HODNOCENÍ OPONENTA DIPLOMOVÉ PRÁCE

Autor práce	**Bc. Jana Líčeníková**
Studijní program	**Bezpečnost společnosti**
Specializace	**Ochrana obyvatelstva**
Forma studia	**kombinovaná**
Akademický rok	**2023/2024**
Téma práce	**Služby pro okamžité zasílání zpráv v kontextu datové bezpečnosti**
Autor posudku	**Ing. Petr Svoboda, Ph.D.**

	Kritéria hodnocení	**Váha**	**Hodnocení**
1	Formulace cílů práce a použité metody	0,07	D
2	Úroveň teoretické části práce	0,15	D
3	Úroveň analyticko-empirické části práce	0,25	E
4	Úroveň aplikační části práce	0,10	D
5	Výstavba textu a jeho logická provázanost, kvalitativní a kvantitativní parametry práce	0,08	C
6	Splnění cílů práce a relevance závěrů	0,15	D
7	Odborný přínos práce a její praktické využití	0,10	D
8	Jazyková úroveň práce	0,05	C
9	Formální náležitosti práce (včetně citací a užití šablony)	0,05	A
	Návrh hodnocení dle váženého průměru	1,00	**D (2,48)**

Předložená diplomová práce se zabývá službami pro okamžité zasílání zpráv v kontextu datové bezpečnosti. Cíle jsou strukturovány do jednoho cíle a zřejmě tří dílčích, ty však nejsou dostatečně precizně specifikovány. O cílech hovoří autorka i v Závěru, tyto se liší. Cíle autorka v průběhu zpracování naplnila převážně za dodržení zásad pro zpracování a na základě doporučené literatury s využitím vyjmenovaných vědeckých metod. Vyjmenované metody jsou však zřejmě nekompletní, oponentem bylo v práci identifikováno využití dalších, např. indukce a dedukce. V práci postrádám v Zásadách doporučenou literární rešerši.
Teoretická část představuje dobrý vhled do historie problematiky, vedle zmíněných však opomíjí některé důležité technologie, konkrétně pak Jabber a IRC. V práci se opakovaně vyskytuje nesprávný název úřadu NÚKIB ve smyslu Národní úřad kybernetické bezpečnosti (chybí „informační“). Mezi kybernetickými hrozbami (viz kapitola 3.3.2 na str. 32) bych vzhledem k cílení tématu očekával odnože phishingu typické pro IM, konkrétně vishing a smishing. DoS a DDoS útoky byly v kapitole 3.3.4 na str. 34 definovány, jako by mezi nimi nebyl žádný rozdíl. Tato kapitola rovněž staví do stejné skupiny pojmy viry, trojské koně, ransomware a spyware, přitom některé hovoří o efektech, jiné o způsobech šíření. V rámci základních definic je využito diskutabilních zdrojů, očekával bych využití Výkladového slovníku kybernetické bezpečnosti.

V praktické části postrádám vlastní analýzu založenou na některé uznávané metodě. Vhodná by byla např. komparativní tabulka s využitím multikriteriálního hodnocení.
Práci vnímám jako povrchovou, zásadním výstupem je pak konstatování na základě proklamovaných informací, že by uživatelé dbalí bezpečnosti informací měli používat Signal, případě málo známé Jami.

Otázky k obhajobě:

1. Můžete vysvětlit následující výrok na str. 17: „Na rozdíl od komunikačních platforem jsou e-emaily asynchronní, což znamená, že účastníci nemusí být online ve stejnou dobu, aby komunikovali“? V případě komunikace prostřednictvím dnešních IM je nezbytně nutné být online?
2. V současnosti se objevují názory (např. Europol) zastávající zrušení end-to-end šifrování za účelem odhalování trestné činnosti, zejména pak vůči mladistvým (dětská pornografie apod.) Jak se k tomuto názoru stavíte?
3. Jaký je stav transpozice NIS 2 do nového Zákona o kybernetické bezpečnosti v kontextu Vámi zmíněného závazného data?

V Uherském Hradišti dne 09.05.2024 **Podpis:**

Hodnocení odpovídá následující stupnici:
A = 1,00-1,24 B = 1,25-1,50 C = 1,51-2,00 D = 2,01-2,50 E = 2,51-3,00 F = 3,01-…