Závěrečná zpráva pro interní rozvojový projekt na rok 2013 - Vzdělávání a výzkumná platforma kybernetické bezpečnosti

Verze 1.0
Dne 16. 1. 2014
Zpracovali: Václav Matyáš, Kamil Malinka

1 Manažerské shrnutí

Cílem projektu bylo navrhnout principy uceleného systému VŠ vzdělávání v oblasti kybernetické bezpečnosti na MU. Plánované výstupy projektu byly:

- profil absolventa navazujícího Mgr. studia oblasti kybernetické bezpečnost,
- výstupy z učení navazujícího Mgr. studia oblasti kybernetické bezpečnost,
- stanovení základních parametrů oboru nebo zaměření v existujícím oboru, včetně sylabů nových a inovovaných předmětů.

V rámci řešení projektu byly splněny všechny vytyčené cíle. Na základě odborného přesahu získaného v první půlce projektu byl stanoven profil absolventa a výstupy z učení navazujícího Mgr. studia oblasti kybernetické bezpečnosti. Na základě výstupů z učení byla dále provedena analýza aktuálně nabízených předmětů z pohledu jejich pokrytí. Výstupem projektu je rozhodnutí realizovat přípravu v rámci nového zaměření stávajícího oboru Bezpečnost IT na FI a zpráva diskutující získané výsledky, profil absolventa, výstupy z učení, základní parametry nového zaměření oboru (kreditová zátěž předmětů, doporučené průchody studiem apod.) a sylaby nových a inovovaných předmětů, které výstupy pokrývají.

Další fáze přípravy předpokládá pokračování projektu, kdy dojde k vlastní inovaci předmětů a přípravě studijních materiálů.

Součástí projektu bylo též stanovení relevantních výzkumných směrů. Výsledkem je mj. podání dvou projektů - společného mezioborového projektu IGA MU a také projektu Kontakt II s Harvardovou univerzitou.

2 Anotace projektu

Mezifakultní projekt - FI, FSS, PrF + ÚVT navazující na smlouvu s Národním bezpečnostním úřadem. Cíl - návrh uceleného systému VŠ vzdělávání a výzkumu v oblastech kybernetické bezpečnosti. Tento projekt reagoval na dohodu mezi MU a NBU o spolupráci, navazoval pak dále na změny prováděné v rámci spolupráce s indickým partnerem (DRDO) v oblasti technické bezpečnosti ICT.

Zaměření „kybernetická bezpečnost“ v rámci Mgr. oboru Bezpečnosti informačních technologií je připravováno v rámci intenzivní spolupráce mezi fakultami informatiky, právnické a sociálních studií. Bude v ČR unikátní (pravděpodobně úplně první) formou magisterského studia, stavějící na úzké spolupráci s NBÚ a jeho absolventi najdou uplatnění především ve společnostech a institucích, které s ohledem na připravovaný zákon o kybernetické bezpečnosti budou muset nasadit specialisty schopné spolupracovat s NBÚ, sekundárně absolventi oboru najdou dobré uplatnění také v samotném NBÚ a státním sektoru.

Cílem projektu bylo navrhnout principy uceleného systému VŠ vzdělávání v oblasti kybernetické bezpečnosti na MU, včetně struktury oboru nebo zaměření v rámci existujícího oboru a stanovení sylabů nových a inovovaných předmětů.

3 Výstupy projektu

- profil absolventa navazujícího Mgr. studia oblasti kybernetické bezpečnost,
- výstupy z učení navazujícího Mgr. studia oblasti kybernetické bezpečnost,
- stanovení základních parametrů oboru nebo zaměření v existujícím oboru, včetně sylabů nových a inovovaných předmětů.

4 Popis řešení

Silnou motivací při řešení tohoto projektu bylo minimalizovat nutnost vytvoření nových předmětů. Netriviální množství práce se tedy věnovalo analýze aktuálně vyučovaných předmětů z pohledu jejich možné inovace, tak aby pokryli požadavky nového zaměření.

4.1 Profil absolventa

V první fázi projektu vymezili vedoucí jednotlivých týmů oblasti, které měli znalostmi pokrýt odborní pracovníci z jiných fakult. Tím jsme zajistili dostatečný odborný přesah účastníků projektu, který byl potřebný pro kvalifikované diskuze o profilu absolventa a dalších výstupech. Odborné zvládnutí těchto oblastí probíhalo kombinací návštěv vybraných přednášek, samostudia a specializovaných seminářů. Kontrola postupu byla řešena formou pravidelných reportů a konzultací.

