



Утвърдил:
Декан (проф. дпсн Соня Карабелова)
Дата

СОФИЙСКИ УНИВЕРСИТЕТ "СВ. КЛИМЕНТ ОХРИДСКИ"

Факултет: Философски

Специалност: (код и наименование)

Ф	Ф	А	2	0	0	2	2	6
---	---	---	---	---	---	---	---	---

МП Публично управление с изкуствен интелект, з.ф.о.

УЧЕБНА ПРОГРАМА

Дисциплина: 3 0 0 7

КИБЕРУСТОЙЧИВОСТ И ЗАЩИТА НА ДАННИ

Преподавател: гл. ас. д-р Деница Хинкова

Учебна заетост	Форма	Хорариум
Аудиторна заетост	Лекции	30
	Семинарни упражнения	0
	Практически упражнения (хоспетиране)	0
Обща аудиторна заетост		30
Извънаудиторна заетост	Реферат	-
	Доклад/Презентация	20
	Научно есе	-
	Курсов учебен проект	-
	Учебна екскурзия	20
	Самостоятелна работа в библиотека или с ресурси	20
Обща извънаудиторна заетост		60
ОБЩА ЗАЕТОСТ		90
Кредити аудиторна заетост		1
Кредити извънаудиторна заетост		2
ОБЩО ЕКСТ		3

№	Формиране на оценката по дисциплината	% от оценката
1.	Workshops {информационно търсене и колективно обсъждане на доклади и реферати)	10%
2.	Участие в тематични дискусии в часовете	10%
3.	Демонстрационни занятия	-
4.	Посещения на обекти	10%
5.	Портфолио	10%
6.	Тестова проверка	-
7.	Решаване на казуси	10%
8.	Текуща самостоятелна работа /контролно	-
9.	Изпит	50%

Анотация на учебната дисциплина:

Киберустойчивостта се интерпретира като адаптивен управленски модел, при който критичният въпрос не е единствено предотвратяването на атаки, а способността на системите да функционират, да се възстановяват и да се адаптират в условия на компрометирана дигитална среда. Този модел позиционира киберустойчивостта като

междусекторен управленски проблем, който обединява технологии, институции, етика и обществено доверие.

Дисциплината интегрира три взаимосвързани аналитични измерения:

- *технологично измерение – киберсигурност, защита на данни и устойчивост на инфраструктури;*
- *интелигентно измерение – приложение на изкуствен интелект за откриване, анализ и реакция на заплахи;*
- *управленско измерение – публични политики, управление на риска и институционална устойчивост.*

В контекста на европейската регулаторна рамка (NIS2, GDPR и AI Act) и нарастващата сложност на киберзаплахите, киберустойчивостта се утвърждава като ключов фактор за сигурна дигитална трансформация и защита на критичната инфраструктура.

Курсът поставя акцент върху прехода от логика на превенция – „как да предотвратим атака“, към логика на устойчивост – „как да продължим да функционираме въпреки нея“, при който стратегическата цел е поддържане на работоспособността на публичните системи при инциденти, а не единствено тяхното избягване.

Основна цел на дисциплината е изграждането на аналитичен и практически ориентиран капацитет за прилагане на политики, модели и добри практики от ЕС, САЩ и Азия за управление на киберрискове, защита на данни и устойчивост на дигитални публични системи.

Обучението е интерактивно и включва:

- тренинги, симулации и модели за киберустойчивост;
- анализ на реални казуси от публичния сектор;
- разработване на политики и стратегии за дигитална устойчивост.

Студентите развиват способности да мислят и действат като:

- стратегически анализатори;
- експерти по киберустойчивост;
- архитекти на дигитална сигурност.

Крайната цел на дисциплината е подготовка на специалисти, които не само да защитават информационни системи, а изграждат устойчиви публични институции, способни да функционират ефективно в среда на постоянна несигурност и системни цифрови рискове.

Предварителни изисквания:

Публичен мениджмънт; Изкуствен интелект в публичното управление.

Очаквани резултати:

Дисциплината цели да формира специалисти, способни да анализират, проектират и управляват киберустойчиви публични системи чрез интеграция на технологични решения, политики и механизми за управление на риска. Курсът е насочен към развиване на практически умения за готовност и аналитични способности за: превенция и управление на киберинциденти; осигуряване на непрекъсваемост на публични услуги; защита на лични и институционални данни; изграждане на доверие в дигиталната държава. Дисциплината подготвя студентите за участие в управлението на киберсигурността в публичната администрация и изграждане на кибер-устойчивост в динамична среда.

След завършване студентите ще могат да:

- разработват политики за киберустойчивост на национално ниво
- интегрират изкуствен интелект в публични политики и системи
- прилагат международни стандарти (NIST CSF, ISO/IEC 27001, GDPR)
- проектират системи за управление на киберрискове
- оценяват алгоритмичен и системен риск
- управляват киберинциденти и кризи
- осигуряват непрекъсваемост на публични услуги
- прилагат принципи на прозрачност, отчетност и етичност в AI системи

• вземат решения в условия на висока несигурност Дипломираните магистри ще могат да заемат позиции като: • Експерт по киберустойчивост в публичния сектор • Data Protection Officer • AI Governance експерт • Анализатор в CERT/CSIRT • Съветник по дигитални политики.
--

