

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: **„Мобилни и уеб технологии“; ОКС „бакалавър“**

КУРС НА ОБУЧЕНИЕ: **4; СЕМЕСТЪР: 8;**

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 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
Тема 1. Теоретични основи на криптографията и защитата на данните		15		15
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
Тема 2. Приложение на криптографията в компютърните системи		15		15
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
Общо:		30		30

III. ФОРМИ НА КОНТРОЛ:

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

IV. ЛИТЕРАТУРА

ЗАДЪЛЖИТЕЛНА (ОСНОВНА) ЛИТЕРАТУРА:

1. Delfs, H., Knebl, H. Introduction to Cryptography Principles and Applications 3rd Ed., Berlin, Springer, 2015.
2. Закон за защита на класифицираната информация ДВ бр. 45/2002 // <http://www.pz.government.bg/z/11.pdf> , (11.12.2017 г.)
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/NR/rdonlyres/52235A0C-9B81-4ED3-943E-DEEBC7EC49A0/0/NAREDBA_za_zadyljitelnite_obsi_usloviq_za_sigurnost_na_avtomatizirane_ite_informacionni_sistemi_ili_mr.pdf , (11.12.2017 г.)
4. Наредба за криптографската сигурност на класифицираната информация ДВ бр. 102/2003 // http://www.dksi.bg/NR/rdonlyres/F918515D-D2D8-4CEF-874D-07CD07910C8E/0/NAREDBA_za_kriptografskata_sigurnost_na_klasificiranata_informacij.pdf, (11.12.2017 г.)
5. Nigel Smart. Cryptography. An Introduction // https://www.cs.bris.ac.uk/~nigel/Crypto_Book/, (11.12.2017 г.)

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> , (11.12.2017 г.)
2. Digital Signature Standard (DSS), FIPS PUB 186-4 July 2013 // <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf> , (11.12.2017 г.)
3. Secure Hash Standard (SHS), FIPS PUB 180-4, August 2015 // <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf> , (11.12.2017 г.)
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> , (11.12.2017 г.)