БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ПО МАТЕМАТИКА И ИНФОРМАТИКА

Утвърдил:
(акад. В. Дренски, Директор на ИМИ-БАН)

Учебна програма
за специализиран докторантски курс

Област на висше образование:	4. Природни науки, математика и информатика
професионално направление:	4.6. Информатика и компютърни науки
докторска програма:	Информатика
тема:	Аспекти на киберсигурност в системи за управление на учебно съдържание
лектор:	Проф. д-р Радослав Даков Йошинов
данни за връзка с лектора (тел., имейл)	+3598888627190, yoshinov@cc.bas.bg
хорариум:	30 часа лекции
кредити съгл. кредитната система на ЦО на БАН:	20

1. Анотация

Учебният курс цели запознаване с аспекти на киберсигурност в системи за управление на учебно съдържание. Курсът представя различни подходи за установяване на потребителската идентичност, когато това не е възможно да се случи пряко – при директен контакт с потребителя. Разглеждат се възможностите за осигуряване на сигурност на данните, с помощта на различни видове кодиране и криптографски алгоритми. Поставя се акцент върху управлението на автентикацията и авторизацията на потребителите, възможните атаки срещу системната архитектура от злонамерени деятели, както и начините за превенция и осигуряване на максимална сигурност.

2. Необходими предварителни знания

Базови познания по системна и мрежова администрация
Задълбочено познаване на HTTP протокола

3. Компетентности, придобити в резултат на обучението

Знания за киберсигурността в системите за управление на учебно съдържание. След завършване на курса докторантите се очаква да могат:

- Да оценяват нивото на защита на данните, използвани от една система
- Да създават подходящи системни архитектури, които да осигуряват максимална гъвкавост и възможности за скалиране на решенията за авторизация и автентикация в системите за управление на учебно съдържание
- Да избират подходящи подходи за установяване на потребителска идентичност във виртуална среда
- Да разбират различни криптографски алгоритми
- Да проектират системни архитектури, осигуряващи висока сигурност на данните и правилна работа на системата

4. Тематично съдържание

Тема	брой часове лекции
Системи за управление на обучение (СУО) и система за управление на учебно съдържание (СУУС)	4
Учебен обект	2
Потребителска идентичност – значение и начини за дистанционно установяване във виртуална среда	3
Релационни и нерелационни бази данни – възможности за защита на данните	3
Услуги за авторирация и автентикация на потребителите	2
Видове криптографски алгоритми	2
Хеширане на данни	3
JSON Web Token (JWT)	1
Видове атаки срещу уеб базирани приложения	2
Публични и частни ключове	2
Принципи на мрежовата и системна администрация и осигуряване на защита на системните архитектури	1
Критични инфраструктури	3
Социално инженерство – методи за компрометиране на сигурността на потребителите без реална атака на данните	2

5. Конспект

1. Възможности и начини за реализация на установяване на идентичност на потребителя на системи за управление за учебно съдържание
2. Възможности за съхранение на потребителски данни за автентикация
3. Управление на автентикацията и авторизацията – външно и вътрешно за системата
4. Криптография
5. Сигурност на данните
6. Обществена сигурност
7. Организационна сигурност
8. Социално инженерство
9. Разпределени изчисления и сигурност
10. Критична инфраструктура
11. Публични и частни ключове
12. Мрежова сигурност
13. Защитни стени
14. Виртуализация
15. JWT
16. Тунелиране
17. DoS атаки
18. Инжекции – SQL, HTML
19. Web Exploit
20. Cross Site Scripting

6. Препоръчана литература:

1. Berkouwer, S. (2019). Active Directory Administration Cookbook: Actionable, proven solutions to identity management and authentication on servers and in the cloud . Packt Publishing.
2. Erl, T. (2016). Service-Oriented Architecture: Analysis and Design for Services and Microservices (The Pearson Service Technology Series from Thomas Erl). Prentice Hall; 2 edition.
3. Kabamba, P. (2019). Know Your Customer (KYC) Policy: The Bank's Account Opening Procedures, Identity Verification Procedures and Customer Risk Assessment Procedures.
4. Meier, A., & Kaufmann, M. (2019). SQL & NoSQL Databases: Models, Languages, Consistency Options and Architectures for Big Data Management. Springer Vieweg; 1st ed. 2019 edition.

