Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

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), Mgr. Veronika Netolická (v.netolicka@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.

Typ výuky, docházka, zkoušky a hodnocení

Výsledná známka bude sestavena z bodů získaných za **závěrečné písemné přezkoušení, tři position papery, prezenci a aktivní účasti na simulaci kybernetického cvičení**, která proběhne během 12. setkání, tedy 26. 11. 2019 a může být ohodnocena až za 5 plusových bodů, za samotnou účast je pak přidělen **1 bod**.

Position papery by měly být textem odborně reflektujícím aktuální témata kybernetické či informační bezpečnosti. Rozsah PP jsou 4 normostrany (povolen je pouze přesah 10 %). Maximální dosažený počet bodů za všechny PP je **24 (1 PP = max. 8)**. Hodnocena bude schopnost vědecké argumentace, využití teorií souvisejících s kurzem a bezpečnostními studiemi, stejně jako relevance závěrů. PP musí být odevzdány nejpozději do 15. 12. 2019.

Pro PP jsou připravená následující témata, z nichž si student volí právě **tři témata** k možnému zpracování:

1. Jakým způsobem ovlivňují vztahy s USA kybernetické operace íránských aktérů?
2. Konflikty na Blízkém východu a jejich manifestace v kybernetickém prostoru:
    a. Sýrie
    b. Jemen

   c. Izrael-Palestina
3. Vztah bezpečnosti a svobody na internetu.
4. Kybernetická obrana vs. Kybernetická bezpečnost.
5. Atribuce – postoje jednotlivých aktérů
6. Ruské chápání informační války a role kybernetických kapacit
7. Trendy v ruských kybernetickýh útocích
8. Institucionální rozměr kybernetické bezpečnosti v RF
9. Libovolné téma, které musí být schváleno do 24. 9. 2019.

Schopnost analyticky přistupovat k tématu kybernetické bezpečnosti ověří **závěrečné písemné přezkoušení**. Maximální možný dosažitelný počet bodů je **25**.

Docházka na kurz je **povinná**. Tolerují se dvě řádně omluvené absence. Při nesplnění podmínek docházky je kurz považován za nesplněný.

Hodnocení

50 – 46 b	A
45 – 41 b	B
40 – 36 b	C
35 – 31 b	D
30 – 26 b	E
25 a méně	F

OBSAH KURZU:

1. ÚVODNÍ HODINA – ORGANIZAČNÍ A FORMÁLNÍ NÁLEŽITOST (17. 9. 2019 - 10:00)

PŘEDNÁŠEJÍCÍ: Mgr. Veronika Netolická

- Požadavky a předpoklady
- Představení koncepce předmětu
- Seznámení s tématy PP
- Seznámení se s povinnou a doporučenou 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 A TEORETICKÉ ASPEKTY KYBERNETICKÉ BEZPEČNOSTI - 24. 9. (10:00–11:30 hod.)

PŘEDNÁŠEJÍCÍ: PhDr. Roman Pačka

- Úvod do kyberprostoru a způsob jeho fungování.
- 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
- Tvorba kybernetické bezpečnostní politiky
- Role a funkce státu v zajišťování kybernetické bezpečnosti
- Praktické info k návštěvě na NCKB

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. KYBERTERORISMUS - 1. 10. (10:00–11:30 hod.)

PŘEDNÁŠEJÍCÍ: Michaela Semecká, M.A. (Národní centrum kybernetické bezpečnosti), m.semecka@nukib.cz

- Kyberterorismus jako hypotetický fenomén?
- Jak velká je dnešní hrozba kyberterorismu?
- Případová studie Daeš
- Reakce a opatření

Povinná četba:

DRMOLA, Jakub. Konceptualizace kyberterorismu. Vojenské rozhledy, roč. 22 (54), č. 2, 2013. s. 94–102, ISSN 1210-3292.

Doporučená četba:

DENNING, Dorothy. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. 2001. Dostupné z: https://bit.ly/2wTKkFJ

LEWIS, James S. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. 2002. Dostupné z: https://bit.ly/2MdkuBH

ALKHOURI, Laith. KASSIER, Alex. NIXON, Allison. Hacking for ISIS: The Emergent Cyber Threat Landscape. 2016. Dostupné z: https://bit.ly/2Mad1TH

4. MEZINÁRODNÍ PRÁVO OPERACÍ V KYBERPROSTORU - 8. 10. (10:00–11:30 hod.)

PŘEDNÁŠEJÍCÍ: Mgr. David Komárek

- Úvod do mezinárodního práva veřejného
- Suverenita a Due diligence v kyberprostoru
- Kybernetické operace v době míru
- Protiopatření, plea of necessity, sebeobrana, atribuce
- Použití síly kybernetickými prostředky

Povinná četba:

SCHMITT, Michael N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. 2017. ISBN: 978-1316630372. Kapitoly 1,2, 4 a 14 (154 s.)

