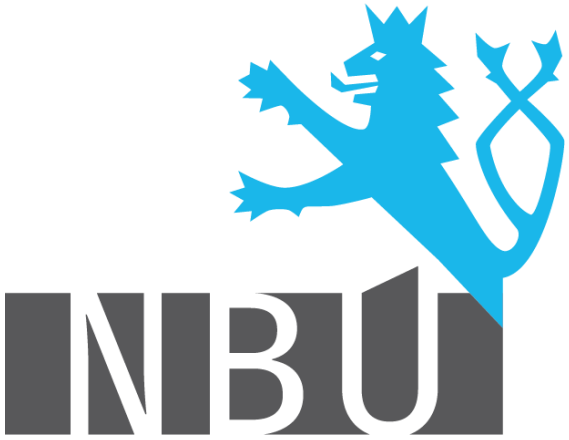
NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
Národní centrum kybernetické bezpečnosti



KYBERNETICKÁ BEZPEČNOST

Sylabus pro předmět
Kybernetická bezpečnost
Univerzita Palackého v Olomouci

SYLABUS

Předmět Kybernetická bezpečnost je jednosemestrální celouniverzitní kurz s alokací 4 hodin za měsíc. Kurz studentům poskytne úvodní seznámení s problematikou kybernetické bezpečnosti. Jednotlivé semináře se postupně věnují teoretickým, historickým, konceptuálním, legislativním a částečně také technickým aspektům kybernetické bezpečnosti. V rámci výuky budou studenti seznámeni se základní teorií kybernetické bezpečnosti, používanou odbornou terminologií, současným zajišťováním kybernetické bezpečnosti v České republice a ve světě či s historií kybernetických útoků, jejich taxonomií a typologií. Specifikem kurzu je rovněž poskytnutí praktických informací z oblasti zajišťování kybernetické bezpečnosti v České republice díky přednášejícím, kterými primárně budou pracovníci Národního centra kybernetické bezpečnosti. 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. Náplní kurzu budou rovněž diskuze o nebezpečích, která nejčastěji číhají na uživatele na internetu i to, jak těmto nástrahám předcházet či jak se jim bránit.

Hodnocení

- Závěrečný test

Program kurzu

1. týden (12. října)

- Seznámení s obsahem a požadavky na zakončení předmětu
- Seznámení se základní terminologií KB
- 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 (současní hlavní aktéři v ČR)

Povinná literatura:

Costigan, Sean. 2014. The Internet of Things and the role of government. Diplomatic Courier. http://www.diplomaticourier.com/2014/12/02/cybersecurity-the-internet-of-things-and-the-role-of-government/.

Melih, Bilgil. 2009. History of the Internet. Film. https://www.youtube.com/watch?v=9hIQjrMHTv4.

Singer, Peter W. – Friedman, Allan. 2014. Cybersecurity and Cyberwar. What Everyone Needs to Know. http://news.asis.io/sites/default/files/Cybersecurity_and_Cyberwar.pdf, s. 34 - 166.

Pačka, Roman. 2015. Difference Between Cyber Security and Cyber Defence from a Czech Perspective. In Cyber Security Review.

SCADA. Film. https://inductiveautomation.com/what-is-scada.

Stránky www.GovCERT.cz.

Výkladový slovník AFCEA. 2015. https://www.govcert.cz/cs/informacni-servis/vykladovy-slovnik/.

2. týden (26. října)

- Geneze kybernetických hrozeb, historie versus současnost, demokratizace a proliferace kyberprostoru
- Nejvýznamnější případové studie z historie
- Taxonomie útoků, code based, content based (IW)
- Základní typologie a motivace útočníků
- Propaganda, informační válka, trolling

Povinná literatura:

Healey, Jason. 2013. A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association. s. 14 – 232.

http://www.rsis.edu.sg/wp-content/uploads/2014/11/ER140527_Rethinking_Information.pdf, s. 5-18.

http://www.tandfonline.com/doi/full/10.1080/01402390.2014.977382, s. 4-37.

GEERS, Kenneth. Cyber war in perspective: Russian aggression against Ukraine. Tallinn: NATO CCD COE Publications, 2015, s. 87-103. ISBN 978-9949-9544-4-5 (16 stran)

Doporučená literatura:

Rid, Thomas. 2013.: Cyber war will not take place. London: Hurst & Company, xvi, 218 s. ISBN 9781849042802.

Pavlíková, Miroslava. Kybernetický boj mezi Ruskem A Ukrajinou v rámci ukrajinského konfliktu. Obrana a strategie [online]. University of Defence, 2016, 16 (1) [cit. 2016-07-17]. DOI: 10.3849/1802-7199.16.2016.1.079-098. ISSN 1802-7199. Dostupné z:

http://www.obranaastrategie.cz/cs/archiv/rocnik-2016/1-2016/clanky/kyberneticky-boj-mezi-ruskem-a-ukrajinou-v-ramci-ukrajinskeho-konfliktu.html#.V4u_0LiLTIU

3. týden (9. listopad)

- Kyberterorismus jako hypotetický fenomén?
- Kybernetický konflikt, kybernetická válka, hybridní konflikt, politicky motivované útoky
- Rozbor a modus operandi
- Reakce a opatření
- České i zahraniční případové studie

Povinná literatura:

Drmola, J. (2013): Konceptualizace kyberterorismu. In Vojenské rozhledy, roč. 22 (54), č. 2, s. 94–102, ISSN 1210-3292

http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1460&context=jss

https://www.usnwc.edu/getattachment/762be9d8-8bd1-4aaf-8e2f-c0d9574afec8/Cyber-War,-Cybered-Conflict,-and-the-Maritime-Doma.aspx

4. týden (23. listopad)

- Nejčastější druhy kriminality páchané v online prostředí
- Tuzemské a zahraniční policejní složky působící v boji proti KK, mezinárodní policejní spolupráce
- Nejčastější psychologie a pachatelů a obětí (jednání, modus operandi)
- význam preventivních programů a osvěty široké veřejnosti – digitální hygiena
- nejznámější tržiště s ilegálními komoditami, skrytá fóra a virtuální měny
- Demonstrace vybraných druhů KK na praktických ukázkách a případových studiích

Povinná literatura:

The Internet Organised Crime Threat Assesment (IOCTA) 2015, EUROPOL (s. 18. – 54). https://www.europol.europa.eu/latest_publications/31

Jirovský, Václav (2007), Kybernetická kriminalita, s. 15–31, s. 47.–52, s. 88–95, s. 111–113, s. 123–127, s. 195–207.

Finn, David. 2014. Combating cybercrime with technology. Microsoft video, 10:47. http://www.microsoft.com/en-us/showcase/details.aspx?uuid=2019fefe-496e-427c-b246-593497c31d45.

Kellerman, Tom. – Gene, West. 2014. What are today´s top cyber crime threats? Bloomberg video, 4:24. http://www.bloomberg.com/news/videos/b/c5b55221-0ca5-4711-8a0a-0a77e86dada5.

Doporučená literatura:

Zákon č. 40/2009 Sb., trestní zákoník, Část druhá - pouze seznam paragrafů.

5. týden (7. prosinec)

- Základy digitální hygieny se zaměřením na studenty coby běžné uživatele
- Závěrečný test *(povinný pro všechny)*