Sylabus: Kybernetická bezpečnost BSS469

Místnost a čas: Út 10:00 - 11:40 U43

Přednášející: pracovníci Národního úřadu pro kybernetickou a informační bezpečnost

Kontakt: Mgr. Petr Martinek (p.martinek@nukib.cz)

Anotace

Kurz studentům poskytne úvodní seznámení s problematikou kybernetické bezpečnosti. Jednotlivé semináře se postupně věnují teoretickým, historickým, konceptuálním a částečně také technickým aspektům kybernetické bezpečnosti. Jeho nedílnou součástí je však i osvojení si základních bezpečnostních pravidel a digitální hygieny. Kurz bude rovněž průběžně doplňován praktickými ukázkami a případovými studiemi.

Po absolvování tohoto jednosemestrálního kurzu budou posluchači seznámeni se základní teorií kybernetické bezpečnosti, používanou odbornou terminologií, současným zajišťováním kybernetické bezpečnosti v České republice a ve světě, s historií kybernetických útoků a s jejich taxonomií a typologií, a charakterem útočníků a jejich motivacemi. Kurz se rovněž věnuje fenoménům jako je kybernetická válka a kybernetická špionáž, či roli nestátních aktérů v kyberprostoru a významu médií a internetu v dnešním světě. Získané znalosti poskytnou výchozí rámec pro analýzu současných i budoucích kybernetických hrozeb a rizik. Studenti budou schopni lépe porozumět současným výzvám kybernetické bezpečnosti a jejich dopadům na národní i mezinárodní bezpečnost. Specifikem kurzu je rovněž poskytnutí praktických informací z oblasti zajišťování kybernetické bezpečnosti v České republice díky přednášejícím, kterými budou primárně pracovníci NÚKIB. Dále budou dílčím způsobem, potažmo k prezentaci vybraných témat, přizváni odborníci z bezpečnostních složek či věcně příslušných orgánů, kteří danou problematiku přímo vykonávají nebo s ní mají praktickou zkušenost.

Hodnocení

Typ výuky, docházka, zkoušky a hodnocení

Výsledná známka bude sestavena z bodů získaných za závěrečné písemné přezkoušení (20b), seminární práci (20b), esej (10b), prezence na lekcích a aktivní účasti na simulaci kybernetického cvičení.

Seminární práce

Studenti si téma vyberou z vypsaných témat v IS MU. Ke každému tématu bude přiřazen maximální počet studentů, kteří jej mohou zpracovávat. Pokud by student chtěl zpracovávat jiné relevantní téma je možnost se domluvit s vedoucím předmětu Mgr. Petrem Martinkem (p.martinek@nukib.cz). Délka seminární práce je striktně 8 – 10 normostran. Je vyžadována práce s relevantní akademickou a aktuální literaturou. Hodnoceno bude jak obsahované zpracování tak právě využití adekvátní literatury. Maximální dosažitelný počet bodů je 20. Přihlašování k tématům bude možno od 12. 10. 2020. Případné změny tématu pak do 31. 10. 2020. **Termín odevzdání seminární práce je 15. 12. 2020.**

Esej

V rámci čtecího týdne je zadáno téma Informační válka. Pro dokázání přečtení povinné literatury studenti vypracují esej, která svým tématem navazuje na zadanou literaturu. Témata budou taktéž

vypsána v IS MU. Pokud by student chtěl zpracovávat jiné relevantní téma je možnost se domluvit s vedoucím předmět Mgr. Petrem Martinkem (p.martinek@nukib.cz). Délka eseje bude 4 – 6 normostran. Hodnocena bude věcná argumentace a vlastní vyhledávání další relevantní literatury k tématu. Maximální počet bodů je 10. Přihlašování k tématům je možno od začátku čtecího týdne tedy 17. 11. 2020. Případné změny tématu pak do 31. 11. 2020. **Termín odevzdání eseje je 31. 12. 2020.**

Kybernetické cvičení

V rámci poslední lekce proběhne kybernetické table-top cvičení. V rámci cvičení lze za aktivní účast získat až 3 bonusové body (nad rámec celkových bodů).

