Mobilní aplikace pro analýzu rizik v oblasti bezpečnosti informací

Bc. Jan Juračka

Diplomová práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva
akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan Juračka**
Osobní číslo:	**L17098**
Studijní program:	**N3953 Bezpečnost společnosti**
Studijní obor:	**Bezpečnost společnosti**
Forma studia:	**prezenční**

Téma práce: **Mobilní aplikace pro analýzu rizik v oblasti bezpečnosti informací**

Zásady pro vypracování:

1. **Zpracujte rešerši vztahující se k problematikám tvorby mobilních aplikací a analýzy rizik v oblasti bezpečnosti informací.**
2. **Zvolte vhodný matematický aparát pro problematiku analýzy rizik v oblasti bezpečnosti informací.**
3. **Za pomoci metod datového modelování s využitím vhodného matematického aparátu vytvořte datový model předmětné mobilní aplikace.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] LACKO, Ľ uboslav. Vývoj aplikací pro Android. Brno: Computer Press, 2015. ISBN 978-80-251-4347-6

[2] WRÓBLEWSKI, Piotr. Algoritmy. Brno: Computer Press, 2015. ISBN 978-80-251-4126-7.

[3] KALUŽA, Jindřich a Ludmila KALUŽOVÁ. Modelování dat v informačních systémech. Praha: Ekopress, 2012. ISBN 978-80-86929-81-1.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce:	**Ing. Petr Svoboda** Ústav ochrany obyvatelstva
Datum zadání diplomové práce:	**30. listopadu 2018**
Termín odevzdání diplomové práce:	**15. května 2019**

V Uherském Hradišti dne 30. listopadu 2018

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 15.5.2019

Jméno a příjmení studenta: Bc. Jan Juračka

.....
podpis studenta

ABSTRAKT

Tato diplomová práce popisuje vytvoření datového návrhu mobilní aplikace pro analýzu rizik v oblasti bezpečnosti informací. V teoretické části se práce zabývá základy datového modelování, uvedením do problematiky informační bezpečnosti a analýzou rizik bezpečnosti informačních systémů. V praktické části se nachází charakteristika navrhnuté aplikace, konceptuální a logický datový model a v poslední části návrh uživatelského rozhraní včetně schématu a popisu funkčnosti aplikace.

Klíčová slova: Datové modelování, datový model, bezpečnost informací, analýza rizik, mobilní aplikace

ABSTRACT

This diploma thesis describes a data design creation of a mobile application designed for a risk analysis in the information security area. In the theoretical part, the thesis deals with the basics of the data modeling, an introduction to the information security problematic and risk analysis of the information systems security. The practical part explains a characteristic of the designed application, conceptual and logical data model. The last part is focused on a user interface design, including a schema with the application functionality description.

Keywords: Data Modeling, Data Model, Informatin Security, Risk Analysis, Mobile Application

Chtěl bych poděkovat mé rodině, přátelům a spolužákům za obrovskou podporu po celou dobu studia. Rovněž patří obrovské díky mému vedoucímu práce panu Ing. Petru Svobodovi za cenné rady a odborné vedení při zpracování této práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Telefony, jakožto mobilní zařízení jsou vyvíjeny od poloviny minulého stolení, ovšem ten největší nárůst uživatelů vlastnících toto zařízení nastal až s nástupem nového tisíciletí. V podstatě téměř každý z nás vlastní nějaký druh mobilního zařízení (chytré telefony, tablety apod.). Tento trend lže přisuzovat jejich klesající ceně, která umožňuje rozsáhlý technologický vývoj. Mobilní telefony lze označit za nejrozšířenější informační a komunikační zařízení na světě. S jejich rostoucí „inteligencí" se nabízí možnost využití této platformy jakožto praktického prostředku. Ruku v ruce s vývojem mobilních telefonů jde i vývoj aplikací, který zaznamenává stejný raketový rozmach. Uživatelé mají možnost tyto aplikace jednoduše stahovat a využívat je k usnadnění každodenního života či uspokojení svých potřeb.

