Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

OPONENTSKÝ POSUDEK BAKALÁŘSKÉ PRÁCE

Student: **Krenželák Nikola** **Oponent:** **Ing. David Malaník, Ph.D.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Informační technologie v administrativě**
Akademický rok: **2017/2018**

Téma bakalářské práce: **Kybernetická bezpečnost malých firem**

Hodnocení práce:

		A	B	C	D	E	F
	Hodnocení: A – nejlepší; F - nevyhovující						
1.	Obtížnost zadaného úkolu	☒	☐	☐	☐	☐	☐
2.	Splnění všech bodů zadání	☐	☐	☐	☐	☐	☒
3.	Práce s literaturou a její citace	☐	☐	☐	☐	☒	☐
4.	Úroveň jazykového zpracování	☐	☐	☐	☒	☐	☐
5.	Formální zpracování – celkový dojem	☐	☐	☐	☒	☐	☐
6.	Logické členění práce	☐	☒	☐	☐	☐	☐
7.	Vhodnost zvolené metody řešení	☐	☐	☐	☒	☐	☐
8.	Kvalita zpracování praktické části	☐	☐	☐	☐	☒	☐
9.	Výsledky a jejich prezentace	☐	☐	☐	☐	☒	☐
10.	Závěry práce a jejich formulace	☐	☐	☐	☐	☒	☐
11.	Přínos práce a její využití	☐	☐	☐	☐	☐	☒

Celkové hodnocení práce:
Výsledná známka není průměrem výše uvedených hodnocení. Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou bakalářskou práci nedoporučuji k obhajobě a navrhuji hodnocení

F - nedostatečně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Otázky k obhajobě:
1. Jak se liší digitální podpis a elektronický podpis?
2. "Digitální podpis sám o sobě nezaručuje pravost dokumentu, o tu se starají certifikační autority. " Jak?
3. kapitola 1.3.3 "Hashování se můţe pouţívat u zpráv (e-mail), souborů, ale také u rychlého vyhledávání dat z databází. " - můžete prosím vysvětlit, jak se hashování používá u emailů a vyhledávání dat z datatbáze?
4. strana 29 "Poskytuje také informovanost o právech občanů a umoţňuje jim zamezit další zpracování jejich údajů cizími osobami, nebude-li k tomu mít závaţný důvod. " - na jakém základě můžete uchovávat osobní údaje osob?
5. Vztah jakých subjektů upravuje GDPR? Vysvětlete, kdo má práva a kdo povinnosti.

6. kapitola 6.2.1.1 A nebylo by vhodné hodnotítí kritérium u Antiviru jeho úspěšnost v testech antivirů? Perioda aktualizace virové databáze? Vámi zvolené kritéria lze použít na cokoliv a nereflektují potřeby při implementaci antivirového řešení.