Závěrečné písemné přezkoušení

Závěrečné písemné přezkoušení bude mít elektronickou (online) podobu. Možnost skládat zkoušku bude navázána na vypsané termíny. Zkouška se bude skládat z 10 uzavřených otázek s více možnými odpověďmi (1 bod za otázku se všemi správnými odpověďmi) a jedné široce položené otevřené otázky za 10 bodů. Celkem tak bude možno za zkoušku získat 20 bodů.

Celkové hodnocení

Pro úspěšné hodnocení je třeba, aby student odevzdal seminární práci a esej v daných termínech a aby se zúčastnil zkoušky. Pokud bude některá z těchto náležitostí nenaplněna tak student nemůže předmět úspěšně ukončit a bude ohodnocen známkou X.

Hodnocení

50 – 46 b	A
45 – 41 b	B
40 – 36 b	C
38 – 34 b	D
33 – 30 b	E
29 a méně	F

OBSAH KURZU:

1. ÚVODNÍ HODINA – ORGANIZAČNÍ A FORMÁLNÍ NÁLEŽITOST - 06. 10. – (10:00 – 10:30 hod.)

PŘEDNÁŠEJÍCÍ: Mgr. Petr Martinek

- Požadavky a předpoklady
- Představení koncepce předmětu
- Seznámení s tématy seminárních prací
- Seznámení se s literaturou

Povinná četba:

SINGER, P.W. a Allan FRIEDMAN. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014. s. 34 – 67. Dostupné z: https://goo.gl/S5iF3C

2. KONCEPTUÁLNÍ ASPEKTY KYBERNETICKÉ BEZPEČNOSTI A ROLE STÁTU - 13. 10. (10:00–11:30 hod.)

PŘEDNÁŠEJÍCÍ: Mgr. et Mgr. Václav Borovička

- Úvod do kyberprostoru.
- Kybernetické útoky: základní terminologie a aktuální trendy.
- Co je kybernetická bezpečnost? Proč je kybernetická bezpečnost dnes tak významná?
- Konceptuální vymezení kybernetické bezpečnosti a kybernetické obrany
- Role a funkce státu v zajišťování kybernetické bezpečnosti
- Tvorba kybernetické bezpečnostní politiky

Povinná četba:

SINGER, P.W. a Allan FRIEDMAN. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014. s. 67 – 166. Dostupné z: https://goo.gl/S5iF3C

PAČKA, Roman. Role státu v zajišťování kybernetické bezpečnosti. Bezpečnostní teorie a praxe. Praha: Policejní akademie České republiky v Praze, 2015(3), s. 93 - 110.

Doporučená četba:

L. BAYUK, Jennifer, Jason HEALEY, Paul ROHMEYER, Marcus H. SACHS, Jeffrey SCHMIDT a Joseph WEISS. Cyber Security Policy Guidebook. Wiley, 2012, 288 s. ISBN 978-1-118-02780-6.

3. PRÁVNÍ ASPEKTY ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI V ČR - 20. 10. (10:00–11:30 hod.)

PŘEDNÁŠEJÍCÍ: Mgr. Petr Procházka

- Prameny práva kybernetické bezpečnosti (úvod do mezinárodních a vnitrostátních právních předpisů, které KB v ČR regulují)
- Zákon o kybernetické bezpečnosti (základní přehled systematiky a institutů ZKB se zaměřením na práva a povinnosti povinných osob a činnost NÚKIB a národního CERT)
- Zajišťování kybernetické bezpečnosti z hlediska jiných právních odvětví (další právní aspekty zajišťování KB ze strany NÚKIB a soukromých a veřejných subjektů, zejména CSIRT/CERT, PČR atd.)

