 3. Прилагане на криптографски методи и средства</b>		<b>12</b>	<b>12</b>	
3.1	Прилагане на симетрични и асиметрични шифри.	2	2	
3.2	Криптографски стандарти и протоколи.	2	2	
3.3	Криптографски библиотеки.	4	4	
3.4	Изграждане на криптографска инфраструктура	4	4	
<b>Общо:</b>		<b>30</b>	<b>30</b>	

### **III. ФОРМИ НА КОНТРОЛ:**

<b>№. по ред</b>	<b>ВИД И ФОРМА НА КОНТРОЛА</b>	<b>Брой</b>	<b>ИАЗ ч.</b>
<b>1.</b>	<b>Семестриален (текущ) контрол</b>		
1.1.	Контролни работи	2	40
<b>Общо за семестриален контрол:</b>		<b>2</b>	<b>40</b>
<b>2.</b>	<b>Сесиен (краен) контрол</b>		
2.1.	Изпит (тест)	1	50
<b>Общо за сесиен контрол:</b>		<b>1</b>	<b>50</b>
<b>Общо за всички форми на контрол:</b>		<b>3</b>	<b>90</b>

### **IV. ЛИТЕРАТУРА**

#### **ЗАДЪЛЖИТЕЛНА (ОСНОВНА) ЛИТЕРАТУРА:**

1. Закон за защита на класифицираната информация ДВ бр. 45/2002, <http://www.dksi.bg/bg/>
2. Закон за киберсигурност. ДВ. бр.94/2018г.
3. Наредба за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация ДВ бр. 46/2003, <http://www.dksi.bg/>
4. Наредба за криптографската сигурност на класифицираната информация ДВ бр. 102/2003, <http://www.dksi.bg/>
5. Наредба за минималните изисквания за мрежова и информационна сигурност. ДВ бр. 59/2019
6. Stinson, D. & Paterson, M. Cryptography. Theory and Practice. Taylor & Francis, 2019
7. Nigel Smart. Cryptography. An Introduction. [https://www.cs.bris.ac.uk/~nigel/Crypto\\_Book/](https://www.cs.bris.ac.uk/~nigel/Crypto_Book/)

#### **ПРЕПОРЪЧИТЕЛНА (ДОПЪЛНИТЕЛНА) ЛИТЕРАТУРА:**

1. Авторски колектив. Компютърна сигурност и защита. AlexSoft, 2006.
2. Каео, М. Проектиране на мрежова сигурност. СофтПрес, 2006.
3. Наредба за системата от мерки, способности и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване ДВ бр. 22/2003 <http://www.dksi.bg/>
4. Павлов, Г. Защита на информацията. УНСС, 2010.
5. Станек, У. Windows Server 2003 – Наръчник на администратора. СофтПрес, 2004.
6. Paar, C et al. Understanding Cryptography. Springer, 2010.
7. Aumasson J-P. Serious Cryptography. A Practical Introduction to Modern Encryption. San Francisco, 2019