

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

---

---

**УТВЪРЖДАВАМ:**

**Ректор:**

(Проф. д-р Пл. Илиев)

**У Ч Е Б Н А П Р О Г Р А М А**

ПО ДИСЦИПЛИНАТА: “КРИПТОГРАФИЯ И ЗАЩИТА НА ДАННИТЕ”;

ЗА СПЕЦ: „Информатика“; 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. ....  
(ас. д-р Бонимир Пенчев)

Ръководител катедра: .....  
„Информатика“ (проф. д-р Владимир Сълов)

## I. АНОТАЦИЯ

Дисциплината „Криптография и защита на данните“ предоставя основни теоретични знания в областта на кодирането и криптографията и тяхното приложение в компютърните системи. Разглежда 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>15</b>		<b>15</b>
1.1	Понятие за информационна сигурност и защита на данните. Аспекти. Атаки срещу информационната сигурност и противодействие. Механизми за безопасност.	1		
1.2	Нормативни документи в областта на сигурността на информацията.	1		
1.3	Модулна аритметика. Основни понятия и алгоритми.	2		3
1.4	Елиптични криви.	1		1
1.5	Класически субституционни и транспозиционни шифри. Криптоанализ.	2		3
1.6	Теоретико-информационна устойчивост на шифрите.	2		2
1.7	Интегритет на данните. Шумоустойчивост.	2		2
1.8	Принципи за изграждане на криптосистеми със симетрични шифри.	2		2
1.9	Принципи за изграждане на криптосистеми с открит ключ.	2		2
<b>Тема 2. Приложение на криптографията в компютърните системи</b>		<b>15</b>		<b>15</b>
2.1	Криптосистеми, използващи симетрични алгоритми.	3		3
2.2	Криптосистеми, използващи асиметрични алгоритми.	3		3
2.3	Криптографски хеш-функции. Електронен подпис.	3		3
2.4	Криптографски стандарти и протоколи.	3		3
2.5	Инфраструктура с публичен ключ.	3		3
<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	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, посл. промяна 14.10.2016 г. <http://www.dksi.bg/bg/>
2. 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, посл. промяна 10.05.2016 г. <http://www.dksi.bg/>
3. Наредба за криптографската сигурност на класифицираната информация ДВ бр. 102/2003, посл. промяна 10.05.2016 г. <http://www.dksi.bg/>
4. Nigel Smart. Cryptography. An Introduction. [https://www.cs.bris.ac.uk/~nigel/Crypto\\_Book/](https://www.cs.bris.ac.uk/~nigel/Crypto_Book/) (rev 10th April 2013)
5. Delfs, H., Knebl, H. Introduction to Cryptography Principles and Applications 3<sup>rd</sup> Ed., Berlin, Springer, 2015.

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

1. Barker, W., Barker, E. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST SP800-67, January 2012.  
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-67r1.pdf>
2. Secure Hash Standard (SHS), FIPS PUB 180-4, August 2015  
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>
3. Digital Signature Standard (DSS), FIPS PUB 186-4 July 2013  
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>
4. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, August 2015, <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>