Další připomínky, vyjádření, náměty k obhajobě práce (možno pokračovat i na další stránce):
1. s13 "O jaké systémy se můţe jednat, aplikujeme-li bezpečnost do systému? " - vytrženo z kontextu skript. Nejedná se o systémy, ale o bezpečnostní politiky.
Není moc česky napsané….
2. kapitola 1.3 "Slovo Kryptografie se skládá z 2 řeckých slov – kryptós (skrytý) a gráphein (text). " - tato informace se v uvedeném zdroji nevyskytuje.
3. kapitola 1.3.1 "Tohle šifrování se můţe zdát riskantní, neboť klíč mají k dispozici obě strany, bezpečnost šifrování je tedy velice závislá na používaném algoritmu. Výhodou tohoto šifrování je právě ten fakt, že celý proces probíhá velice rychle z důvodu právě sdíleného klíče. " - tvrzení, že sdílení klíče znamená, že je šifra rychlá není podložené ničím. A navíc to není pravda.
4. kapitola 1.3.2 "Tyto dva klíče spolu tvoří pár, přičemž nejprve je vytvořen klíč soukromý a až poté klíč veřejný, ovšem lze vytvořit dodatkový veřejný klíč. " - nejprve generován veřejný klíč a až poté soukromý. Čili přesně naopak, než uvádí student.
5. kapitola 1.3.2 "Oproti symetrickému šifrování je však tento způsob bezpečnější, jelikoţ je nutné vlastnit privátní klíč z klíčového páru, za cenu pomalejšího šifrování. " - opět nepodložená spekulace o tom, co se podílí na rychlosti. Navíc věta nedává smysl.
6. strana 18 "Při vytvoření digitálního podpisu musíme nejprve vytvořit hash a tento hash poté privátním klíčem zašifrovat. " - nepřesná informace, jakým privátním klíčem se šifruje?
7. strana 28 "Pověřenec je zvolen, je-li hlavní činnost orgánů veřejné moci a firem, rozsáhlé sledování občanů, zpracování citlivých údajů a údajů u rozsudků trestních činností. " - to není pravda!
8. strana 28 "Jeden pověřenec může pracovat pro více firem s podobnou organizační strukturou najednou, ale musí plnit svou činnost co nejlépe." - to je opravdu definice. GDPR jasně stanovuje, možnosti, jak může být jeden pověřenec ve více firmách.
9. strana 28 "Pověřenci zpracovávají informace například o pacientech nemocnic, telefonických a internetových datech, datech bank a pojišťoven, lokalitách zákazníků a osobních údajích získaných vyhledáváním z důvodu reklam. " - to není pravda!
10. strana 28 "Dalším důvodem je zamezení shromažďování informací o osobách nejrůznějšími institucemi, jako například tajné služby států mimo evropský prostor. " - to není pravda!!
11. strana 29 "Stane-li se, že se ve firmě vyskytne problém s bezpečností, je potřeba nyní tuto událost nahlásit, neboť existuje nebezpečí úniku osobních údajů. " - problém s bezpečností = únik osobních dat? Jedná se o hodně zavádějící a navíc vágní formulaci.
12. strana 30 "Poruší-li firma toto ustanovení, pak jim hrozí pokuta maximálně 20 milionů eur nebo 4 % z celkového ročního obratu firmy " - nepravdivá formulace 4% z celosvětového ročního obratu. Konkrétně je to "V některých případech může být udělena pokuta 20 000 000 EUR nebo jedná-li se o podnik, až do výše 4 % celkového obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší."
13. strana 31 "Právo na výmaz je právo, kdy můţe osoba (subjekt), o níţ se vedou údaje, poţádat o jejich smazání ze systému a ze záloh. " - výmaz se netýká záloh!
14. kapitola 5.4 "WPA3 bude k dispozici ve třetím nebo čtvrtém čtvrtletí roku 2018. [48] " - daný zdroj takovou informaci neuvádí!
15. kapitola 5.5 - naprosto zcestné, vše už tu bylo i dřív. "Dosahují tím právě vyuţitím SSL certifikátů, které jde velice snadno získat. " - naprosti vytrženo z kontextu a zavádějící (úmyslně?)
16. V bodě 6.2 jsou namátkou vybrány sw komponenty. Není zde ani znínka o tom, na základě je autor vybral.

17. strana 47 "Největší výhoda open source antivirových programů je ta, že jsou uživatelé schopni upravovat program podle své potřeby. " - Opravdu si myslíte, že bude uživatel zasahovat do kódu antiviru a, že je to největší benefit opensourcových softwarů?

Práce je psaná velmi nekonzistentně - působí místy spíše jako sestříhaná ze zdrojů bez logicky navazujících vět např. "Jsou to veškeré informace, u kterých díky kombinace s jinými informacemi lze identifikovat osobu či osoby." Některé pasáže práce působí v kontextu technické bakalářské práce velmi úsměvně: "Každý člověk má nějaké potřeby. Ať už jde o potřeby biologické (spánek, potrava, vylučování), tak i potřeby psychické (osobní rozvoj, pocit lásky, vědění). Existuje ale i další nezbytná potřeba, a tou je pocit bezpečí. Co nám dává pocit bezpečí? Dává nám především klid na duši. Máme-li střechu nad hlavou, nemusíme se obávat, že nám bude zima, nebo nám někdo ublíží, zatímco spíme. "

Práci nedoporučuji k obhajobě na základě výtek, které jsou uvedeny v tomto posudku, práce obsahuje spoustu nepravdivých informací, které jsou ze zdrojů přebrány ledabyle a často vytrženy z kontextu. Což jim dává jiný význam, než ve skutečnosti mají. Po stylistické stránce je práce velmi slabá. Dále si nejsem jistý naplněním bodu zadání č.4 a č.7. Dle mého názoru není vysvětlena souvislost mezi GDPR a kybernetickou bezpečnostní malých firem. V práci je popis co je GDPR(navíc s fatálními chybami), ale ona souvislost poněkud chybí. Co se týká bodu č.7. Je tu popis vlastností "navržených" sw prvků, není tu ale žádné doporučení pro implementační postupy ani nic podobného. Na čitatele to působí ne jako návrh ale spíše rešerše toho co je na trhu a když jsou v bodě 6 srovnáni vždy 2 náhodně vybraní jedinci, tak je autor nezi sebou porovnává. Bohužel, ne zcela vhodnou metrikou. Takže je výběr opět na uživateli.

Datum 1.6.2018 Podpis oponenta bakalářské práce