| Název rámcového tématu česky/anglicky | | Anotace (česky) | Anotace (anglicky) | Školitel | Školitel-specialista | Číslo a název projektu/grantu |
|---|---|---|---|---|---|---|
| **Koncepce zajištění kybernetické bezpečnosti vojenského zdravotnictví** | **Concept of ensuring cybersecurity of military health care** | Využívání ICT služeb v rámci zdravotnictví neustále roste. Stejně tak roste závislost tohoto sektoru na těchto službách a možné dopady kybernetických bezpečnostních incidentů představují reálnou hrozbu, která může mít vliv nejen na ICT infrastrukturu zdravotnických zařízení, ale i na zdraví a životy pacientů jako takových.<br>V souvislosti s tím a se stále častějšími kybernetickými útoky na zdravotnická zařízení je třeba řešit bezpečnost a odolnost informačních a komunikačních systémů. Současně je třeba řešit i stavy, kdy tyto systémy nebude možné v rámci zdravotnického zařízení využít zcela či pouze v omezené míře.<br>Vojenská zdravotnická zařízení zaujímají v ekosystému zdravotnických služeb ČR specifické postavení. Jedná se o zařízení poskytující zdravotní péči jak běžným pacientům, tak vojenskému personálu, či vrcholným představitelům státu. Vedle diverzity poskytované zdravotní péče jsou vojenská zdravotnická zařízení fakticky řízena Ministerstvem obrany, avšak svoji činnost a výstupy jsou povinny propojovat i s dalšími subjekty státu (např. UZIS, min. zdravotnictví aj.) či soukromými subjekty. Z tohoto pohledu je oblast bezpečnosti, a to i té kybernetické, zásadní otázkou, kterou je třeba v tomto ne zcela homogenním prostředí řešit.<br><br>Disertační práce přinese jednak analýzu a přehled teoretických poznatků v oblasti zajištění kybernetické bezpečnosti ve vojenských zdravotnických zařízeních a jednak doporučení ke zlepšení současné, ne zcela dostatečné propojenosti těchto oblastí. Práce vyplní bíle místo, které v současné době leží na pomezí těchto problematik. Přínos práce tak bude i pro futuro, neboť si práce klade mimo jiné za cíl předložit návrhy a argumenty ke změně a zlepšení současného stavu. | The use of ICT services within the healthcare sector is constantly growing. The sector's dependence on these services is also growing, and the potential impact of cyber security incidents is a real threat that can affect not only the ICT infrastructure of healthcare facilities, but also the health and lives of patients themselves.<br>In this context, and with cyber-attacks on healthcare facilities becoming more frequent, the security and resilience of ICT systems needs to be addressed. At the same time, it is also necessary to address situations where these systems cannot be used fully or only to a limited extent within a healthcare facility.<br>Military medical facilities occupy a specific position in the ecosystem of healthcare services in the Czech Republic. They are facilities providing health care to both ordinary patients and military personnel or top state officials. In addition to the diversity of health care provided, the Ministry of Defence effectively manages military health care facilities. Still, they are obliged to link their activities and outputs with other state entities (e.g. UZIS, Ministry of Health, etc.) or private entities. From this perspective, the area of security, including cyber security, is a crucial issue that needs to be addressed in this not entirely homogeneous environment.<br><br>The dissertation will provide both an analysis and overview of the theoretical knowledge in the field of ensuring cyber security in military medical facilities and recommendations for improving the current, not fully adequate interconnection of these areas. The thesis will fill the white space currently at the intersection of these issues. Thus, the contribution of the thesis will also be for the future, as the thesis aims, among other things, to present proposals and ar-guments to change and improve the current situation.<br><br>The aim of the thesis is to analyze the currently effective regulation of crisis management and cybersecurity within military medical facilities. The findings will be further compared with the situation in selected states of the European Union and Israel. On the basis of the findings, appropriate measures to improve the current situation and the possibilities of their implementation in the national regulation will be proposed. | doc. JUDr. Jan Kolouch, PhD. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Cílem práce je analyzovat aktuálně účinnou úpravu krizového řízení a kybernetické bezpečnosti v rámci vojenských zdravotnických zařízení. Zjištěné poznatky budou dále komparovány se situací ve vybraných státech Evropské unie a Izraele. Na základě provedených zjištění budou navržena vhodná opatření ke zlepšení současné situace a možnosti jejich implementace do vnitrostátní úpravy.<br><br>Literatura:<br><br>Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. ISBN 9781316822524<br>KOLOUCH, Jan a BAŠTA PAVEL. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-34-8.<br>KLIMBURG, Alexander. National cyber security: Framework manual. Tallin: NATO CCD COE, 2021. ISBN 978-9949-9211-1-9<br>DOUCEK., P., M. KONEČNÝ. a L. NOVÁK. Řízení kybernetické bezpečnosti a bezpečnosti informací. 1. vyd. 2020: Professional Publishing, 2020. 270 s. ISBN 978-80-88260-39-4.<br>Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon).<br>Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)<br>Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) | Literature:<br><br>Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. ISBN 9781316822524<br>KOLOUCH, Jan a BAŠTA PAVEL. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-34-8.<br>KLIMBURG, Alexander. National cyber security: Framework manual. Tallin: NATO CCD COE, 2021. ISBN 978-9949-9211-1-9<br>DOUCEK., P., M. KONEČNÝ. a L. NOVÁK. Řízení kybernetické bezpečnosti a bezpečnosti informací. 1. vyd. 2020: Professional Publishing, 2020. 270 s. ISBN 978-80-88260-39-4.<br>Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon).<br>Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)<br>Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) | | | |

**doc. Mgr. Zdeněk Hon, Ph.D., dr.h.c.**
**vedoucí KZOOO**

**prof. MUDr. Leoš Navrátil, CSc., MBA, dr.h.c.**
**předseda oborové rady CNP**