FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Karel Pohl
Student:	Julia Plotnikova
Název práce:	Aplikace pro řízení rizik kybernetické bezpečnosti
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	9. června 2023

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
  [2] zadání splněno s menšími výhradami
  [3] zadání splněno s většími výhradami
  [4] zadání nesplněno

Práce je logicky členěna tak, aby jednotlivé kapitoly odpovídaly struktuře zadání. Větší prostor je věnován samotné aplikaci, což je logické a žádoucí zejména s ohledem na cíl práce, kterým je právě návrh aplikace a souvisejících procesů. Mohlo být věnováno více prostoru existujícím nástrojům, je však třeba přiznat, že řada těchto nástrojů je komerční povahy a přístup k nim (obzvláště za účelem vytvoření konkurenční náhrady) není snadný.

Výsledkem práce je funkční prototyp aplikace vytvořený na základě předchozí analytické činnosti, která probíhala v reálném prostředí.
Je tedy možné konstatovat, že práce splňuje zadání ve všech bodech.

2. Písemná část práce 80 / 100 (B)

Práce je zpracována v přiměřeném rozsahu, více prostoru je věnováno výsledkům práce, tedy prototypu aplikace. Úvodní části práce (zejména porovnání softwarových produktů) mohly být informačně bohatší, očekával bych shrnutí argumentů, které podporují vývoj nové aplikace jako potvrzení předpokladů uvedených v zadání práce.
Logicky práce odpovídá posloupnosti bodů zadání a vytváří tak smysluplný informační řetězec vedoucí k naplnění cílů práce. V práci se nevyskytují věcné nepřesnosti, nicméně práce by měla projít důkladnější jazykovou korekturou, která by odstranila nejen občasné překlepy, ale též některé formulace, jejichž informační obsah není na první pohled úplně zřejmý. Příkladem je věta v kapitole 5.1.1 na straně 46: "Také to má „termin“, kde toto se dá propojit s „ReviewUntil“, kde tyto položky mají stejný význam."
Z jazykového hlediska je mírně problematická kombinace češtiny a "počeštěných" anglických výrazů, typicky slovo "featury". V oboru se jistě vyskytuje řada anglických slov,

které se obtížně překládají (v literatuře je možné se setkat i s nevhodnými překlady), nicméně pro "aplikační feature" by se jistě vhodné slovo našlo.
Typografické zpracování je zdařilé, vzhledem k prostoru, který formát A4 poskytuje, je dle mého názoru trochu zbytečné dělit slova na konci řádku, v některých případech dělení slov čitelnosti textu příliš neprospívá. Například rozdělení názvu stavu na straně 43: "Re-viewUntil".
Formální nedostatky z hlediska autorského práva či citace zdrojů jsem neshledal.
Nižší hodnocení této části je způsobeno zejména jazykovou stránkou textu. Text je srozumitelný pro čtenáře, který se věnuje oboru informační bezpečnosti a vývoje software, dle mého názoru však může být méně srozumitelný pro čtenáře, kteří se primárně věnují jiným oborům (například manažeři a vedoucí pracovníci, kteří mohou být cílovou skupinou vytvořené aplikace).

3. Nepísemná část, přílohy

90 /100 (A)

