

ИКОНОМИЧЕСКИ УНИВЕРСИТЕТ – В А Р Н А
ФАКУЛТЕТ „ИНФОРМАТИКА“
КАТЕДРА „ИНФОРМАТИКА“

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: „КИБЕРСИГУРНОСТ“

ЗА СПЕЦ: „Дигитални технологии в бизнеса“;

ОКС „магистър“ – редовно обучение

КУРС НА ОБУЧЕНИЕ: 5 за СС и СНУ, 6 за ДНДО и СПН;

СЕМЕСТЪР: 9 за СС и СНУ, 11 за ДНДО и СПН;

ОБЩА СТУДЕНТСКА ЗАЕТОСТ: 240 ч.; в т.ч. аудиторна 60 ч.

КРЕДИТИ: 8

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	180	-

Изготвили програмата:

1.
(проф. д-р Силвия Парушева)

2.
(гл. ас. д-р Михаил Радев)

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

I. АНОТАЦИЯ

Дисциплината „Киберсигурност“ има за цел за предостави на студентите теоретични знания и практически умения относно основите на киберсигурността.

Основните акценти при обучението се поставят върху следните направления:

- запознаване с важността на киберсигурността за бизнеса и обществото, нейната ключова терминология и основни концепции;
- получаване на знания за различните типове хакерски техники за атаки и източниците на заплахи;
- овладяване на знания относно превантивните мерки и начините за защита срещу основните типове атаки;
- придобиване на способности за прилагане на техники за анализ и ефективна кибер защита.

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 компетентност в областта на точните науки, технологиите и инженерството – група 3.* Чрез обучението по дисциплината се създават умения за практическо приложение на теоретичните знания и подготовката на студентите за работа в областта на анализите, администрирането и одитирането на киберсигурността и нейната успешна защита, както и се развиват техните математически компетенции.

- *Цифрова компетентност – група 4.* Дисциплината способства за развитие на способности на студентите за самообучение, работа в екип, за продължаващо обучение и формиране на нови умения и цифрови компетенции, за вземане на решения относно разработване и прилагане в действие на подходящи кибер стратегии.

II. ТЕМАТИЧНО СЪДЪРЖАНИЕ

No. по ред	НАИМЕНОВАНИЕ НА ТЕМИТЕ И ПОДТЕМИТЕ	БРОЙ ЧАСОВЕ		
		Л	СЗ	ЛУ
Тема 1. Основи на киберсигурността		4	2	
1.1	Ключова терминология в киберсигурността. Значение на киберсигурността.	2	2	
1.2	Оценка на информационните активи и критичността им за бизнеса.	2	-	
Тема 2. Техники за атаки и основни източници на атаки срещу киберсигурността		6	6	
2.1	Основни категории заплахи	3	3	
2.2	Основни типове заплахи. Смесени техники за атаки.	3	3	
Тема 3. Мрежова сигурност		4	4	
3.1	Заплахи за мрежата	2	2	
3.2	Защита срещу мрежово сканиране и атаки	2	2	
3.3	Защита на безжични мрежи	-	-	
Тема 4. Системна сигурност		6	6	
4.1	Заплахи срещу системите	2	2	
4.2	Криптиране на данните	2	2	
4.3	Защита от системни заплахи	2	2	

Тема 5. Сигурност на крайните точки		4	8	
5.1	Заплахи срещу крайните точки	1	2	
5.2	Подобряване на сигурността на крайни точки	1	2	
5.3	Инструменти за събиране на информация за организациите и мрежите	1	2	
5.4	Защита срещу събиране на информация	1	2	
Тема 6. Управление на киберсигурността		6	4	
6.1	Политики и процедури за киберсигурност	2	2	
6.2	Оценка на риска	2	1	
6.3	Планиране за реагиране при инцидент	1	1	
6.4	Обучение и осведоменост на персонала	1	-	
Общо:		30	30	

III. ФОРМИ НА КОНТРОЛ

№. по ред	ВИД И ФОРМА НА КОНТРОЛА¹	Брой	ИАЗ ч.
1.	Семестриално оценяване		
1.1.	Контролна работа	1	40
1.2.	Разработване на курсова работа	1	40
1.3.	Защита на курсова работа и практическа демонстрация	1	30
Общо за семестриално оценяване:		3	110
2.	Сесийно оценяване		
2.1.	Изпит (тест)	1	70
Общо за сесийно оценяване:		1	70
Общо за всички форми на контрол:		4	180

IV. ЛИТЕРАТУРА

ЗАДЪЛЖИТЕЛНА (ОСНОВНА) ЛИТЕРАТУРА:

1. Велу, В. К., Бегс, Р. Изучете Kali Linux: Етично хакване в примери, Асеновци, 2021.
2. Möller, D.P.F. Cybersecurity in Digital Transformation: Scope and Applications. Springer, 2021.

ПРЕПОРЪЧИТЕЛНА (ДОПЪЛНИТЕЛНА) ЛИТЕРАТУРА:

1. Mckinnon, G. The Fundamentals of Computer Security for Beginners: A simple and comprehensive guide to start working in cybersecurity. Ethical Hacking to learn and protect your family and business. 2020.
2. Chowdhry, D.G., Verma, R., Mathur, R. The Evolution of Business in The Cyber Age. Digital Transformation, Threats, and Security. Apple Academic Press, 2020.

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.