Digitally signed by Technical Scientific Library, TUM
Reason: I attest to the accuracy and integrity of this document

UNIVERSITATEA TEHNICĂ A MOLDOVEI

FACULTATEA CALCULATOARE, INFORMATICĂ ȘI MICROELECTRONICĂ
DEPARTAMENTUL INGINERIA SOFTWARE ȘI AUTOMATICĂ

FUNDAMENTE ALE SECURITĂȚII CIBERNETICE

Suport de curs

EDITURA TEHNICA-UTM

2024

CZU 004.056(075.8)
A 40

Suportul de curs a fost discutat și aprobat pentru editare la ședința Consiliului Facultății Calculatoare, Informatică și Microelectronică, proces-verbal nr.1 din 30.08.2024.

Lucrarea va servi drept suport al cursului *Fundamente ale securității cibernetice* pentru masteranzii anului II, semestrul III, programul de studii *Tehnologia informației pentru afaceri*, Facultatea Calculatoare, Informatică și Microelectronică.

La finale cursului *Fundamente ale securității cibernetice* masteranzii trebuie să însușească conceptele-cheie și terminologia specifică domeniului de securitate cibernetică; să identifice amenințările la adresa securității cibernetice; să definească strategiile de identificare și remediere a vulnerabilităților din activele informaționale; să determine componentele sistemice (inclusiv personalul) necesare pentru un program de securitate cibernetică eficient.

Suportul de curs este secționat în 9 teme, în fiecare dintre care sunt specificate: preliminarii, scopul, obiectivele educaționale, finalitățile și metodele de evaluare, conținutul teoretic completat cu exemple relevante, întrebări pentru aprofundarea cunoștințelor.

Autor: lect. univ., dr. Arina Alexei

Recenzenți: prof. univ., dr. hab. Ion Bolun
conf. univ., dr. Viorica Sudacevschi

DESCRIEREA CIP A CAMEREI NAȚIONALE A CĂRȚII DIN RM

Alexei, Arina.

Fundamente ale securității cibernetice: Suport de curs / Arina Alexei; Universitatea Tehnică a Moldovei, Facultatea Calculatoare, Informatică şi Microelectronică, Departamentul Ingineria Software şi Automatică.
– Chişinău: Tehnica-UTM, 2024. – 176 p.: fig., tab.
Aut. indicat pe verso f. de tit. – Bibliogr.: p. 173-176 (33 tit.). – 30 ex.

ISBN 978-9975-64-464-8.

© UTM, 2024

CUPRINS

INTRODUCERE

În contextul dezvoltării rapide a tehnologiilor informaționale și a dependenței tot mai mari de mediul cibernetic pentru desfășurarea activităților economice, sociale și guvernamentale, securitatea cibernetică a devenit o prioritate esențială.

În era digitalizării, protejarea informațiilor și a resurselor IT nu mai reprezintă doar o necesitate tehnică, ci un aspect critic pentru asigurarea continuității și integrității proceselor organizaționale.

Cursul *Fundamente ale securității cibernetice* oferă masteranzilor o înțelegere profundă a conceptelor-cheie și a terminologiei specifice domeniului, identificarea principalelor amenințări cibernetice, precum și definirea strategiilor de remediere a vulnerabilităților din infrastructura informațională. De asemenea, cursul explorează componentele esențiale ale unui program de securitate cibernetică eficient, inclusiv politica de securitate, tehnologii de protecție și managementul riscurilor.

Obiectivele cursului *Fundamente ale securității cibernetice* sunt:

- însușirea conceptelor-cheie și a terminologiei specifice domeniului de securitate cibernetică;
- identificarea amenințărilor la adresa securității cibernetice;
- definirea strategiilor de identificare și remediere a vulnerabilităților din activele informaționale;
- determinarea componentelor sistemice (inclusiv personalul) necesare pentru un program de securitate cibernetică eficient.