Doporučená četba:

Národní úřad pro kybernetickou a informační bezpečnost, **podpůrné materiály.** Dostupné zde: https://www.govcert.cz/cs/regulace-a-kontrola/podpurne-materialy/

POLČÁK, Radim. a kol. **Právo informačních technologií**. 1. vyd. Praha: Wolters Kluwer, 2018. 656 s. ISBN 978-80-7598-045-8. **Kapitola 11 Kyberkriminalita a 12 Kybernetická bezpečnost**

POLČÁK, Radim. HARAŠTA, Jakub. STUPKA, Václav. **Právní problémy kybernetické bezpečnosti**. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2016. 215 s. ISBN 978-80-210-8426-1.

Dostupné zde: https://science.law.muni.cz/knihy/monografie/Polcak_Kyberneticka_bezpecnost.pdf

KOLOUCH, Jan. BAŠTA, Pavel. a kol. **Cybersecurity.** 1. vyd. Praha: CZ.NIC, z. s. p. o., 2019. 562 s. ISBN 978-80-88168-34-8.Dostupné zde: https ://knihy.nic.cz/files/edice/cybersecurity.pdf

4. ČÍNA V KYBERPROSTORU - 27. 10. (10:00–11:30 hod.)

PŘEDNÁŠEJÍCÍ: Mgr. Michal Thim

- Úvod: Strategická úloha kyberprostoru v domácí a zahraniční politice ČLR
- Domácí politika: Internet a vláda jedné strany
- Zahraniční politika: alternativní správa Internetu
- Kyberprostor a vojensko-civilní fúze: role čínských ICT firem
- Kybernetická špionáž: pokračující a pokročilá hrozba

Povinná četba:

Alex Joske. 2020. The party speaks for you. ASPI. https://www.aspi.org.au/index.php/report/party-speaks-you

ASPI. 2019. Mapping more of China's tech giants: AI and surveillance. https://www.aspi.org.au/report/mapping-more-chinas-tech-giants

Alex Joske. 2019. The China Defence Universities Tracker. ASPI.
https://www.aspi.org.au/report/china-defence-universities-tracker

ThreatConnect. 2015. Project CameraShy: Closing the Aperture on China's Unit 78020.
https://threatconnect.com/camerashy/ (po registraci)

Mandiant. 2011. APT1: Exposing One of China's Cyber Espionage Units.
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Intrusion Truth. https://intrusiontruth.wordpress.com/

U.S. Department of Justice. 2018. Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

5. RUSKO V KYBERPROSTORU – 03. 11. (10:00 – 11:30 hod.)

PŘEDNÁŠEJÍCÍ: Mgr. Michael Myklín

- Kybernetické útoky jako součást ruského pojetí války
- Cíle, schopnosti a struktura ruských kybernetických sil
- Ruské kybernetické útoky a Česká republika

Povinná četba:

WIRTZ J., James. Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy in *Cyber War in Perspective: Russian Aggression Against Ukraine*. NATO CCD COE. Talin 2015. 11 s. Dostupné z: https://bit.ly/2ktP9CC

Doporučená četba:

BAGGE, P. Daniel. 2019. Unmasking Maskirovka: Russia´s Cyber Influence Operations. Defense Press. New York. p 52-63, 140-173

6. ROLE CERT/CSIRT V SYSTÉMU ZAJIŠŤOVÁNÍ NÁRODNÍ BEZPEČNOSTI – 10. 11. (10:00–11:30 hod.)

PŘEDNÁŠEJÍCÍ: Ing. Jakub Onderka

- Historie CERT/CSIRT
- Typologie CERT/CSIRT
- Funkce a role CERT/CSIRT v systému zajišťování národní bezpečnosti
- Případová studie České republiky

Povinná četba:

MORGUS, Robert, Isabel SKIERKA, Mirko HOHMANN a Tim MAURER. National CSIRTs and Their Role in Computer Security Incident Response. Tallin: CCDCOE, 2015. 34 s. Dostupné také z: https://bit.ly/2BDskCP

http://www.cert.org/

Doporučená četba:

https://www.sei.cmu.edu/reports/03hb002.pdf str. 9-34.

