УЧЕБЕН ПЛАН

за

провеждане на специализиран курс за обучение по образователна и научна степен „доктор“, на тема: **„Интелигентни системи за сигурност на критична инфраструктура”/ Intelligent security systems of critical infrastructure**

I. АНОТАЦИЯ

Институтът по металознание, съоръжения и технологии с център по хидро- и аеродинамика „Акад. Ангел Балевски“ – БАН/ Institute of metal science, equipment, and technologies with hydro- and aerodynamics center“Acad. A. Balevski” – BAS е акредитиран за обучение и присъждане на образователна и научна степен **„доктор”** по докторска програма „Защита па населението и народното стопанство в критични ситуации (технологии и средства за сигурност и защита на критична инфраструктура при кризи)“ в областта на „5. Технически науки“, професионално направление 5.13. „Общо инженерство“.

В тази връзка, за нуждите на Института и Българската академия на науките, се организира специализиран курс за обучение по образователна и научна степен „доктор“, на тема: „Интелигентни системи за сигурност на критична инфраструктура”.

Курсът представя теоретичните принципи и практически подходи за разработването на интелигентни системи за сигурност на критична инфраструктура. Акцентът е поставен върху създаване на условия за определяне и защита на съответната критична инфраструктура, която предоставя основни услуги на националния и европейски пазар. Тази дейност обхваща всички възможни рискове, което изисква актуализиране на оценките на риска или на съществуващите еквивалентни анализи, в съответствие с променящия се характер на текущите заплахи за критична инфраструктура, особено в ключови сектори, подсектори и категории субекти, в съответствие с актуалните изменения в европейската и националната политики в тази област.

Основната цел на обучението е да се предоставят базови и разширени познания по създаване на предварителна организация за изграждане и управление на интелигентни системи за сигурност на критична инфраструктура, вкл. рамката за възможна интеграция между техните параметри и процесите на управление на непрекъснатостта на дейността на организацията, както и:

- изграждане на умения за прилагане на адекватен, според спецификата на мисията на съответната критична инфраструктура, подход за разработване на модел на интелигентна система за

сигурност;

- придобиване на практически умения за разработване на документи, свързани с проектирането и функционирането на ситемите за сигурност, осигуряването на сигурността и защитата на обекти от критичната инфраструктура.

Основните задачи на обучението са:

- изучаване на съвременни стандартизирани подходи при определяне на процесите, даващи входни данни за разработване на интелигентни системи за сигурност;
- извършване на анализ на възможната интеграция между параметрите на системите за сигурност и процесите на управление на непрекъснатостта на дейността за създаване на устойвост на критичната инфраструктура;
- запознаване с вариант на подход за разработване на модел на интелигентна система за сигурност и защита на критична инфраструктура;
- придобиване на практически умения за обучение, тестване и разработване на изисквания за проектиране на системи за физическа защита;
- придобиване на практически умения за разработване на базова структура на бизнес модел за управление на научните изследвания в обхвата на интелигентни системи за сигурност на критична инфраструктура;
- придобиване на знания в областта на научните изследвания за повишаване на устойчивостта на критичната инфраструктура, при отчитане на съответните рискове, особено каскадните ефекти, които са от решаващо значение за поддържането на жизненоважни обществени и икономически функции, обществената безопасност и сигурност, здравето на населението или околната среда.

II. СЪДЪРЖАНИЕ

№	ТЕМА	БРОЙ ЧАСОВЕ	ОТ ТЯХ	
			ТЕОРИЯ	ПРАК-ТИКА
1.	**Стандартизирани особености, при определяне на процесите/етапите, даващи входни данни за разработване на интелигентни системи за сигурност**	2	2	
2.	**Устойчивост на организацията**	3	3	
3.	**Рамка за възможна интеграция между параметрите на Интелигентните**	2	2	

№	ТЕМА	БРОЙ ЧАСОВЕ	ОТ ТЯХ	
			ТЕОРИЯ	ПРАК-ТИКА
	системи за сигурност и процесите на Управление на непрекъснатостта на дейността			
4.	**Възможен подход за разработване на модел на интелигентна система за сигурност** **Практически упражнения:** Обучение, тестване и разработване на изисквания за проектиране на системи за физическа защита	4	2	2
5.	**Оптимизиране на разработването на интелигентни системи за сигурност чрез прилагането на скалата за нивата на технологична готовност**	2	2	
6.	**Стандартизирани оперативни процедури за функциониране на ИСС** **Практически упражнения:** Разработване на вариант на СОП за функциониране на МИСС	5	3	2
7.	**Бизнес модел и профил на риска** **Практически упражнения:** Разработване на базова структура на бизнес модел за управление на научните изследвания в обхвата на ИСС	4	2	2
8.	**Вникване в профила на риска на организацията**	2	2	
9.	**Рамка на бизнес модела и на профила на риска.** **Практически упражнения:** 1. Разработване на вариант на Рамка на бизнес модела 2. Разработване на вариант на Рамка на профила на риска на бизнес модела	6	2	2 2
10.	**Ситуационна игра**	2		2
11.	**Изпит**	2	2	
	Общо:	**34**	**22**	**12**

III. ОСНОВНА ЛИТЕРАТУРА

1. Kiril Stoichev, Dimitar Dimitrov, Valeri Panevski. "VULNERABILITY ASSESSMENT OF SECURITY AND PROTECTION SYSTEMS", 2017, ISBN:978-619-90310-7-0, стр. 250;

2. Пъневски В. С., „ПОДОБРЯВАНЕ НА УПРАВЛЕНИЕТО НА НЕПРЕКЪСНАТОСТТА НА ДЕЙНОСТТА НА КРИТИЧНА ИНФРАСТРУКТУРА ЧРЕЗ ОПТИМИЗИРАНЕ НА ФУНКЦИОНАЛНОСТТА НА СИСТЕМИТЕ ЗА ФИЗИЧЕСКА ЗАЩИТА", 1, Издателство на БАН „Проф. Марин Дринов", 2020, ISBN:978-619-245-026-7, стр. 192;

3. Георгиев Нколай Личков, Пъневски В. С., „Възможен подход за създаване на сигурност на организации от националните ведомства и националната критична инфраструктура". 1, ИМСТЦХА-БАН, 2021, ISBN:978-619-7466-08-9, стр. 240;

4. ISO 22313:2020 Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301;

5. ISO 22316:2017 - Security and resilience — Organizational resilience — Principles and attributes;

6. ISO/TS 22317:2021 Security and resilience — Business continuity management systems — Guidelines for business impact analysis;

7. ISO 31000:2018; Risk management — Guidelines;

8. IEC 31010:2019; Risk management — Risk assessment techniques;

9. Директива 2008/114/ЕО на Съвета, от 8 декември 2008 година, относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита;

10. ПРЕПОРЪКА НА СЪВЕТА, от 8 декември 2022 година, относно координиран подход на равнището на Съюза за укрепване на устойчивостта на критичната инфраструктура (2023/С 20/01);

11. ДИРЕКТИВА (ЕС) 2022/2557 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА, от 14 декември 2022 година, за устойчивостта на критичните субекти.

СЪСТАВИЛ ПЛАНА:

Доцент д-р Валери Пъневски
Assoc. Professor Valeri Panevski, PhD
"Technologies and systems for protection",
IMSETHC – BAS
Tel.: + 359 2 46 26 283
Fax: + 359 2 46 26 202