Konkrétně se jednalo o návštěvu těchto předmětů:

- ZUR388 Specifika online komunikace,
- BVV03K Kyberkriminalita,
- BI201K Úvod do práva ICT I,
- PV157 Autentizace a řízení přístupu.

Dále v rámci samostudia byly k nastudování vybrány následující publikace:

- Oxford Handbook of Internet Psychology. Adam N. Joinson, Katelyn Y. A. McKenna, Tom Postmes, Ulf-Dietrich Reips.
- Handbook for Computer Security Incident Response Teams (CSIRTs). Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek.
- Materiály ke kurzům TRANSITS I a II pořádaných organizací TERENA.
- Computer networking. James Kurose.

- Event Processing in Action. Opher Etzion, Peter Niblett.
- Komplexní zpracování událostí v systémech pro správu budov. Kučera Adam.
- Visualize This: The FlowingData Guide to Design, Visualization, and Statistics. Nathan Yau.
- Managing the Human Factor in Information Security. David Lacey.
- Autorizace elektronických transakcí a autentizace dat i uživatelů. Václav (Vašek) Matyáš, Jan Krhovják a kol.

Na pravidelných schůzkách se upřesňoval návrh profilu absolventa navazujícího Mgr. studia oblasti kybernetické bezpečnosti. Výsledný návrh profilu absolventa byl následně diskutován s NBÚ a dalšími odbornými pracovišti.

S ohledem na aktuální stav oboru BIT jsme se rozhodli, že není potřeba vytvářet zcela nový obor, ale je možné aktuální obor rozdělit na dvě zaměření, jedno více technologicky orientované a druhé zaměřené na kybernetickou bezpečnost. Nová podoba oboru a profily absolventů oboru by tedy vypadaly následovně:

Obor je zaměřený na získání znalostí z oblastí bezpečnosti v počítačových systémech a sítích, kryptografie a jejích aplikací. Cílem je příprava takového absolventa, který bude schopen pracovat v různých rolích kritických pro zajištění bezpečnosti IT – konkrétní vyprofilování (např. směrem ke kryptografii, technologickým aspektům či řízení bezpečnosti) nad rámec společného oborového základu je ponecháno na volbě studenta.

Zaměření *bezpečnost počítačových a komunikačních technologií* lépe připraví absolventa na práci v oblasti vývoje a správy systémů podporujících bezpečnost, příp. vhodně volit a aplikovat kryptografické metody pro zajištění konkrétních bezpečnostních funkcí. Absolventi najdou uplatnění ve společnostech vyvíjejících či dodávajících systémy zohledňující bezpečnostní požadavky, ale i při pokročilé správě a provozu takových systémů.

Zaměření *kybernetická bezpečnost* zohledňuje aspekty přesahu počítačového zpracování dat mimo pevně definované systémové perimetry (např. s dopadem na kritické infrastruktury), reflektované v oblasti tzv. kybernetické bezpečnosti a umožňující specifický víceoborový přesah jak technických, tak společenských a právních aspektů kybernetické bezpečnosti. Absolventi najdou uplatnění především ve společnostech a institucích, které s ohledem na předpisy ke kybernetické bezpečnosti budou muset nasadit specialisty schopné spolupracovat s relevantními koordinačními institucemi a zajistit řízení procesů kybernetické bezpečnosti.

4.2 Výstupy z učení pro obor Bezpečnost informačních technologií, zaměření Kybernetická bezpečnost

Souběžně se specifikací profilu absolventa probíhal návrh výstupů z učení navazujícího Mgr. studia oblasti kybernetické bezpečnost. Zde jsme se primárně opírali o znalosti získané v první fázi projektu. Diskutovalo se o vhodném rozsahu výstupů z učení, tak aby reflektovali požadavky kladené na absolventa tohoto zaměření. Finální definice výstupů z učení (viz níže) byla následně opět konzultována s dalšími odbornými pracovišti a má tuto podobu:

Osobní dovednosti

Absolvent je po úspěšném ukončení studia schopen:

1) rozlišovat různé druhy uživatelů ICT a porozumět jejich specifickému chování;
2) ovládat prezentační a komunikační dovednosti a bude schopen efektivně využívat týmovou práci při řešení problémů;
3) interpretovat sociální aspekty online komunikace a porozumět vnímání online rizik uživateli.