Учебно съдържание

№	Тема:	Хорариум
1	Основи на киберустойчивостта като публична политика ▪ Киберсигурност vs. киберустойчивост: от защита към адаптивност ▪ Киберпространството като ново поле на публично управление ▪ Критична инфраструктура в дигиталната епоха (енергетика, здравеопазване, e-government) ▪ Въведение в системния риск и събития „черен лебед“ събития ▪ Казус: глобални кибератаки срещу държави (Естония, Иран, Украйна, SolarWinds)	2 ч.
2	Управление на риска, политики и киберустойчивост ▪ Киберустойчивост като част от държавния капацитет (state capacity) ▪ Управление на кибер-риска в публичната сфера: как държавите управляват несигурността ▪ Рамки и стандарти (NIST, ISO 27001) - не като техника, а като инструмент на политиките ▪ Доверие, легитимност и политическа цена на кибер-инцидентите ▪ Управление на неопределеността: как се вземат решения при кризи	2 ч.
3	Искусствен интелект и киберустойчивост • Машинно обучение (Machine Learning) в реална среда (не теория, а приложения) • AI за откриване на аномалии в публични системи • Интелигентни SOC (Security Operations Centers) • <i>Предвиждане в управлението и използване на AI за прогнозиране на риск</i> • <i>Автоматизация vs. контрол: къде остава човекът?</i>	2 ч.
4.	AI-базирани заплахи и генеративен AI • Generative AI като инструмент за атаки (deepfakes, phishing, automation) • Как алгоритмите могат да бъдат „манипулирани“ • AI като риск за демокрацията и публичното управление • Казус: Дезинформационни кампани чрез AI кампании • Защитни стратегии срещу AI-базирани атаки	2 ч.
5.	Киберкризи и управление на инциденти • Кризисно управление с AI: кой взема решения? Рамка за отговор на кибер-инциденти (NIST, EU) • <i>Координация между институции (whole-of-government)</i> • <i>Симулация: реакция при атака срещу държавна система</i>	2 ч.
6.	Хибридни заплахи и дезинформация • Кибератаки + информационна война • Дезинформация като инструмент за дестабилизация • Социални мрежи като поле на киберконфликт • <i>Влияние върху избори и публични политики</i>	2 ч.

	Киберустойчивост срещу когнитивни атаки	
7.	Европейски политики и дигитален суверенитет - EU Cybersecurity Strategy и Digital Decade - Дигитален суверенитет: защо е важен? - Регулации: GDPR, AI Act - Cloud и данни като стратегически ресурс - Ролята на ЕС в глобалната киберсигурност <i>Казус: Добри практики и примери за стратегии от ЕС.</i> <i>Дискусия върху EU Cybersecurity Strategy</i>	2 ч.
8.	Непрекъсваемост на публичните услуги (continuity) - Disaster recovery за държавни системи „Fail-safe“ vs. „Fail-resilient“ модели <i>Как държавата функционира при срив на системи</i> <i>Вградена устойчивост</i>	2 ч.
9.	Киберустойчивост на сложни системи - Системно мислене при системи-от-системи - Ключови уязвимости <i>Взаимозависимости между публични системи</i> <i>Каскада на провалите (ефект на доминото)</i>	2 ч.
10.	Защита на данните и AI governance - Управление на данни в публичния сектор - Дилеми на сигурността: Сигурност vs. неприкосновеност и свобода <i>Алгоритмична отчетност и прозрачност</i> <i>Етика и превенция на дискриминацията в AI системи</i>	2 ч.
11.	Публична администрация в дигитална среда - Дигитално управление и киберсигурност, - Ролята на администрацията като системен интегратор <i>Управление на дигитална трансформация</i> <i>Капацитет за киберустойчивост в публичния сектор</i>	2 ч.
12.	Култура на сигурност и организационно учене - Човешкия фактор в киберсигурността - Организационно учене след кризи <i>Културата за сигурност като стратегически ресурс</i>	2 ч.
13.	Иновации и бъдеще на киберустойчивостта - AI + Quantum computing рискове - Autonomous systems и сигурност <i>Smart cities и нови уязвимости</i> <i>Future scenarios: как изглежда киберсигурността след 10 г.</i>	2 ч.
14.	Практически модул: симулации и policy lab - Симулация на кибератака срещу държавна институция - Python/AI лаборатории <i>Работа в екипи: реакция, комуникация, решения</i> <i>Презентации и защита на стратегии</i>	2 ч.
15.	Интеграция и стратегическо мислене - Свързване на технологии, политики и управление <i>Разработване на цялостна стратегия за киберустойчивост</i> <i>Подготовка за изпит и проект</i>	2 ч.

Конспект за изпит

№	Въпрос
1.	Киберустойчивостта като елемент на държавния капацитет.
2.	Управление на кибер-рискове в публичния сектор.
3.	Европейски политики за киберсигурност.

4.	Критична инфраструктура и устойчивост.
5.	Ролята на AI в киберсигурността и защита при хибридни заплахи.

Библиография

Основна:

1. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
2. Stevens, T. (2016). *Cyber security and the politics of time*. Cambridge University Press.
3. Clarke, R. A., & Knake, R. K. (2019). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Press.
4. Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.
5. Shackelford, S. J. (2014). *Managing cyber attacks in international law, business, and relations: In search of cyber peace*. Cambridge University Press.

Допълнителна:

1. Stevens, T. (2016). *Cyber security and the politics of time*. Cambridge University Press.
2. Taleb, N. N. (2007). *The black swan: The impact of the highly improbable*. Random House.
3. Sikos, L. F. (2021). *Artificial Intelligence in Cybersecurity*. Springer.
4. Chio, C., & Freeman, D. (2018). *Machine learning and security: Protecting systems with data and algorithms*. O'Reilly Media.
5. Слатински, Н. (2017). *Киберсигурност*. София: Военно издателство.

Дата: 15.04.2026 г.

Съставил: гл.ас. д-р Деница Хинкова