Prin structura sa, acest suport de curs este conceput pentru a ghida masteranzii în procesul de învățare prin obiective educaționale clare, conținut teoretic actualizat, exemple practice și studii de caz relevante. Astfel, masteranzii vor fi pregătiți să contribuie la dezvoltarea și implementarea unor strategii de securitate cibernetică robuste în cadrul organizațiilor în care vor activa.

BIBLIOGRAFIE

1. WIENER, N. 1948. Cybernetics; or control and communication in the animal and the machine. John Wiley.
2. ALEXEI, Ar., ALEXEI, An. The difference between cyber security vs information security. In: *Journal of Engineering Science*, Vol. XXIX, no. 4 (2022), pp. 72 – 83. DOI: https://doi.org/10.52326/jes.utm.2022.29(4).08.
3. Cybersecurity essentials course. CISCO 2023 version. Accessed: 02.03.2024. Available: https://www.netacad.com /courses/ cybersecurity/cybersecurity-essentials.
4. WHITMAN, M. E., MATTORD, H.J. 2021. Principles of Information Security. 7th ed. Cengage Learning, p. 658. ISBN: 9780357710777.
5. Cost of a Data Breach Report 2024. IBM Security, 2024 [citat 6.07.2024]. Disponibil: https://www.ibm.com/downloads /cas /3R8N1DZJ.
6. WHITMAN, M. E., MATTORD, H.J. 2016. Management of Information Security, 6th ed. Cengage, p.752. ISBN: 978-1-337-40571-3.
7. ALEXEI, Arina, ALEXEI, Anatolie. Analysis of IoT security issues used in Higher Education Institutions. In: *International Journal of Mathematics and Computer Research*, Vol. 09, No 5, 2021, pp. 2277-2286. ISSN: 2320-7167. DOI: https:// doi. org/10.47191/ijmcr/v9i5.01.
8. CIAMPA, Mark. 2022. CompTIA Security+. Guide to Network Security Fundamentals. Ed. Cengage Learning, p. 784. ISBN: 9780357424377.
9. ISO/IEC 27005: Information technology – Security techniques – Information security risk management. International Organization for Standardization. Geneva, Switzerland, 2018.
10. WILLS, Mike. 2020. The Official (ISC)2 SSCP CBK Reference. 5th ed. John Wiley & Sons, Inc. Indianapolis, Indiana. ISBN 1119874866.

11. SIKORSKI, Michael, HONIG, Andrew. 2012. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press, 1st edition, p. 800. ISBN: 9781593272906.
12. SEIDL, David. 2021. CompTIA Security+. Practice tests. Sybex; 2nd edition, p. 336. ISBN: 9781119735465.
13. BEAMAN, C., et al. Ransomware: Recent advances, analysis, challenges and future research directions. In: *Computer Security*, vol. 111, p. 102490, Dec. 2021. DOI: 10.1016/ j.cose.2021.102490.
14. MAURYA, A. K., et al. Ransomware Evolution, Target and Safety Measures. In: *International Journal of Computer Sciences and Engineering*, vol. 6, no. 1, Jan. 2018, doi: 10.26438/ijcse/v6i1.8085.
15. ALEXEI, An., ALEXEI, Ar. The problem of information systems security in SME. In: *CEEeGov: Central and Eastern European eDem and eGov Days*, Budapest, Hungary, September 2023. ACM, New York, NY, USA, 6 Pages. DOI: https://doi.org/10.1145/3603304. 3603346.
16. ALEXEI, A. Network Security Threats to Higher Education Institutions. In: *CEE e|Dem and e|Gov Days*, Budapest, May 2021, pp. 323–333. doi: 10.24989/ocg.v341.24.
17. ELIYAN, L. F., PIETRO, R. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. In: *Future Generation Computer Systems*, vol. 122, pp. 149–171, Sep. 2021. DOI: 10.1016/j.future.2021.03.011.
18. PRABADEVI, B., JEYANTHI, N. A Review on Various Sniffing Attacks and its Mitigation Techniques. In: *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 3, p. 1117, Dec. 2018. DOI: 10.11591/ ijeecs.v12.i3. pp1117-1125.