Právo/Management

Absolvent je po úspěšném ukončení studia schopen:

4) charakterizovat jednotlivé role v týmech při implementaci bezpečnostní politiky se zohledněním rozsahu nasazení politiky (uvnitř/vně organizace) a důležitosti situace (běžná/krizová);
5) aplikovat platné vnitrostátní předpisy v oblasti kybernetické bezpečnosti a aktivně se účastnit tvorby a provozu systému kybernetické bezpečnosti ve střední a velké veřejnoprávní nebo soukromoprávní organizaci;
6) samostatně pořizovat dokumentaci bezpečnostních opatření, třídit kybernetické bezpečnostní události, jakož i vyhodnocovat a stanoveným postupem hlásit kybernetické bezpečnostní incidenty v malé soukromoprávní nebo veřejnoprávní organizaci;
7) interpretovat právní úpravu počítačové kriminality, identifikovat počítačovou trestnou činnost, používat prostředky k zajištění elektronických důkazů a účinně spolupracovat s orgány činnými v trestním řízení;
8) interpretovat ve vzájemných souvislostech mezinárodní a evropskou právní úpravu kybernetické bezpečnosti a počítačové kriminality;
9) chápat strukturu duševního vlastnictví a prakticky používat základní ochranné instituty autorského práva;
10) posoudit hodnotu digitální identity, kategorizovat možnosti jejího zneužití a odhadnout případné dopady tohoto zneužití.

Informatické/technické

Absolvent je po úspěšném ukončení studia schopen:

11) připravit návrh a implementaci bezpečnostní politiky v malé organizaci a případně ji nově sestavit. V rozsahu větší organizace je schopen existující bezpečnostní politiku posoudit a prosazovat.
12) Posoudit vhodnost klasifikace, řízení a vyhodnocování incidentů v malé organizaci a navrhnout tyto metody. V rozsahu větší organizace je schopen dané metody praktikovat a ovládat. Dále je schopen využívat metod forenzní analýzy.
13) Zorganizovat správnou praxi v síťové bezpečnosti, jejíž nedílnou součástí je i příprava, realizace a vyhodnocení penetračního testování;
14) navrhnout a zorganizovat sledování provozu ICT systémů;
15) identifikovat prvky kritické infrastruktury, je schopen vyjádřit požadavky na příslušný dohledový systém a aplikovat metody CEP (complex event processing).

4.3 Pokrytí předměty

Dalším krokem byla analýza pokrytí výstupů z učení aktuálními předměty vyučovanými na MU. Analýza ukázala nutnost vzniku dvou nových předmětů, jinak je možné většinu výstupů pokrýt stávajícími předměty, pokud prodělají větší či menší inovaci (viz Tabulka 1).

Tabulka 1: Pokrytí výstupů z učení aktuálními předměty

Výstup z učení	Předmět
1,2	PV206
3	ZUR388
4,5,6,7,11	PV017
5,6,7,8	BVV03K
5,4,7,9	BI301K
9	BI201K
10	PV080
12,13,14	PV210
15	PA018

Obecně se dá složitost úprav předmětů rozdělit do tří úrovní (viz Tabulka 2): vytvoření nového předmětu ( ), velká modifikace stávajícího předmětu ( ), modifikace malého rozsahu ( ).

Tabulka 2: Rozsah nutných úprav předmětů

Výstup z učení	Předmět	Nutné úpravy
5,7,8	nový kurz Teorie a metoda práva ICT	Vytvoření nového kurzu metodologie práva pro zajištění dostatečného úvodu do problematiky práva. Rozsah: 1x za 2 semestry, 3 hod týdně – přednáška + semináře.
12,13,14	dva nové kurzy (povinné)	Vytvoření dvou nových předmětů Kybernetická bezpečnost v organizaci (bakalářský) a Advanced Topics of Cyber Security (magisterský) rozdělením předmětu PV210.
15	inovace PA018 (povinný)	Vytvoření nového obsahu pro cca ½ předmětu
3	inovace ZUR388 (povinný)	Vytvoření dvou nových přednášek pro pokrytí druhé části výstupu a změna vyučujícího.
4,5,6,7,11	inovace BI201K, BI301K, BVV03K, PV017 (povinný) + nový projekt v rámci PA018	Teoretické zázemí pro tyto výstupy bude obsaženo v uvedených předmětech. Je nutno zajistit spojitost právnických předmětů s PV017. Pro zajištění praktických dovedností vznikne nový projekt v rámci PA018.
5,4,7,9	Inovace BI301K	Rozšíření témat o veřejnoprávní ochranu duševního vlastnictví, ochranu informační bezpečnosti základních registrů a právní úpravu kybernetické bezpečnosti (včetně praktické aplikace prováděcích předpisů k zákonu o kybernetické bezpečnosti)
9	BI201K	Rozšíření témat o komplexní soukromoprávní řešení ICT outsourcingu (včetně ochrany osobních údajů, předávání osobních údajů ke zpracování, externího zajištění dohledu nad ICT a smluvního zajištění plnění povinností správců kritické informační a komunikační infrastruktury a správců významných informačních systémů a sítí)