Lze tedy konstatovat, že se informační systémy staly neoddělitelnou součástí současného světa. Pokrok jde neustále dopředu, v oblasti informačních technologií je daleko znatelnější než v jiných oblastech. Roste výpočetní výkon, světem hýbe digitalizace dat a informací, internetové bankovnictví, firemní informační systémy atd. Každá mince má ovšem dvě strany a za obrovským potenciálem této oblasti se skrývá i možnost jejího zneužití a to od malých firem až po vlády jednotlivých států. Informace se staly cenou komoditou na trhu, lze je považovat za jeden z klíčových faktorů úspěchu či neúspěchu.

Vyvstává otázka nejen pro management firem, státní organizace, ale i pro jednotlivce ohledně bezpečnosti a ochrany dat a informací před živelnými pohromami, trestnou činností, neoprávněným přístupem, zneužití důležitých informací, aby nedocházelo ke ztrátě dat při zpracování, přenosu, ukládání a opětovném využití dat, dále pak před vznikem chyb, neoprávněné modifikaci dat, sabotáži apod.

Problematika bezpečnosti informací je v dnešní době velice aktuální téma, je obsažena v řadě strategických dokumentů, jako je například Analýza hrozeb pro Českou republiku z roku 2015. Dosáhnout přijatelného řešení bezpečnosti informací lze prostřednictvím stanovení organizačních, režimových, personálních, hardwarových, softwarových a dalších opatření. Hlavním předpokladem ke stanovení těchto opatření je kvalitně zpracovaná analýza rizik. Pro provedení analýzy rizik bezpečnosti informací lze využít různé metody či softwary. Právě tato problematika se stala hlavním předmětem této práce, ve které je navrhnut datový model mobilní aplikace pro analýzu rizik v oblasti bezpečnosti informací.

I. TEORETICKÁ ČÁST

1 DATOVÉ MODELOVÁNÍ

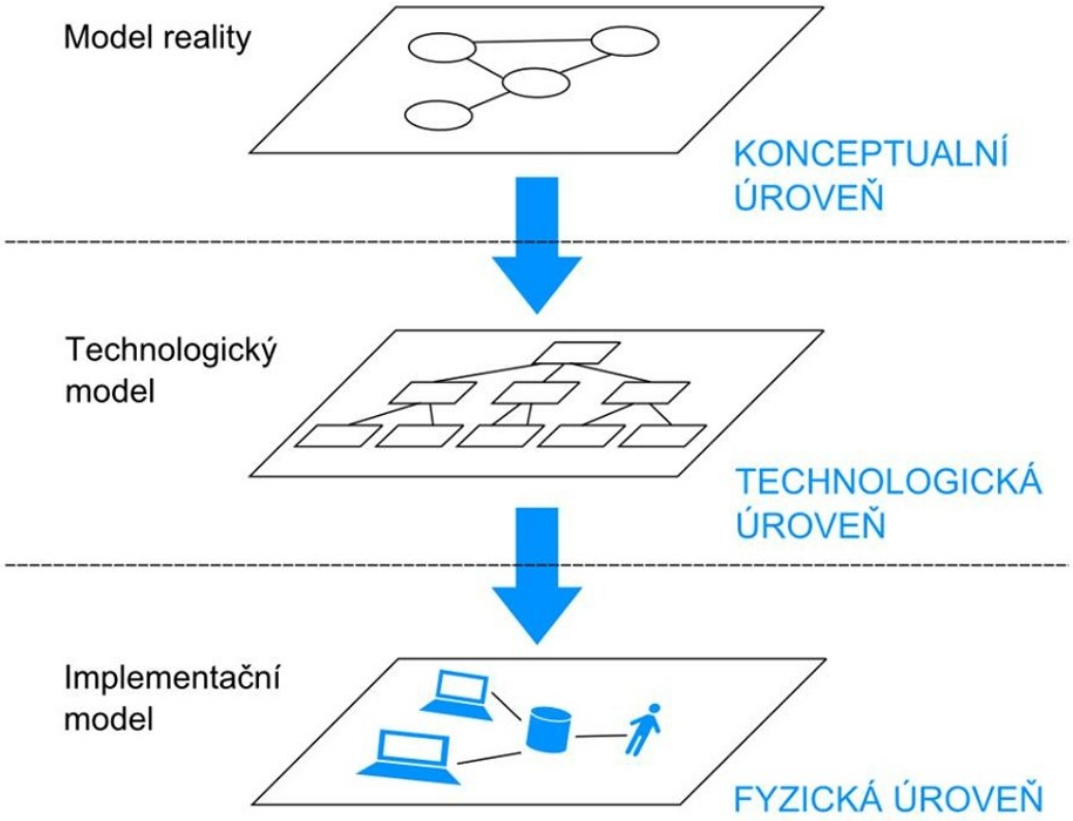
Jedná se o proces, který definuje a analyzuje požadavky na strukturu dat, s nimiž pracuje informační systém (IS). Výstupem procesu datového modelování je datový model, který definuje formát a strukturu dat v informačních systémech a určuje vztahy jednotlivých datových prvků. Tímto procesem je v nich reprezentována vymezená část reality. Cílem datového modelování je zachytit a popsat část reality, o které chceme uchovat informace. Je to tedy proces návrhu struktury a uspořádání dat s cílem převedení reálných objektů na objekty datové. Datové modelování tedy umožňuje vytvořit standardizovaný a konzistentní návrh datové struktury s možným využitím v oblastech jako jsou například návrh databází a datových uložišť, integraci informačních systémů nebo při správě dat. [1]