Doporučená četba:

CARR, Jeffrey. Responsible Attribution: A Prerequisite for Accountability. CCDCOE. 2014. 11 s. https://bit.ly/1r2CXVT

5. RUSKO V KYBERPROSTORU – 15. 10. (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 – 22. 10. (10:00–11:30 hod.)

PŘEDNÁŠEJÍCÍ: PhDr. Roman Pačka

- Historie CERT/CSIRT
- Typologie CERT/CSIRT
- Funkce a role CERT/CSIRT v systému zajišťování národní bezpečnosti
- Kultura CERT komunity a aktuální výzvy
- 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/

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

Doporučená četba:

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

7. ČTECÍ TÝDEN - PROPAGANDA A INFORMAČNÍ VÁLKA – 29. 10.

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

Povinná četba:

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 5. 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 2018, Dostupné z: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

KOLOUCH, Jan. CyberCrime. 2016. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

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

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

9. PRAKTICKÁ UKÁZKA: EXKURZE NA NÚKIB, adresa: Mučednická 31, Brno – 12. 11. (začátek od 9:00 - 10:45)

- Národní autorita KB a struktura NCKB
- Strategický a organizační rámec kybernetické bezpečnosti v ČR
- Představení činnosti a kompetencí GovCERT a Odboru kybernetických bezpečnostních politik
- Mezinárodní spolupráce při zajišťování kybernetické bezpečnosti (nejdůležitější organizace a hráči na poli zajišťování kybernetické bezpečnosti)

Povinná četba:

Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. NCKB, 2015. 35 s. Dostupné z: https://bit.ly/2CyK4RS

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. 2015, 24 s. Dostupné také z: https://bit.ly/2wT618j

Co je NÚKIB. Národní úřad pro kybernetickou a informační bezpečnost [online]. 2018 [cit. 2018-09-08]. Dostupné z: https://www.nukib.cz

10. NASTUPUJÍCÍ VÝZVY KYBERNETICKÉ BEZPEČNOSTI – 19. 11. (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/**

11. VZNIK MEZINÁRODNÍHO REŽIMU PRO KYBERNETICKOU BEZPEČNOST – 26. 11. (10:00–11:30 hod.)

PŘEDNÁŠEJÍCÍ: Jakub Otčenášek, MA., MSc.

- Úvod do problematiky normotvorby v kyberprostoru
- Přednáška formou řízené diskuze (Oxbridge formát)

Povinná četba:

Carr, M., „Cyberspace and International Order“, in H. Suganami, M. Carr, A. Humphreys (eds.), The Anarchical Society at 40: Contemporary Challenges and Prospects, Oxford: Oxford University Press, 2017. K dispozici na https://ict4peace.org/wp-content/uploads/2017/02/Carr-Attribution-in-International-Order.pdf

Forsyth, J. W. Jr and M. B. E. Pope, „Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace“, Strategic Studies Quarterly, Winter 2014. K dispozici na https://apps.dtic.mil/dtic/tr/fulltext/u2/a618954.pdf

Mazanec, B. M., „Why International Order in Cyberspace Is Not Inevitable“, Strategic Studies Quarterly, Summer 2015. K dispozici na https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-09_Issue-2/mazanec.pdf

Doporučená četba:

Finnemore, M. and D. B. Hollis, „Constructing Norms for Global Cybersecurity“, The American Journal of International Law, Vol. 110, No. 3, July 2016, pp. 425 – 479. Věnujte především pozornost kapitole III. The Novelty of Cyberspace for Normative Processes.

Developments in the field of information and telecommunications in the context of international security, rezoluce Ruské federace předložená Prvnímu výboru Valného shromáždění OSN, první verze 22. října 2018 (http://undocs.org/A/C.1/73/L.27), revidovaná verze 29. října 2018 (http://undocs.org/A/C.1/73/L.27/Rev.1)

Advancing responsible State behaviour in cyberspace in the context of international security, rezoluce USA předložená Prvnímu výboru Valného shromáždění OSN, 18. října 2018 (http://undocs.org/A/C.1/73/L.37)

Permanent Council Decision No. 1106 a 1202, opatření pro budování důvěry OBSE, (https://www.osce.org/pc/109168 a https://www.osce.org/pc/227281)

12. TABLE-TOP CVIČENÍ – 3. 12. (10:00–11:30 hod.)

POVEDOU: Mgr. Kateřina Hábová, Mgr. Pavla Jedličková

Table-top cvičení

- Vyhodnocení před hodinou 10. 12. 2019

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

13. PŘEDTERMÍN ZÁVĚREČNÉHO PÍSEMNÉHO PŘEZKOUŠENÍ – 10. 12. (10:00)