1,2	inovace PV206 (povinný)	Přizpůsobení jedné seminární skupiny pro potřeby oboru.
10	inovace PV080	Vytvoření jedné nové přednášky.
	MV735K, MVV59K, BI301K a BI201K	Harmonizace obecných prerekvizit kursů

5 Relevantní výzkumné směry

Součástí projektu bylo též stanovení relevantních výzkumných směrů. V průběhu prací na projektu došlo k vytyčení dvou hlavních výzkumných směrů. Rozhodli jsme se rovnou podat dva projekty, které je reflektují. V rámci veřejné soutěže MŠMT ve výzkumu, vývoji a inovacích VES14 k programu mezinárodní spolupráce ve výzkumu a vývoji KONTAKT II byl podán projekt „NEPASS“, který je zamýšlen ve spolupráci s Harvardskou skupinou CRCS.

V rámci IGA MU byl podán mezioborový projekt „Experimentální výzkum chování uživatelů ICT v oblasti bezpečnosti perspektivou sociálních věd, práva a informatiky.“

5.1 Experimentální výzkum chování uživatelů ICT v oblasti bezpečnosti perspektivou sociálních věd, práva a informatiky

Oblast zkoumání chování uživatelů informačních a komunikačních technologií (dále ICT) v oblasti bezpečnosti ICT je tématem, které je třeba zkoumat perspektivou různých oborů. Technické rozhraní platforem udává celkové možnosti toho, co je v něm koncový uživatel schopen udělat (zkoumá obor informatiky), pravidla chování uživatele mají usměrňovat (obor práva) a sám uživatel pak na obě tyto oblasti určitým způsobem reaguje (obor sociálních věd). Všem těmto oblastem je přitom třeba věnovat dostatečnou pozornost, aby byla zajištěna výsledná vyšší úroveň bezpečnosti. Jako nejslabší článek těchto oblastí jsou nejčastěji popisováni právě koncoví uživatelé (Vance, Siponen, & Pahnila, 2012), kteří přímo či nepřímo, vědomě či nevědomě, způsobují více než polovinu případů narušení bezpečnosti (Stanton, Stam, Mastrangelo, & Jolton, 2009) i značné finanční ztráty organizací (Herath & Rao, 2009). Ovlivnění chování koncových uživatelů směrem k vyšší obezřetnosti a dodržování bezpečnostních pravidel proto představuje velmi aktuální téma, na které se zaměřujeme v předkládaném projektu. Dosavadní zkoumání však probíhá v drtivé většině v rámci jednotlivých oborů, což neumožňuje dostatečně komplexní pohled na problematiku. Předkládaný projekt plánuje zkoumání chování uživatele ICT v oblasti bezpečnosti perspektivou sociálních věd, informatiky a práva, čímž by se stal unikátním nejenom v rámci Masarykovy univerzity, ale v kontextu celé mezinárodní vědy zabývající se tématem bezpečnosti ICT.

Projekt se zaměřuje na zkoumání chování uživatelů ICT v oblasti bezpečnosti. Plánujeme uživatele ICT experimentálně vystavit použití více různých opatření v oblasti bezpečnosti ICT (technických, školení, informací o nové zákonné normě, směrnic) a sledovat změny chování uživatelů v oblasti bezpečnosti v závislosti na působení daného experimentálního vlivu. Obecným cílem projektu je hledání způsobů ovlivňování uživatelů, aby se změnilo jejich chování směrem k bezpečnějšímu používání ICT. Ptáme se, jaké působení na uživatele ICT má vliv a jaké naopak nemá účinek. Projekt může proto významně přispět jednak k pochopení chování uživatelů ICT v oblasti bezpečnosti a jednak k zlepšení vlastností budoucího softwaru.

