И К О Н О М И Ч Е С К И У Н И В Е Р С И Т Е Т – В А Р Н А

Ф А К У Л Т Е Т „И Н Ф О Р М А Т И К А“

К А Т Е Д Р А „И Н Ф О Р М А Т И К А“

Приета от ФС (протокол № 9/24.04.2024 г.)

Приета от КС (протокол № 10/16.04.2024 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: Всички специалности от ПН 4.6 Информатика и компютърни науки;

ОКС „бакалавър“ – редовно обучение

КУРС НА ОБУЧЕНИЕ: 2; СЕМЕСТЪР: 4

ОБЩА СТУДЕНТСКА ЗАЕТОСТ: 180 ч.; в т.ч. аудиторна 60 ч.

КРЕДИТИ: 6

РАЗПРЕДЕЛЕНИЕ НА СТУДЕНТСКАТА ЗАЕТОСТ СЪГЛАСНО УЧЕБНИЯ ПЛАН

ВИД УЧЕБНИ ЗАНЯТИЯ	***ОБЩО (часове)***	***СЕДМИЧНА НАТОВАРЕНОСТ (часове)***
АУДИТОРНА ЗАЕТОСТ: т.ч. • ЛЕКЦИИ • УПРАЖНЕНИЯ (семинарни занятия/ лабораторни упражнения)	 30 30	 2 2
ИЗВЪНАУДИТОРНА ЗАЕТОСТ	120	-

Изготвили програмата:

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

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

I. А Н О Т А Ц И Я

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 ѝ. 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.

В хода на обучение се прилагат и развиват следните ключови компетентности, съгласно препоръката на Съвета на Европейския съюз от 22 май 2018 г, а именно:

- *Математическа компетентност и точни науки – група 3. Способност и желание за използване на математически начини за мислене и представяне (формули, модели и концепции).*
- *Цифрова компетентност – група 4. Способност за ползване на цифрова информация и използване на софтуерни продукти.*
- *Предприемаческа компетентност – група 7. Способност за изграждане на аналитично мислене при самостоятелно изпълнение на задачи.*

II. Т Е М А Т И Ч Н О С Ъ Д Ъ Р Ж А Н И Е

No. по ред	**НАИМЕНОВАНИЕ НА ТЕМИТЕ И ПОДТЕМИТЕ**	**БРОЙ ЧАСОВЕ**		
		Л	**СЗ**	**ЛУ**
ТЕМА 1. ТЕОРЕТИЧНИ ОСНОВИ НА КРИПТОГРАФИЯТА И ЗАЩИТАТА НА ДАННИТЕ		**8**	**8**	
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	
ТЕМА 2. СЪВРЕМЕННИ ШИФРИ		**10**	**10**	
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	
ТЕМА 3. ПРИЛАГАНЕ НА КРИПТОГРАФСКИ МЕТОДИ И СРЕДСТВА		**12**	**12**	
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	
	Общо:	**30**	**30**	

III. ФОРМИ НА КОНТРОЛ

No. по ред	ВИД И ФОРМА НА КОНТРОЛА[1]	Брой	ИАЗ ч.
1.	**Семестриално оценяване**		
1.1.	Контролни работи	2	40
1.2.	Домашна работа	1	20
	Общо за семестриалното оценяване:	**3**	**60**
2.	**Сесийно оценяване**		
2.1.	Изпит	1	60
	Общо за сесийното оценяване:	**1**	**60**
	Общо за всички форми на контрол:	**4**	**120**

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/

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, способи 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
8. Михайлов, Д. Криптография и криптоанализ с MS Excel. Математика и информатика: том. 65 (1), стр. 53-71, 2022 г.

[1] При дисциплини, които завършват с текуща оценка се попълва само т. 1 Семестриално оценяване, съгласно чл.21, ал. 2 от Правилника за оценяване на знанията, уменията и компетентностите на студентите в Икономически университет – Варна.