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“

УТВЪРЖДАВАМ:
Ректор:
(Проф. д-р Пл. Илиев)

У Ч Е Б Н А П Р О Г Р А М А

ПО ДИСЦИПЛИНАТА: “ПЛАНИРАНЕ И УПРАВЛЕНИЕ СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ”;

ЗА СПЕЦ: „Бизнес информационни системи“; 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

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

Изготвили програмата:

1. ……..
(доц. д-р Силвия Парушева)

2. ……
(ас. Михаил Радев)

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

I. А Н О Т А Ц И Я

Целта на дисциплината „Планиране и управление сигурността на информационните системи" е да предложи знанията, които ще бъдат необходими на студентите, бъдещи специалисти по информационна сигурност.

Дисциплината изисква предварителни знания по операционни системи, организация на протоколите от протоколния стек TCP/IP, компютърни мрежи.

Разглеждат се основните понятия на информационната сигурност, необходимите мерки за реализиране на информационната сигурност, управлението на информационните рискове за корпоративните информационни системи, за изграждане на политика по информационна сигурност.

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. Същност на информационната сигурност. Видове информационна сигурност.		**4**		**3**
1.1	Същност на информационната сигурност. Основни понятия, цели, заплахи, уязвимости			
1.2	Видове информационна сигурност			
Тема 2. Системна сигурност		**3**		**4**
2.1	Сигурност на хардуера			
2.2	Сигурност на операционната система			
2.3	Сигурност на приложенията			
Тема 3. Организационна сигурност		**3**		**3**
3.1	Рамка на информационната сигурност			
3.2	Политики за сигурност, стандарти, процедури и ръководства			
3.3	Одитиране на информационната сигурност			
Тема 4. Мрежова сигурност		**4**		**4**
4.1	Проектиране на сигурна мрежова инфраструктура. Избор на преносна среда и мрежови устройства. Мрежови протоколи и портове.			
4.2	Инструменти за мрежова сигурност – защитни стени, VPN, IDS и филтри. Сигурност на отдалечения достъп. Безжична сигурност			
Тема 5. Основни заплахи за сигурността на информационните системи		**4**		**4**
5.1	Вектори на заплахите. Източници, заплахи и цели на заплахите. Външни и вътрешни заплахи			
5.2	Типове атаки. Атаки със зловреден код. Видове зловреден код.			
5.3	Атаки на мрежово ниво. Атаки на ниво приложения. Други атаки			
Тема 6. Сигурност на достъпа до информационните ресурси		**3**		**3**

6.1	Модели за контрол на достъпа. Аутентикационни модели.			
6.2	Логически и физически контрол на достъпа. Правила за имена и пароли, политики.			
Тема 7. Социален инженеринг		**3**		**3**
7.1	Същност на социалния инженеринг. Потенциални пробиви в сигурността в резултат на социалния инженеринг			
7.2	Методи, използвани в социалния инженеринг			
7.3	Политики и процедури за защита от социален инженеринг			
Тема 8. Криптиране на ресурси		**3**		**3**
8.1	Криптография – алгоритми, шифри, форми на криптиране. Хеширане, алгоритми за хеширане.			
8.2	Криптиране на данни – криптиране на диск и на файлове. Стеганография.			
Тема 9. Управление на сигурността чрез политики		**3**		**3**
9.1	Администриране на сигурността чрез политики за потребители и компютри. Директорийна услуга			
9.2	Прилагане на политики за сигурност. Изключения от правилата за политики.			
	Общо:	**30**		**30**

III. ФОРМИ НА КОНТРОЛ:

No. по ред	**ВИД И ФОРМА НА КОНТРОЛА**	**Брой**	**ИАЗ ч.**
1.	**Семестриален (текущ) контрол**		
1.1.	Тест - проверка на практическите умения за работа	1	35
1.2.	Разработка на курсова работа	1	35
	Общо за семестриален контрол:	**1**	**70**
2.	**Сесиен (краен) контрол**		
2.1.	Изпит (тест)	1	20
	Общо за сесиен контрол:	**1**	**20**
	Общо за всички форми на контрол:	**2**	**90**

IV. ЛИТЕРАТУРА

ЗАДЪЛЖИТЕЛНА (ОСНОВНА) ЛИТЕРАТУРА:

1. Каракънева, Ю., “Киберсигурност – основни аспекти”, Авангард Прима, 2013.
2. Павлов, Г., Пудин, К. “Информационна сигурност в организацията”, Университетско издателство Стопанство, 2011.
3. Stallings, W., Brown L., “Computer Security Principles and Practice”, Third Edition, Pearson Education, Inc., 2015.

ПРЕПОРЪЧИТЕЛНА (ДОПЪЛНИТЕЛНА) ЛИТЕРАТУРА:

1**.** Kizza , J. “Computer Network Security and Cyber Ethics”, 4th Ed., 2014.
2. Rhodes-Ousley, Mark, “Information Security The complete Reference”, McGraw-Hill, 2013.
3. Rountree, D., Windows 2012 Server Network Security, Syngress, 2013.
4. Парушева, С., „Кибератаките в интернет банкирането - предизвикателства към финансовите институции.”, Наука и икономика, Икономически университет - Варна, 2012.
5. Parusheva, S., „A comparative study on the application of biometric technologies for authentication in online banking“, Egyptian Computer Science Journal, ISSN-1110-2586, Vol. 39, No. 4, Sept. 2015.
6. Parusheva, S., Atanasova, T. “Card fraud prevention capabilities with intelligent methods”, 16th International Multidisciplinary Scientific GeoConferences SGEM 2016, Albena, Bulgaria, Book 2, Volume I, 2016.
7. Parusheva, S. (2015) Card-not-present fraud–challenges and counteractions, “Narodnostopanski arhiv”, Academic publishing house “Tsenov” – Svishtov, D. A. Tsenov Academy of Economics – Svishtov, issue 2, pp. 40-52.
8. Atanasova, T., Parusheva, S. Spam filtering through neural networks. 16th International Multidisciplinary Scientific GeoConferences SGEM 2016, Book 2, Volume I, 2016.