Konkrétní cíle projektu jsou následující:

1) Návrh a ověření nových způsobů měření chování uživatelů ICT: cílem je vyvinout nové způsoby měření chování uživatelů, jak na úrovni vnímání uživatelem (dotazníkové metody), tak na úrovni technické (záznamy událostí).

2) Testování míry vlivu různých typů působení na uživatele, od IT prostředků, přes (online) školení, po vysvětlení nových právních povinností. Sledování míry změny v chování uživatelů ICT v závislosti na jejich psycho-sociálních charakteristikách.

3) Srovnání vybraných možností pro volbu a správu metod alternativní obnovy přístupu (AOP) z hlediska jejich kvality a uživatelské přívětivosti. Sledování různých možností AOP v kontextu psycho-sociálních charakteristik uživatelů.

4) Vyzkoušení různých typů vysvětlení právních povinností - jakým způsobem nejlépe podat uživatelům dopady právního předpisu nebo interní instrukce. Cílem je určit systematiku základních znaků, které je třeba sledovat při hodnocení srozumitelnosti předpisu, pokynu nebo varování v oblasti IT bezpečnosti.

5) Právní a etické aspekty takového výzkumu: experimentální výzkum koncových uživatelů má značná etická a právní úskalí, které plánujeme v tomto výzkum nejen ošetřit, ale především také zprostředkovat vědcům pro účely dalšího výzkumu. Budeme také sledovat a popisovat právní aspekty takového výzkumu.

Metodou výzkumu bude realizace následujících třech experimentů, na kterých se budou podílet odborníci ze třech fakult (FSS, FI, PrF), UVT a ze třech komerčních firem:

(1) Experiment na koncových uživatelích systémů pro ochranu uživatelských výpočetních prostředků (antivir, základní systémová a síťová ochrana, rodičovská kontrola) ve spolupráci s firmou ESET.

(2) Experiment zkoumající nejvhodnější metody a postupy pro tzv. záložní přístup k systému, s využitím alternativních metod pro obnovu přístupu, známých obvykle jako záložní hesla. Tento experiment bude prováděn ve spolupráci se společností SodatSW.

(3) Experiment bude založen na expozici cílové skupiny různými typy pravidel (právní předpis, doporučení, „dobrá praxe“, interní předpis apod.) a měření míry úspěchu resp. míry toho, jak si cílová skupina příslušné pravidlo IT bezpečnosti internalizuje. Tento experiment bude proveden jednak v prostředí MU a také v prostředí společnosti NetSuite.

Dopady

Jelikož se domníváme, že předkládaný projekt je ve své podstatě unikátní, očekáváme významné dopady především v mezinárodním měřítku, sekundárně pak v měřítku lokálním. Konkrétní výstupy projektu popisujeme dále, zde se zaměříme na dopady pro jednotlivé obory.

Zkoumání chování uživatelů ICT v oblasti bezpečnosti je v sociálních vědách prakticky na svém počátku, zkoumány jsou sice často dopady a faktory prevalence samotných rizik (např. kyberšikany, problémů s osobními daty, excesivní používání internetu), ale experimentální zkoumání chování uživatelů ICT je velmi výjimečné. Pochopení chování uživatelů ICT z pohledu psycho-sociálních faktorů, které přispívají k různým typům chování v oblasti IT bezpečnosti, může mít proto významný dopad na zkoumání této oblasti. Projekt může mít také významné dopady v oblasti metodologie sociálních věd, neboť umožní srovnat data z dotazníků, které budou uživatelé v experimentech vyplňovat, se záznamem jejich reálného chování v prostředí ICT.

Pro oblast informatiky projekt napomůže k nastavení vhodného uživatelského rozhraní bezpečnostních řešení pro koncového uživatele, výběr vhodné metody alternativní obnovy přístupu a prezentaci bezpečnostních pravidel koncovým uživatelům v systému MU a společnosti NetSuite. Z dlouhodobého hlediska očekáváme nové znalosti v oblasti expozice uživatelů různým druhům bezpečnostních opatření a získání následné zpětné vazby.

