UNIVERSITY OF ŽILINA
Faculty of Electrical Engineering and Information Technology

Téma dizertačnej práce (DzP)

Akademický rok *2026/2027*

Názov	**Kybernetická bezpečnosť IoT a embedded zariadení**		
Inštitúcia	Fakulta elektrotechniky a informačných technológií Žilinská univerzita v Žiline		
Miesto	Žilina, Slovensko		
PhD. program	riadenie procesov		
Školiteľ	**doc. Dr. Ing. Peter Vestenický** Katedra riadiacich a informačných systémov		
Školiteľ špecialista	Ing. Pavol Kuchár, PhD., EUR ING Katedra riadiacich a informačných systémov		
Forma štúdia	**denná**		
Dĺžka štúdia	3 roky		
Jazyk štúdia	**slovenský**		
Dátum nástupu	1.9.2026		
Výskumná oblasť	**Kybernetická bezpečnosť**		
Kontakt zadávateľa	Tel. číslo:	E-mail:	Web stránka:
	+421 41 513 3345	peter.vestenicky@uniza.sk	https://kris.uniza.sk/

Anotácia témy DzP

Kybernetické útoky proti IoT a embedded zariadeniam vykazujú dlhodobo vzostupný trend a predstavujú významnú hrozbu pre spoločnosť, priemyselné podniky aj kritickú infraštruktúru. Tieto zariadenia sú často navrhované s dôrazom na funkčnosť a nízke náklady, pričom bezpečnostné mechanizmy nie sú implementované v dostatočnej miere, čo z nich robí atraktívny cieľ pre útočníkov. Útočníci môžu zneužívať zraniteľnosti vo firmvéri, komunikačných protokoloch alebo autentizačných mechanizmoch, čím získajú neoprávnený prístup k zariadeniam, manipulujú s ich činnosťou alebo ich zneužijú ako súčasť rozsiahlejších útokov, napríklad botnetov. Úspešný útok môže spôsobiť nielen technologické a ekonomické škody, ale aj ohroziť bezpečnosť používateľov a dôvernosť spracovávaných údajov. V prípade identifikácie bezpečnostného incidentu je nevyhnutné vykonať analýzu zraniteľností a mechanizmov, ktoré umožnili realizáciu útoku, s cieľom pochopiť jeho priebeh a identifikovať slabé miesta zariadenia. Cieľom dizertačnej práce je výskum zraniteľností IoT a embedded zariadení, analýza existujúcich bezpečnostných mechanizmov a identifikácia ich nedostatkov. Práca sa bude ďalej zaoberať návrhom odporúčaní, metód a bezpečnostných mechanizmov prípadne algoritmov na báze umelej inteligencie na zvýšenie úrovne ochrany týchto zariadení. Experimentálne výstupy práce by mali prispieť k zvýšeniu bezpečnosti IoT a embedded zariadení a k zníženiu rizika ich zneužitia v kybernetických útokoch.

Rozšírené informácie, výskumné zodpovednosti a úlohy doktoranda

Dizertačná práca sa zameriava na výskum zraniteľností a ochrany IoT a embedded zariadení, ktoré sa stávajú významnou súčasťou moderných informačných systémov, avšak často obsahujú bezpečnostné nedostatky spôsobené obmedzenými zdrojmi, nedostatočnými bezpečnostnými mechanizmami alebo nevhodným návrhom. Výskum bude zameraný na analýzu súčasného stavu bezpečnosti, identifikáciu a klasifikáciu zraniteľností na úrovni hardvéru, firmvéru a komunikácie, ako aj na analýzu existujúcich metód ochrany a experimentálny návrh inovovaných metód ochrany s použitím metód umelej inteligencie. Výsledkom práce bude rozšírenie poznatkov v

Financovanie: uveďte projekt, v rámci ktorého je téma DzP riešená (iba financované projekty, nie podané)

oblasti bezpečnosti IoT a embedded zariadení a návrh riešení využiteľných na zvýšenie ich odolnosti voči kybernetickým útokom, pričom doktorand bude samostatne realizovať výskum, experimenty, publikovať jeho výsledky a aktívne sa zapájať do vedecko-výskumných a marketingových aktivít pracoviska.

Profil uchádzača

Požadované zručnosti:
(Školiteľ zadá svoju špecifikáciu požadovaných zručností a vedomostí pre danú tému DzP.)

Nevyhnutné znalosti:• ukončené vysokoškolské vzdelanie II. stupňa v odbore kybernetika, kybernetická bezpečnosť, počítačové inžinierstvo alebo príbuznom odbore,• základné znalosti počítačových sietí, operačných systémov a informačnej bezpečnosti,• základná orientácia v problematike hrozieb, zraniteľností a ochranných mechanizmov.Výhodné znalosti:• pokročilejšie znalosti kryptografie, bezpečnosti sietí alebo bezpečnosti softvéru,• prehľad o aktuálnych trendoch a výskume v oblasti kybernetickej bezpečnosti,• základná znalosť právnych, etických alebo organizačných aspektov bezpečnosti.2. Technické a metodické zručnosti• základná schopnosť programovania (napr. Python, C/C++, Java alebo podobné),• skúsenosti s prácou v prostredí Linux/Unix,• schopnosť pracovať s bezpečnostnými alebo analytickými nástrojmi a analyzovať technické dáta,• základné skúsenosti s experimentálnou alebo laboratórnou prácou sú výhodou.3. Jazykové a komunikačné schopnosti• schopnosť čítať a porozumieť odbornej literatúre v anglickom jazyku,• základná schopnosť prezentovať a písomne spracovať odborné výsledky v angličtine,• ochota rozvíjať akademický a vedecký štýl komunikácie.4. Osobnostné predpoklady• samostatnosť, zodpovednosť a systematický prístup k riešeniu výskumných úloh,• analytické myslenie a schopnosť riešiť komplexné problémy,• motivácia pre dlhodobú vedecko-výskumnú činnosť,• schopnosť spolupracovať v tíme a aktívne komunikovať so školiteľom.5. Ďalšie výhodné predpoklady• skúsenosti s riešením projektov v oblasti IT alebo bezpečnosti,• účasť na súťažiach, projektoch alebo výskume v oblasti kybernetickej bezpečnosti,• skúsenosti s publikovaním, prezentáciou alebo odbornou činnosťou,• záujem o vedeckú kariéru alebo aplikovaný výskum v oblasti kybernetickej bezpečnosti.

Vypracovanie návrhu PhD. témy max. 2 strany!