1.1 Princip tří architektur

Objektivní realita je modelována pomocí abstrakce, která rozeznává z pohledu svého cíle podstatné rysy reality a zachycuje je v modelu. Při datovém modelování se využívá principu tří architektur (dle obr.1), jehož prostřednictvím definujeme způsob použití abstrakce. To znamená, že nám umožňuje rozčlenit zkoumaný datový model na mentálně zvládnutelné části, které představují různé úrovně abstrakce. Dle principu tří architektur rozdělujeme abstrakci do tří úrovní:

- konceptuální (někdy se rozděluje na sémantickou a konceptuální),
- logickou (technologickou),
- fyzickou (implementační).

Každá z těchto úrovní se zaměřuje na jeden z hlavních aspektů vyvíjeného systému (obsah, technologii a implementační specifika) a logicky tvoří přirozenou posloupnost. [2]



Obrázek 1: Princip tří architektur [23]

Výstupem jednotlivých fází je model, který se v následujících fázích stává konkrétnějším. Finálním výsledkem je datový model. [2]

1.2 Konceptuální datový model

Vyznačuje se vysokou mírou abstrakce, v této fázi se selektují a popisují veškeré potřebné informace včetně vazeb, potřebné pro vytvářený systém. V této části vzniká model reality, jehož cílem je identifikování typů objektu odrážejících modelovanou realitu. Konceptuální modelování lze chápat obecněji jako modelování vztahů a pojmů.

Je možné specifikovat tři typy abstrakce použité při konceptuálním datovém modelování:

- **klasifikace** – aplikuje se pro identifikaci typů objektů jako základních konstruktorů odrážejících objektivní realitu. Takovým typem objektu může být například „zaměstnanec“ s výskyty vyjadřujícími jednotlivé konkrétní zaměstnance podniku.
- **agregace** – popisuje nový typ objektu z množiny typů objektů, které se stanou jeho komponentami. Jako příklad lze uvést typ objektu „zaměstnanec“ agregací jeho komponent „jméno, věk, adresa“ apod.
- **generalizace** – definuje vztah podmnožiny mezi výskyty dvou nebo více typů objektů. Jako příklad může posloužit objekt „zaměstnanec“ jako generalizace objektů „manažer a dělník“. Tyto objekty následně dědí všechny vlastnosti objektů, jich že generalizací.

