

УНИВЕРСИТЕТ
ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

ФАКУЛТЕТ „ИНФОРМАЦИОННИ НАУКИ“

УТВЪРЖДАВАМ,

РЕКТОР:

/проф. д.н. Ирена Петева /

К О Н С П Е К Т

за ДЪР ЖАВЕН ИЗПИТ

**за специалност “ИНФОРМАЦИОННА СИГУРНОСТ”, ОКС „бакалавър”
за учебната 2021/2022 г.**

1. Информационна сигурност: базови понятия и определения.
2. Хакерски и антихакерски технологии.
3. Технологични аспекти на сигурността
4. Управление на процеси и проекти в ИТ среда
5. Същност и съдържание на стандартите за информационна сигурност (общо описание).
6. Предназначение и основни функции на операционните системи.
7. Основните изисквания за конфиденциалност, цялостност и достъпност на данните в киберсигурността. Видове кибер заплахи. Уязвимости в уеб приложенията според OWASP (Open Web Application Security Project). Модел за развитие на кибератака. Социален инженеринг.
8. Сигурност в крайната точка. Модели за контрол на достъпа в операционните системи. Защитни механизми в операционните системи. Конфигуриране на защитата на операционните системи. Необходимост от ъпдейти. Видове ъпдейти. Система за управление на ъпдейтите. Процеси при управление на ъпдейтите. Рискове при внедряване на ъпдейти.
9. Сигурност в мрежата. Инфраструктурни мрежови услуги NTP (Network Time Protocol), ARP (Address resolution Protocol), DHCP (Dinamic Host Configuration Protocol). Контрол на достъпа до мрежата. Периметрова сигурност чрез защитни стени (firewall) и системи за откриване на проникване (IDS, Intrusion Detection Systems).
10. Сигурност по дизайн. Жизнен цикъл на софтуера. Сигурност по дизайн през SDLC (Software Development Life Cycle). Тестване на сигурността на приложенията и сигурност през STLC (Software Testing Life Cycle). Видове уязвимости в софтуерните приложения. Начини за намаляване на риска от атаки срещу софтуерните приложения.

11. Основни понятия и принципи за защита. Видове защиты.
12. Системи за откриване на нарушения (IDS): предназначение, обхват и функции, архитектури.
13. Системи за предотвратяване на нарушения (IPS): предназначение, обхват и функции, архитектури.
14. Класификация на криптографските системи.
15. Криптография с публични ключове.
16. Видове комуникационни системи и мрежи.
17. Въведение и основни понятия в компютърните мрежи и комуникации.
18. Класификация на компютърните мрежи.
19. Мрежови концепции, модели и стандарти.
20. Сравнение на мрежовите архитектури.
21. Видове компютърни мрежи. Връзка между LAN и WAN. Основни архитектурни решения.
22. Виртуални частни мрежи. Протоколи. Типове VPN.
23. Технически канали за неоторизиран информационен достъп.
24. Технически средства за защита на информацията.
25. Основни дефиниции и направления в интелигентните системи за информационна сигурност.
26. Основни форми за представяне на знания.
27. Дескриптивни логики за създаване на агенти – семантични ризъньори.
28. Интелигентни приложения в системи за откриване на нарушения и системи за предотвратяване на нарушения (IDS и IPS).

Литература

1. Web Service Modeling Ontology <http://www.wsmo.org/> to date
2. Йоцов, В. Изкуствен интелект и експертни системи. София: За буквите о писменехъ, 2014. - 248 с.
3. The power of AI, VR and AR. // <https://towardsdatascience.com/the-power-of-artificial-intelligence-ai-virtual-and-augmented-reality-vr-and-ar-on-medical-4949c7a6fd72> to date
4. Applying Artificial Intelligence to Virtual Reality: Intelligent Virtual Environments. // https://www.researchgate.net/publication/2329214_Applying_Artificial_Intelligence_to_Virtual_Reality_Intelligent_Virtual_Environments to date
5. Semantic Web. // <http://roamingpanda.wordpress.com/~category/tech/semantic-web/> to date

УНИВЕРСИТЕТ
ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

ФАКУЛТЕТ „ИНФОРМАЦИОННИ НАУКИ“

6. Semantic Web Reasoner. // <http://semanticweb.org/wiki/-Category:Reasoner> to date
7. Simulation of Ant Colony Optimization. // <http://www.djoh.net/inde/ANTColony/applet.html> to date
8. <http://www.energycentral.com/c/ua/design-thinking-and-data-sciences-lethal-combination-making>
9. <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>
10. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-27ra.pdf>
11. Security_by_Design_Principles // [https://www.owasp.org/index.php/Security by Design Principles](https://www.owasp.org/index.php/Security_by_Design_Principles)
12. SAS Enterprise Miner // <https://www.SAS.com>
13. Йоцов, В. Логическо програмиране. София: За буквите о писменехъ, 2014. - 168 с.
14. Йоцов, В. Сигурност и защита на информацията. София: За буквите о писменехъ, 2006. - 156 с.
15. Fensel, D. Ontologies: A silver bullet for knowledge management and electronic commerce. Springer, 2005, 163 p.
16. Web Service Modeling Ontology // <http://www.wsmo.org/> to date
17. OWL-S: Semantic Markup for Web Services // <http://www.daml.org/services/owl-s/1.1> to date
18. Ontology Web Language for Services (OWL-S), a guide by Carnegie Mellon University. // Available at: www.sei.cmu.edu/isis/guide/technologies/owl-s.htm to date
19. Protégé // www.stanford.edu/protege to date
20. The official web page about XML // <http://www.w3c.org> to date
21. Resource Description Framework // <http://www.w3c.org/Metadata> to date
22. Йоцов, В. Интелигентни системи за информационна сигурност. София: За буквите о писменехъ, 2010. - 280 с.
23. Artificial Intelligence and Emerging Technologies in Schools. // https://docs.education.gov.au/system/files/doc/other/aiet_final_report_august_2019.pdf to date

Конспектът е приет на катедрено заседание с Протокол № 11 от 20.09.2021 г.

Ръководител на катедра
“Информационни системи и технологии”

/проф. д.н. Иван Гарванов/

20.09.2021 г.