Pro právo a právní vědu přinese projekt rozpracování metodologie pro hodnocení vhodnosti, potřebnosti a míry platnosti interních instrukcí v oblasti bezpečnosti ICT v závislosti na jejich technické kvalitě, srozumitelnosti a formě prezentace jejich recipientům. Pro další vědecká zadání s obdobným tematickým zaměřením přinese tento projekt též vytvoření postupů pro hodnocení souladu výzkumných aktivit s právními předpisy (zejm. experimentálního zkoumání chování uživatelů) vzhledem k ochraně soukromí, ochraně osobních údajů a ochraně výzkumných dat.

5.2 Projekt NEPASS

Projekt NEPASS se zaměřuje na analýzu navržených algoritmů a jejich reálných implementací z pohledu funkčnosti a požadovaných vlastností. Cílem je analýza výstupů projektu a využití zkušeností členů výzkumné skupiny s cílem poskytnou expertní posouzení jako zpětnou vazbu do výzkumných skupin CRCS a IQSS (Institut pro kvantitativní sociální vědy).

Hlavní témata projektu

Projekt NEPASS se jako hlavnímu tématu výzkumu věnuje oblasti ochrany soukromí a úzké spolupráci s výzkumnou skupinou CRCS. Hlavní témata výzkumu pokrývají oblasti *analýzy navržených matematických a právních definicí pro soukromí* s ohledem na různé modely útočníků; *spolupodílení se při vylepšování algoritmů a nástrojů pro správu citlivých souborů dat; posuzování a analýzy reálných implementací a praktické experimenty* ve spolupráci se zainteresovanými výzkumnými skupinami na Masarykově Univerzitě. Instituce na Masarykově univerzitě mohou také dále využít výsledky projektu – *vyvinuté nástroje* – pro vlastní výzkumné projekty v oblasti zpracování datových souborů s citlivými informacemi.

Projekt NEPASS se jako hlavnímu tématu výzkumu věnuje oblasti ochrany soukromí a úzké spolupráci s výzkumnou skupinou CRCS. Hlavní témata výzkumu pokrývají oblasti analýzy navržených matematických a právních definicí pro soukromí s ohledem na různé modely útočníků; spolupodílení se při vylepšování algoritmů a nástrojů pro správu citlivých souborů dat; posuzování a analýzy reálných implementací a praktické experimenty ve spolupráci se zainteresovanými výzkumnými skupinami na Masarykově Univerzitě. Instituce na Masarykově univerzitě mohou také dále využít výsledky projektu – vyvinuté nástroje – pro vlastní výzkumné projekty v oblasti zpracování datových souborů s citlivými informacemi.

Využití výsledků

Projekt NEPASS (ve spolupráci se skupinou CRCS z Harvardu) se zaměřuje na analýzu algoritmů a principů, které vzniknou v rámci výzkumu ve skupině CRCS a analýzu jejich implementací s ohledem na funkčnost a bezpečnost/ochranu soukromí. Cílem je analýza výstupů projektu TWC a poskytnutí expertní zpětné vazby skupinám CRCS a IQSS. Tato aktivita mimo jiné podpoří výzkumné aktivity v oblasti ochrany soukromí na půdě Masarykovy univerzity a participujících výzkumných skupinách. Tyto výzkumné skupiny budou moci těžit z výstupů projektu a to jak na úrovni reálných implementací, tak vyvinutých algoritmů, ve svém vlastní výzkumné činnosti.

Dopady

Očekávané výstupy navrhovaného projektu ovlivní nejen výzkum v oblasti IT, ale též práva (ochrana soukromí a sdílení citlivých dat) a sociálních věd – oblast, kde jsou datové soubory obsahující citlivé informaci jedním z hlavních zdrojů pro výzkum a analýzy.

Těsná spolupráce mezi výzkumnými skupinami na Fakultě informatiky a CRCS v Bostonu vytvoří prostředí na mezinárodní úrovni, ve kterém se uplatní výzkumní pracovníci, doktorští a magisterští studenti.

6 Přílohy

- Profil absolventa navazujícího Mgr. studia obor Bezpečnost informačních technologií, zaměření Kybernetická bezpečnost
- Výstupy z učení pro obor Bezpečnost informačních technologií, zaměření Kybernetická bezpečnost
- Parametry oboru Bezpečnost informačních technologií

6.1 Profil absolventa navazujícího Mgr. studia obor Bezpečnost informačních technologií, zaměření Kybernetická bezpečnost

Obor je zaměřený na získání znalostí z oblastí bezpečnosti v počítačových systémech a sítích, kryptografie a jejích aplikací. Cílem je příprava takového absolventa, který bude schopen pracovat v různých rolích kritických pro zajištění bezpečnosti IT – konkrétní vyprofilování (např. směrem ke kryptografii, technologickým aspektům či řízení bezpečnosti) nad rámec společného oborového základu je ponecháno na volbě studenta.