PAČKA, Roman. CSIRT: V přední linii boje proti kybernetickým hrozbám. Centrum pro studium demokracie a kultury/Masarykova univerzita: Brno. 2019.

7. ČTECÍ TÝDEN - PROPAGANDA A INFORMAČNÍ VÁLKA – 17. 11.

- Současné teoretické přístupy k výzkumu IW
- Způsoby a metody manipulace s informacemi
- Ruská informační válka

Povinná četba:

ŘEHKA, Karel. Informační válka. Praha: Academia, 2017. XXI. století, sv. 46. ISBN 978-80-200-2770-2.

GILES, Kier. The Next Phase of Russian Information Warfare. NATO STRATCOM, 2016. 16. s. Dostupné z: https://bit.ly/2Nxk5hQ

Doporučená četba:

HOFFMAN, Frank G., 2012. Review Essay: History and Hybrid Warfare. Small Wars Journal. [online] Dostupné z: https://bit.ly/2NXXmZj

EBERLE, Jakub a Jan DANIEL. Hybrid Warriors: Transforming Czech Security through the 'Russian Hybrid Warfare' Assemblage. Sociologický časopis. 2018. Dostupné z: https://bit.ly/2NZJWMB

8. KYBERNETICKÁ KRIMINALITA - 24. 11. (10:00–11:30 hod.)

ŘEDNÁŠEJÍCÍ: Mgr. Kateřina Hábová

- Organizační struktura a role Policie ČR v potírání kybernetické kriminality
- Mezinárodní policejní spolupráce a její význam
- Nejčastější případy trestné činnosti páchané v kyberprostoru a modus operandi/psychologie pachatele a oběti
- Vybraná případová studie

Povinná četba:

IOCTA 2019, Dostupné z: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019KOLOUCH, Jan. CyberCrime. 2016. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

Doporučená četba:

Zákon č. 141/1961 Sb. v aktuálním znění, trestní řád. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141

Zákon č. 40/2009 Sb. v aktuálním znění, trestní zákoník. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

KIRWAN, Gráinne. The Psychology of Cybercrime: Concepts and Principles. 2012. 372 s.

9. BLÍZKÝ VÝCHOD V KYBERPROSTORU - 01. 12. (10:00 – 11:30 hod.)

ŘEDNÁŠEJÍCÍ: Mgr. Marek Dolejší

- Soupeření v kyberprostoru – Írán vs. Izrael
- Inovátorský přístup k zajištění KB – case study Izrael
- Noví aktéři – Turecko, Pákistán, Sýrie

Povinná četba:

FIXLER, Annie; CILLUFFO, Frank. Evolving Menace Iran's Use of Cyber-Enabled Economic Warfare, 2018. Dostupné online z**:** https://www.fdd.org/wp-content/uploads/2018/11/REPORT_IranCEEW.pdf

FT Magazine. Unit 8200: Israel's cyber spy agency. Dostupné online z: https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c

GEWIRTZ, Jason. Inside the IDF's Super-Secret Elite Brain Trust. Dostupné online z: http://www.thetower.org/article/inside-the-idfs-super-secret-elite-brain-trust-talpiot/

10. NASTUPUJÍCÍ VÝZVY KYBERNETICKÉ BEZPEČNOSTI – 08. 10. (10:00–11:30 hod.)

PŘEDNÁŠEJÍCÍ: Mgr. Luboš Přikryl

- Telekomunikační sítě nové generace (5G) a jejich bezpečnost: Jak ochránit nervový systém společnosti?
- Průmysl 4.0, IoT a autonomní doprava
- Kvantové počítače vs. současné šifrování
- AI, strojové učení a deep fakes
- Rapidní vývoj technologií a teorie černé labutě: Jak očekávat neočekávatelné?

