ЮЗУ „Неофит Рилски

Правно - исторически факултет

2700 Благоевград, пл. „Георги Измирлиев - Македончето"

тел./факс: 073/88 66 17; e- mail : admin@law.swu.bg

Конспект

по „**Киберразузнаване и дигитални доказателства“**

Магистри „МКЗЛД“

1. Същност, цели и задачи на киберразузнаването
2. Актьори, заплахи и среда в киберпространството: държавни и недържавни субекти
3. Методи и източници на киберразузнавателна информация: OSINT, SIGINT, HUMINT в дигитален контекст
4. Кибершпионаж и контраразузнаване в условията на дигитална среда
5. Информационни операции, кибервойна и хибридни заплахи
6. Анализ и оценка на заплахи чрез индикатори за компрометиране
7. Правна и етична рамка на киберразузнавателната дейност: международни и национални норми
8. Криптография и стеганография: приложение в киберразузнаването и разкриването на скрита информация
9. Същност и класификация на дигиталните доказателства. Видове носители и източници

10. Събиране и извличане на дигитални доказателства: методи, инструменти и добри практики
11. Форензика на информационни системи, мобилни устройства и мрежови среди
12. Верига на съхранение (chain of custody) и допустимост на цифрови доказателства в съдебната практика
13. Анализ на цифрови следи: логове, метаданни, зловреден софтуер и аномалии в трафика
14. Инструменти и платформи за разследване на киберпрестъпления (Kali Linux, Autopsy, Wireshark, др.)
15. Симулационни сценарии и практически казуси: разследване на киберинциденти и изграждане на доказателствена логика

ЛИТЕРАТУРА

- Clarke, R. A., & Knake, R. K. (2012). Cyber War: The Next Threat to National Security and What to Do About It. Ecco.
- Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.
- Casey, E. (Ed.). (2020). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (4th ed.). Academic Press.
- Vacca, J. R. (2014). Computer and Information Security Handbook (3rd ed.). Morgan Kaufmann.
- Tikk, E., Kaska, K., & Vihul, L. (2010). International Cyber Norms: Legal, Policy and Industry Perspectives. NATO Cooperative Cyber Defence Centre of Excellence.
- Lyon, D. (2019). Surveillance Society: Monitoring Everyday Life. Open University Press.
- NATO CCDCOE. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
- Shackleford, S. J. (2014). Managing Cyber Attacks in International Law, Business, and Relations. Cambridge University Press.
- Geers, K. (Ed.). (2011). Cyber War in Perspective: Russian Aggression against Ukraine. NATO CCDCOE.
- Lemos, R. (2018). Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents. Apress.
- Hiller, J. S., & Russell, R. S. (2019). Privacy in the Age of Big Data (2nd ed.). Rowman & Littlefield.
- Sammons, J. (2015). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics (2nd ed.). Syngress.

- Boddington, P. (2017). Towards a Code of Ethics for Artificial Intelligence. Springer.
- Bejtlich, R. (2013). The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press.
- West, J. & Bhattacharya, M. (2016). Intelligence and National Security: A Reference Handbook. ABC-CLIO.
- Bowen, M. & Hash, J. (2006). Information Security Handbook: A Guide for Managers. NIST Special Publication.
- Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence.
- Baggili, I., & Breitinger, F. (2019). Digital Forensics: Threatscape and Best Practices. Elsevier.
- Grossman, L. (2016). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
- ISO/IEC 27037:2012. Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence.

Изготвил: гл. ас. д-р Владимир Бабанов

04. 14. 2025г.