Zaměření *bezpečnost počítačových a komunikačních technologií* lépe připraví absolventa na práci v oblasti vývoje a správy systémů podporujících bezpečnost, příp. vhodně volit a aplikovat kryptografické metody pro zajištění konkrétních bezpečnostních funkcí. Absolventi najdou uplatnění ve společnostech vyvíjejících či dodávajících systémy zohledňující bezpečnostní požadavky, ale i při pokročilé správě a provozu takových systémů.

Zaměření *kybernetická bezpečnost* zohledňuje aspekty přesahu počítačového zpracování dat mimo pevně definované systémové perimetry (např. s dopadem na kritické infrastruktury), reflektované v oblasti tzv. kybernetické bezpečnosti a umožňující specifický víceoborový přesah jak technických, tak společenských a právních aspektů kybernetické bezpečnosti. Absolventi najdou uplatnění především ve společnostech a institucích, které s ohledem na předpisy ke kybernetické bezpečnosti budou muset nasadit specialisty schopné spolupracovat s relevantními koordinačními institucemi a zajistit řízení procesů kybernetické bezpečnosti.

6.2 Výstupy z učení pro obor Bezpečnost informačních technologií, zaměření Kybernetická bezpečnost

Osobní dovednosti

Absolvent je po úspěšném ukončení studia schopen:

1) rozlišovat různé druhy uživatelů ICT a porozumět jejich specifickému chování;
2) ovládat prezentační a komunikační dovednosti a bude schopen efektivně využívat týmovou práci při řešení problémů;
3) interpretovat sociální aspekty online komunikace a porozumět vnímání online rizik uživateli.

Právo/Management

Absolvent je po úspěšném ukončení studia schopen:

4) charakterizovat jednotlivé role v týmech při implementaci bezpečnostní politiky se zohledněním rozsahu nasazení politiky (uvnitř/vně organizace) a důležitosti situace (běžná/krizová);
5) aplikovat platné vnitrostátní předpisy v oblasti kybernetické bezpečnosti a aktivně se účastnit tvorby a provozu systému kybernetické bezpečnosti ve střední a velké veřejnoprávní nebo soukromoprávní organizaci;
6) samostatně pořizovat dokumentaci bezpečnostních opatření, třídit kybernetické bezpečnostní události, jakož i vyhodnocovat a stanoveným postupem hlásit kybernetické bezpečnostní incidenty v malé soukromoprávní nebo veřejnoprávní organizaci;
7) interpretovat právní úpravu počítačové kriminality, identifikovat počítačovou trestnou činnost, používat prostředky k zajištění elektronických důkazů a účinně spolupracovat s orgány činnými v trestním řízení;
8) interpretovat ve vzájemných souvislostech mezinárodní a evropskou právní úpravu kybernetické bezpečnosti a počítačové kriminality;
9) chápat strukturu duševního vlastnictví a prakticky používat základní ochranné instituty autorského práva;
10) posoudit hodnotu digitální identity, kategorizovat možnosti jejího zneužití a odhadnout případné dopady tohoto zneužití.

Informatické/technické

Absolvent je po úspěšném ukončení studia schopen:

11) připravit návrh a implementaci bezpečnostní politiky v malé organizaci a případně ji nově sestavit. V rozsahu větší organizace je schopen existující bezpečnostní politiku posoudit a prosazovat.
12) Posoudit vhodnost klasifikace, řízení a vyhodnocování incidentů v malé organizaci a navrhnout tyto metody. V rozsahu větší organizace je schopen dané metody praktikovat a ovládat. Dále je schopen využívat metod forenzní analýzy.
13) Zorganizovat správnou praxi v síťové bezpečnosti, jejíž nedílnou součástí je i příprava, realizace a vyhodnocení penetračního testování;
14) navrhnout a zorganizovat sledování provozu ICT systémů;
15) identifikovat prvky kritické infrastruktury, je schopen vyjádřit požadavky na příslušný dohledový systém a aplikovat metody CEP (complex event processing).