Tyto tři typy abstrakce jsou vůči sobě nezávislé, ale zároveň žádný z nich nemůže být vyjádřen typem jiným. Jejich pomocí se určí, ale vstupních datových požadavků struktura typů objektů konceptuálního datového modelu. [3]

Formy analýzy datových požadavků

Pro identifikaci a analýzu vstupních datových požadavků lze v podstatě využít čtyři základní způsoby:

- dotazníky,
- pozorování,
- rozborem písemných materiálů,
- rozhovorem projektanta s uživateli systému.

Dotazníky

Jejich funkce je spíše doplňková a chybí jim praktická možnost osobní interakce. Je možné je využít spíše v úvodní fázi vývoje k ujasnění cílů projektu, rozsahu řešení a stanovení omezujících podmínek. Jejich výhoda je na druhé straně v nízkých nákladech při dotazování velkého počtu osob.

Pozorování

Z praktického hlediska se jedná o doplňkovou formu, podobně jako u dotazníku. To z důvodu časové náročnosti, finanční nákladnosti, nižší spolehlivosti a obtížnosti získání kompletního výsledku.

Rozbor písemných materiálů

Jde o hlavní součást postupu konceptuálního modelování. Předmětem zkoumání jsou všechny dokumenty, které mají z datového hlediska vztah k řešenému modelu. Písemné materiály je možné dle způsobu jejich analýzy do tří skupin:

- textové materiály (legislativní předpisy, návody, popis práce apod.),
- klasické (papírové) nebo elektronické podobě,
- formáty datových struktur již vytvořené a používané ve starších aplikacích.

Rozhovor projektanta s uživateli systému

Jedná se o řízený rozhovor ze strany vývojáře s uživatelem. Výhodou je volný popis a neomezená možnost charakterizování jakéhokoliv pozorovaného jevu. Nevýhodou může být nejednoznačnost popisu, nesrozumitelnost, dále pak časová náročnost. Ovšem jasnou předností této metody je osobní kontakt s budoucím uživatelem, přičemž výsledkem může být zjištění, že původně navržený scénář nemířil správně ke zjištění podstaty fungování systému a je tedy třeba otázky upravit, případně rozvést. Další možností je využití skupinového rozhovoru, jehož výhodou je interakce mezi respondenty ve stejném čase a tudíž značná úspora času. Důležitou součástí skupinového rozhovoru je vedení dokumentace. [4]

Grafická podoba konceptuálního modelu

K zachycení datového modelu na konceptuální úrovni se využívá celá řada modelovacích nástrojů. Mezi nejznámější a nejvíce využívané lze jednoznačně zařadit různé modifikace tzv. E-R diagramů / modelů (entity-relationship). Jako druhou nejvíce využívanou metodu lze označit tzv. diagram tříd.

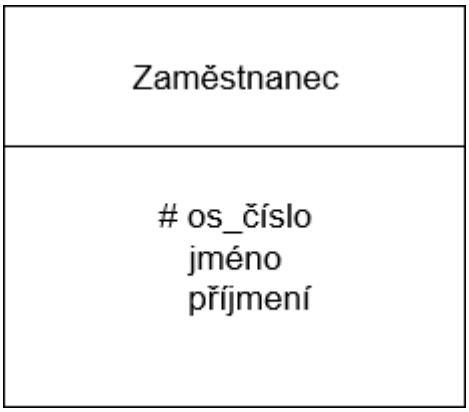
Metoda E-R diagramu

Používá se k vyjádření datových konstruktů (konstrukčních prvků) – entit (Entity), jejich podstatných vztahů (Relationship) a atributů (Attribute) těchto objektů a vztahů. Přestože v terminologické oblasti je problematika relativně jednotná, v grafické prezentaci lze najít jisté rozdíly. Mezi základní konstrukty tedy patří:

- entita,
- vztah,
- atribut,
- doména,
- klíč. [5]