19. JAVEED, D., BADAMASI, U.M. Man in the Middle Attacks: Analysis, Motivation and Prevention. In: *International Journal of Computer Networks and Communications Security*, vol. 8, no. 7, pp. 52–58, Jul. 2020. DOI: 10.47277/ IJCNCS/ 8(7)1.
20. RAMESH, P., BHASKARI, D. L. A Comprehensive Analysis of Spoofing. In: *International Journal of Advanced Computer Science and Applications*, vol. 1, no. 6, 2010. DOI: 10.14569 /IJACSA.2010.010623.
21. FRENZEL, L. E. Principles of Electronic Communication Systems. McGrawHill Education, 4th ed., 2016. ISBN: 978-0-07-337385-0.
22. THAKUR, K., PATHAN, A. Cybersecurity Fundamentals. CRC Press, 2020. DOI: 10.1201/9781003035626.
23. SAPALO SICATO, J. C., et al. VPN Filter Malware Analysis on Cyber Threat in Smart Home Network. In: *Applied Sciences*, vol. 9, no. 13, p. 2763, Jul. 2019. DOI: 10.3390/ app 9132763.
24. NAJJAR, M. Using Improved d-HMAC for Password Storage. In: *Computer and Information Science*, vol. 10, no. 3, p. 1, Jul. 2017. DOI: 10.5539/cis.v10n3p1.
25. ALEXEI, Arina. Indicații metodice la lucrările de laborator ”Tehnologii ale securității informaționale”. Editura UTM, Chișinău, 2024. ISBN 978-9975-64-448-8.
26. BOLUN, I., CIORBĂ, D., ZGUREANU, A., BULAI, R. Informatics security assessment in the Republic of Moldova. In: *Journal of Engineering Science*, vol. XXVII, no. 4, pp. 103–119, 2020. DOI:10.5281/zenodo.4288297. ISSN 2587-347.
27. ALEXEI, A. Cadrul Sistemic de Securitate a Comunicațiilor Electronice pentru Instituțiile de Învățământ Superior din Republica Moldova. UTM, Chișinău, 2023.

28. ISO/IEC 27001: INFORMATION SECURITY MANAGEMENT. International Organization for Standardization. Geneva, Switzerland, 2023. [citat 02.08.2024]. Disponibil: https: //www.iso.org/isoiec-27001-information-security.html.
29. ALSHAIKH, M., et al. Information Security Policy: A Management Practice Perspective. In: *Australasian Conference on Information Systems*, 2015.
30. ISMAIL, W. B., et al. A generic framework for information security policy development. In: 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI). 2017, pp. 1-6. DOI: 10.1109/EECSI. 2017.8239132.
31. ALEXEI, Arina. Ensuring Information Security in Public Organizations in the Republic of Moldova through the ISO 27001 Standard. In: *Journal of Social Sciences*, B+, Vol. IV, No 1, 2021, pp. 84-94. ISSN 2587-3490. DOI: https://doi.org/10.52326/jss. utm. 2021. 4(1).11.
32. HAUFE, K., et al. ISMS Core Processes: A Study. In: *Procedia Computer Science*. 2016, vol. 100, pp. 339–346. DOI: 10.1016/J.PROCS.2016.09.167.
33. ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary, "International Organization for Standardization," Geneva, Switzerland. Accessed: 05.08.2024. [Online]. Available: https://www.iso.org/standard/73906.html.

Redactor: E. Balan

Bun de tipar 17.09.24	Formatul hârtiei 60x84 1/16
Coli de tipar 11,0	Tirajul 30 ex.
Hârtie ofset. Tipar RISO	Comanda nr. 110

MD-2004, Chişinău, bd. Ştefan cel Mare şi Sfânt, 168, UTM
MD-2045, Chişinău, str. Studenţilor, 9/9, Editura „Tehnica-UTM"