Povinná četba:

LEE-MAKIYAMA, Hosuk. 2018. Stealing Thunder. ECIPE. Dostupné z: https://ecipe.org/wp-content/uploads/2018/02/ECIPE_Occasional0218_HLM_V7.pdf

MEDIN, Milo, GILLMAN, Louie. 2019. The 5G Ecosystem: Risks & opportunities for Dod. Defense Innovation Board. Dostupné z: https://media.defense.gov/2019/Apr/04/2002109654/-1/-1/0/DIB_5G_STUDY_04.04.19.PDF

Doporučená:

TALEB, Nassim Nicholas. 2007. *The black swan: the impact of the highly improbable*. New York: Random House. Kapitola 10.

GILES, Martin. 2019. *Explainer: What is a quantum computer?* MIT Technology Review. Dostupné z: **https://www.technologyreview.com/s/612844/what-is-quantum-computing/**

NATO Science & Technology Organization. Science & Technology Trends 2020-2040. Dostupné online z: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

11. ZÁKON O KYBERNETICKÉ BEZPEČNOSTI – 15. 12. (10:00–11:30 hod.)

PŘEDNÁŠEJÍCÍ: Ing. Michaela Vašková, Ph.D.

- Kybernetická bezpečnost – proč je důležitá a jak je v ČR řešena
- Zákon o kybernetické bezpečnosti – co je jeho obsahem
- Povinné osoby dle zákona o kybernetické bezpečnosti – na koho zákon dopadá
- Základní povinnosti povinných osob
- Nejčastější zjištění kontrol

Doporučená literatura:

Národní úřad pro kybernetickou a informační bezpečnost, **podpůrné materiály.** Dostupné zde: https://www.govcert.cz/cs/regulace-a-kontrola/podpurne-materialy/

POLČÁK, Radim. a kol. **Právo informačních technologií**. 1. vyd. Praha: Wolters Kluwer, 2018. 656 s. ISBN 978-80-7598-045-8. **Kapitola 11 Kyberkriminalita a 12 Kybernetická bezpečnost**

POLČÁK, Radim. HARAŠTA, Jakub. STUPKA, Václav. **Právní problémy kybernetické bezpečnosti**. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2016. 215 s. ISBN 978-80-210-8426-1.

Dostupné zde: https://science.law.muni.cz/knihy/monografie/Polcak_Kyberneticka_bezpecnost.pdf

KOLOUCH, Jan. BAŠTA, Pavel. a kol. **Cybersecurity.** 1. vyd. Praha: CZ.NIC, z. s. p. o., 2019. 562 s. ISBN 978-80-88168-34-8.Dostupné zde: https ://knihy.nic.cz/files/edice/cybersecurity.pdf

12. LIDSKÝ FAKTOR A VZDĚLÁVÁNÍ V KYBERNETICKÉ BEZPEČNOSTI – 05. 01. (10:00–11:30 hod.)

Přenášející: Mgr. Martin Hájek Dis.; Mgr. Petr Martinek

- Člověk jako příčina řady kyberbezpečnostních incidentů
- Nejčastější incidenty způsobené lidskou chybou
- Role vzdělávání v zajišťování kybernetické bezpečnosti na různých úrovních
- Český systém vzdělávání a role NÚKIB ve vzdělávání v kybernetické bezpečnosti
- Praktické ukázky zabezpečení na úrovni jednotlivce

Povinná literatura:

Alruwaili, A. (2019). A review of the impact of training on cybersecurity awareness. International Journal of Advanced Research in Computer Science, 10(5), 1-03.

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Koshutanski, H. (2020). Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. *Applied Sciences, 10*(16)

13. TABLE-TOP CVIČENÍ – 12. 01. (10:00–11:30 hod.)

POVEDOU: pracovníci Oddělení cvičení

Table-top cvičení

Povinná četba:

HEALEY, Jason a Klara TOTHOVA JORDAN. NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow. BRENT CENTER ON INTERNATIONAL SECURITY: Atlantic Council, 2014, 9 s. Dostupné z: https://bit.ly/1lLFa5U

SINGER, P.W. a Allan FRIEDMAN. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014. s. 247- 257. Dostupné z: https://goo.gl/S5iF3C