Název rámcového tématu česky/anglicky		Anotace (česky)	Anotace (anglicky)	Školitel	Školitel-specialista	Číslo a název projektu/grantu
Kybernetická bezpečnost zdravotnických zařízení se zaměřením na netechnická opatření	**Cybersecurity of healthcare facilities with a focus on non-technical measures**	Zdravotnická zařízení jsou jedním z častých a současně velmi kritických cílů kybernetických útoků. Implementace technických opatření může přispět k zvýšení zabezpečení těchto zařízení před kybernetickými útoky, avšak zpravidla dochází k narušení bezpečnosti v případě selhání lidského faktoru. *Předpokládaný cíl navrhované disertační práce:* Práce by se měla zabývat analýzou legislativních limitů a podmínek pro zajištění kybernetické bezpečnosti ve zdravotnických zařízeních v souvislosti s implementací Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (NIS2). V návaznosti na provedenou analýzu jak mezinárodní, tak národní právní úpravy podmínek kybernetické bezpečnosti by se autor/-ka měl/-a zaměřit na netechnická (zejm. organizační) opatření sloužící k zajištění kybernetické bezpečnosti zdravotních zařízení. *Očekávaný přínos pro vědní obor a pro praxi:* V rámci zpracování práce by mělo dojít ke komparaci podmínek, pro zajištění kybernetické bezpečnosti, stanovených právní úpravou EU a ČR se zaměřením na zdravotnická zařízení. Dále by měl být proveden kvantitativní výzkum zaměřený na implementaci netechnických opatření ve zdravotnických zařízeních. Na základě analýzy výsledků výzkumu by měla být navržena možná opatření na odstranění zjištěných nedostatků. Součástí práce by mělo být i vytvoření e-learningových modulů zajišťujících lepší plnění organizačních opatření ve zdravotnických zařízeních. Literatura:	Healthcare facilities are one of the frequent and currently very critical targets of cyber-attacks. Implementation of technical measures can help to increase the security of these facilities against cyber-attacks, but usually security breaches occur in case of human failure. *Anticipated objective of the proposed dissertation:* The thesis should analyse the legislative limits and conditions for ensuring cyber-security in healthcare facilities in the context of the implementation of Directive (EU) 2022/2555 of the European Parliment and of the Council of 14 December 2022 on measures to ensure a high common level of cyber-security in the Union (NIS2). Following the analysis of both international and national legislation on cyber-security conditions, the author/s should focus on non-technical (especially organisational) measures serving to ensure cyber-security of healthcare facilities. *Expected contribution to the discipline and to practice:* The work should include a comparison of the conditions for ensuring cyber security set by the EU and Czech legislation, with a focus on healthcare facilities. In addition, quantitative research should be conducted on the implementation of non-technical measures in healthcare facilities. On the basis of the analysis of the research results, possible measures should be proposed to eliminate the identified shortcomings. The work should also include the development of e-learning modules to ensure better implementation of organisational measures in healthcare facilities. Literature: Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. ISBN 9781316822524 KOLOUCH, Jan a BAŠTA PAVEL. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-34-8. KLIMBURG, Alexander. National cyber security: Framework manual. Tallin: NATO CCD COE, 2021. ISBN 978-9949-9211-1-9	doc. JUDr. Jan Kolouch, PhD.		

		Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. ISBN 9781316822524 KOLOUCH, Jan a BAŠTA PAVEL. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-34-8. KLIMBURG, Alexander. National cyber security: Framework manual. Tallin: NATO CCD COE, 2021. ISBN 978-9949-9211-1-9 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. Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon). Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) 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)	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. Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon). Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) 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