5. Paar, C., Pelzl, J., & Preneel, B. (2009). Understanding Cryptography: A Textbook for Students and Practitioners. Springer; 1st ed. 2010 edition.
6. R. Graziani, A. Johnson. Routing protocols and concepts. Indianapolis, IN 46240 USA, Cisco Press, 2008.
7. M. Conde-Gonza´lez, F. Garc´ıa-Pen˜alvo, M. Guerrero, M. Forment. Adapting LMS architecture to the SOA: an Architectural Approach., 322–327, 10.1109/ICIW.2009.54, 2009.
8. K. El-Khatib, L. Korba, Y. Xu, G. Yee. Privacy and Security in E-Learning. International Journal of Distance Education Technologies 1, 4 (2003), 1–19, doi: 10.4018/jdet.2003100101.
9. Baier, T. Bernoulli, T. Braun, C. Graf, U. Ultes-Nitsche. Case Study of the Us- age of an Authentication and Authorization Infrastructure (AAI) in an E-Learning Project. Proceedings of the ISSA 2006 from Insight to Foresight Conference, 5–7 July 2006, Sandton, South Africa, 10 pp.
10. R. Vasiu, A. Ternauciuc, M. Onita, Bogdan Dragulescu. Single Sign-On Solutions for Moodle. Conference proceedings of "eLearning and Software for Education", issue:01, 2009, 217-224.
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eurlex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679, Accessed 2019-06-27.
12. D. Amo et al. GDPR security and confidentiality compliance in LMS' a problem analysis and engineering proposal. A: International Conference on Technological Ecosystems for En- hancing Multiculturality. TEEM'19: Proceedings of the Seventh International Conference on Technological Ecosystems for Enhancing Multiculturality: Le´on, Spain, October 16–18, 2019. New York: Association for Computing Machinery (ACM), 2019, 253–259.

7. Ресурсно осигуряване на обучението:

Не е предвидено специализирано ресурсно осигуряване.

8. Критерии за оценка

Изпитът се състои от две части – писмен и устен.
На писмения изпит докторантът развива своите идеи и концепции по два въпроса от конспекта.
На устния изпит докторантът отговаря на зададени от журито въпроси, свързани с темата на курса.

Крайната оценка е от 2 до 6 (с точност до 0.5).
Тя се формира на базата на следното съответствие:

Отличен (6)	Мн. добър (5)	Добър (4)	Среден (3)	Слаб (2)
Отлично владее материала. Изложението е изчерпателно, последователно, компетентно, логично и хармонично. Правилно обосновава предлаганите решения, знае как да обобщава и излага материала без да прави грешки. Притежава необходимите умения за изпълнение на практически задачи.	Познава материала. Излага го правилно без да допуска съществени неточности. Може правилно да прилага теоретични принципи и притежава необходимите умения за изпълнение на практически задачи.	Владее голяма част материала, но допуска неточности при изложението и отговорите на въпросите. Има известни неясноти при опитите за прилагане на материала в практически ситуации.	Владее само част от материала, но се затруднява в отделните детайли. Допуска неточности във формулировките и нарушава последователността при представянето на материал. Има затруднения при изпълнение на практически задачи.	Не познава значителна част от материала, допуска съществени грешки и с големи трудности изпълнява практически задачи.

Учебната програма е обсъдена и одобрена на заседание на секция „Математическа лингвистика“ на 28.02.2020.

Ръководител секция:
(доц. д-р Десислава Панева-Маринова)

Учебната програма е разгледана от Директорския съвет на ИМИ-БАН
на 12.03.2020 г. (протокол № 10).

Учебната програма е приета от Научния съвет на ИМИ-БАН
на 13.03.2020 г. (протокол № 4).