6.3 Parametry oboru Bezpečnost informačních technologií

BIT základ

Mat (3 z):

- IV111 Pravděpodobnost v informatice (4+2 kr.) (anglicky od JS2014 nebo 2015)
- M0170 Kryptografie (3+2 kr.)
- M8170 Teorie kódování (3+2 kr.)
- MA007 Matematická logika (2+2 kr.)
- MA009 Algebra II (2+2 kr.)
- MA010 Graph Theory (3+2 kr.)
- MA012 Statistika II (4+2 kr.) (později Statistika pro informatiku – v angličtině)
- MV008 Algebra I (2+2 kr.)
- PřF:M8190 Algoritmy teorie čísel (2+2 kr.)

TeoInf (3 z):

- IA011 Sémantiky programovacích jazyků (3+2 kr.)
- IA012 Složitost (2+2 kr.)
- IA014 Funkcionální programování (3+2 kr.)
- IA062 Randomized Algorithms and Computations
- IA101 Algoritmika pro těžké problémy
- IA158 Real Time Systems
- IA159 Formal Verification Methods
- IV054 Kódování, kryptografie a kryptografické protokoly (5+2 kr.)
- IV100 Paralelní a distribuované výpočty (do budoucna v angličtině)

AplInf:

- jeden z:
  - PA039 Architektura superpočítačů a intenzivní výpočty
  - PA150 Principy operačních systémů (2+2 kr.)
  - PA174 Design of Digital Systems II
  - PA192 Secure hardware-based system design (6+2 kr.)
  - PV208 Advanced Topics od Linux Administration
- jeden z:
  - PA151 Soudobé počítačové sítě (2+2 kr.)
  - PA159 Počítačové sítě a jejich aplikace I
  - PA191 Advanced Computer Networking (2+2 kr.)
  - PVeee - Secure Network Design – nový předmět
- jeden z:
  - PA017 Softwarové inženýrství II
  - PA103 Objektové metody návrhu informačních systémů (2+2 kr.)
  - PA128 Similarity Searching in Multimedia Data
  - PA152 Efektivní využívání databázových systémů
  - PA193 Secure coding principles and practices (6+2 kr.)

Povinné předměty oboru BIT

- PA018 Advanced Topics in Information Technology Security (4+2 kr.)

- PA168 Postgraduate seminar on IT security and cryptography (2+1 kr.)
- Jeden z:
    - PV181 Laboratory of security and applied cryptography I (2 kr.)
    - PV204 Laboratory of security and applied cryptography II (2 kr.)
- PV079 Applied Cryptography (3+2 kr.)
- IV054 Kódování, kryptografie a kryptografické protokoly (5+2 kr.)

Povinné předměty zaměření Kybernetická bezpečnost

- PV017 Bezpečnost informačních technologií (2+2 kr.)
- PV206 Communication and Soft Skills (5+2 kr.)
- XXXXX Advanced Topics of Cyber Security (3+2 kr.) – nový předmět
- ZUR388 Specifika online komunikace (4 kr.)
- XXXXX Teorie a metody práva ICT (2+1 kr.) – nový předmět
- BI301K Úvod do práva ICT II (3+1 kr.)
- BVV03K Kyberkriminalita (2+1 kr.)

Povinně volitelné předměty zaměření Kybernetická bezpečnost

- BI201K Úvod do práva ICT I (3+1 kr.)
- MVV59K Software Law (3+1 kr.)
- MV735K Normativní systémy v kyberprostoru (2+1 kr.)
- MP57901K IT v právní praxi (1+1 kr.)
- BZ209K Právní informatika (4+1 kr.)

Povinné předměty zaměření BICT

- PA193 Secure coding principles and practices (6+2 kr.)
- PV181 Laboratory of security and applied cryptography I (2 kr.)
- PV204 Laboratory of security and applied cryptography II (2 kr.)
- PVddd System verification and assurance (8 kr.) – nový předmět

Povinně volitelné předměty zaměření BICT

- PřF: M8170 Teorie kódování (3+2 kr.)
- MA009 Algebra II
- PV206 Communication and Soft Skills (5+2 kr.)
- XXXXX Advanced Topics of Cyber Security (3+2 kr.) – nový předmět
- PV222 Security Architectures (2+1 kr.)
- PA192 Secure hardware-based system design
- PA193 Secure coding principles and practices