Hlavní přílohou práce je funkční prototyp aplikace. Zde oceňuji zejména volbu použité technologie. Ačkoli je technologie Microsoft Blazor poměrně mladá, poskytuje velké možnosti při tvorbě webových aplikací. Autorka se musela zorientovat v nové technologii, která v současné době stále prochází bouřlivým rozvojem a informační zdroje jsou ve srovnání s jinými technologiemi na výrazně nižší úrovni.
Navzdory skutečnosti, že se jedná o prototyp, poskytuje aplikace celou řadu zajímavých funkčností, a i v předložené podobě by mohla být nasazena do reálného provozu. Určitě je možné konstatovat, že ve srovnání s evidencí vedenou v tabulkovém kalkulátoru (nebo v papírové podobě) poskytuje aplikace i ve své rané verzi velkou přidanou hodnotu.
Přínosné jsou zejména možnosti přizpůsobení aplikace, konkrétně například možnost nastavení stavů rizik. Dle mého názoru obsahuje aplikace příliš velký počet stavů rizik, díky možnosti přizpůsobení je však možné stavy přizpůsobit konkrétní situaci a zvyklostem ve firmě.
Rozhraní aplikace používá angličtinu, což je sice v oboru běžné, z hlediska cílové skupiny by bylo vhodné uvažovat o lokalizaci. Jelikož se však jedná o prototyp, není chybějící lokalizace problémem. Autorka si v závěru práce stěžuje na nevhodnou volbu (českého) jazyka. Je pravdou, že pro některé pojmy se obtížně hledají české ekvivalenty. Na druhou stranu je třeba vzít v úvahu skutečnost, že menší společnosti v ČR nemusí mít zaměstnance, kteří dobře ovládají technickou angličtinu, a právě jazyk může rozhodovat nejen o volbě nástroje, ale zejména o správném pochopení celé problematiky, které je jedním z klíčů pro efektivní řízení rizik v jakémkoli podniku.
Drobným nedostatkem byla absence testovací dokumentace, konkrétně informace o testovacích uživatelích a jejich heslech. Tento nedostatek mírně komplikoval vyzkoušení prototypu. Pro vyzkoušení prototypu tak byl nutný ruční zásah do databáze, což vzhledem k dostatečné dokumentaci a popisu aplikace nepředstavovalo zásadní problém.

4. Hodnocení výsledků, jejich využitelnost

100 /100 (A)

Práce samotná nepřináší žádné převratné novinky nebo objevy v oboru. Na druhou stranu to ani nebylo cílem práce. Výsledky práce (konkrétně funkční prototyp aplikace) ukazují, že je možné s minimálními náklady efektivně pokrýt oblast řízení rizik v oblasti informační bezpečnosti. Ušetřené zdroje (a to nejen finanční, ale též lidské) mohou být využity například k dalšímu budování systému řízení informační bezpečnosti, a to zejména v oblasti technických opatření, kde je nutné často spoléhat na externí dodavatele.
Oblast řízení rizik je pro svou "administrativní" povahu často opomíjená, zejména v menších společnostech či podnicích. Při správném a efektivním přístupu však může

přinést značné úspory. Řízení rizik je založené na jednoduchých principech, které mohou být degradovány právě použitím komplikovaných nástrojů, které jsou určeny k řešení výrazně složitější agendy velkých podniků.
Malý a jednoduchý nástroj přinese i menším podnikům možnost efektivně a systematicky řídit rizika. Výsledky práce tedy mají značné možnosti praktického využití a bude určitě na místě aplikaci dále rozvíjet. To usnadní i volba licenčního modelu MIT.

Celkové hodnocení

93 /100 (A)

Práce bezezbytku naplňuje své cíle a prakticky ukazuje, jak je možné řídit rizika v oblasti informační bezpečnosti (vzhledem k jisté univerzálnosti navržené aplikace je možné ji použít i v jiných oborech). Textová část neobsahuje věcné nepřesnosti ani zavádějící informace a z práce je zřejmé, že byla vytvořena na základě praktických zkušeností, což výrazně zvyšuje možnost využití výsledků práce v praxi. Drobné jazykové či stylistické nedostatky v žádném případě nesnižují praktickou hodnotu a význam práce.
Navrhuji hodnocení klasifikačním stupněm A.

Otázky k obhajobě

1. V práci jsou zmíněny role Garanta a Delegáta. Delegát je označen jako zástupce Garanta. Můžete jejich vztah blíže osvětlit a uvést příklady využití rolí v praxi?
2. V práci je zmíněno několik metod pro identifikaci rizik. Demonstrujte některou metodu na praktickém příkladě.
3. V práci jsou zmíněny nedobré zkušenosti s ADO.NET. Vysvětlete, jakým způsobem by dle vašeho názoru použití Entity Framework (místo ADO.NET) usnadnilo vývoj či ladění aplikace? Demonstrujte na příkladě.

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.