Entita

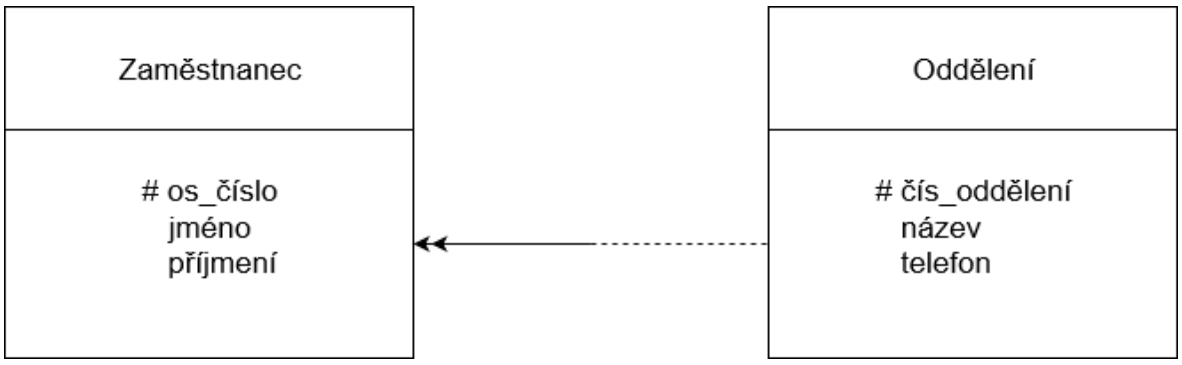
Jedná se o rozlišitelný a identifikovatelný objekt reálného světa, který popisujeme. Graficky se znázorňuje obdélníkem, v jehož horní části se nachází název entity a ve spodní části se uvádí výčet atributů. Název by měl být vyjádřen pomocí podstatného jména, viz obr. 2.



Obrázek 2: Grafické vyjádření entity [4].

Vztah

Zachycuje, jakým způsobem jsou entity vztažené mezi sebou. Graficky se vztahy vyjadřují spojnicí s verbálním popisem (slovesem) viz obr. 3. Nejběžnější typ vztahu se nazývá asociativní vztah, ten je dále charakterizován stupněm, kardinalitou a volitelností. [6]



Obrázek 3: Grafické vyjádření vztahu [4].

Stupeň

Definuje množství jednotlivých entit asociovaných v jednom konkrétním vztahu, přičemž nejnižší je stupeň jedna, kdy se vztah váže pouze k jedné entitě (unární nebo rekurzivní vztah). Vztah druhého stupně se označuje jako binární, mezi třemi ternární a analogicky dále.

Kardinalita

Popisuje počet výskytů entit účastnících se jednoho výskytu vztahu, neboli počet vztahů přiřazených k dané entitě. Výjimečně se může objevovat kardinalita pod názvem proporcionalita či multiplicita.

Kardinalitu můžeme vyjádřit celkem třemi způsoby, a to 1:1 – vztah, ve kterém na obou stranách vystupuje pouze jeden objekt dané entity; 1:N – na jedné straně je jediný objekt, který je ve vztahu s jedním nebo více objekty na straně druhé; M:N – každý z objektů je ve vztahu s více objekty na straně druhé.

Volitelnost

Určuje, zdali je vztah povinný či nepovinný ze strany jedné nebo druhé entity, zjednodušeně jestli každému výskytu vztahu musí příslušet jeden nebo několik výskytů příslušné entity. Volitelnost má grafickou podobu jako přerušovaná nebo plná čára.

Druhým typem vztahu je generický vztah (generalizace), jehož protikladem je specializace. Jedná se tedy o nadřazenou entitu (super-entitu), která může mít své podřadné entity (sub-entities). Podřazená entita představuje speciální případ nadřazené entity, dědí od ní všechny atributy a může k nim dále přidat své specifické atributy. Každá entita nesmí mít více jak jednu nadřazenou entitu. [7,8]

Atribut

Označuje základní vlastnosti konkrétní entity nebo vztahu. V grafické části jsou atributy uvedeny ve spodní části entity, viz obr. 2. V případě velkého množství atributů je lze v grafické části uvést odkázáním na příslušný seznam či tabulku. Atributy můžeme rozlišovat na jednoduché a složené. Jednoduché jsou nerozložitelné a mají pouze jednu komponentu (např. cena), zatímco atributy složené mají více komponent, které mají společný význam nebo použití (např. kontaktní údaje).

Doména

Reprezentuje množinu hodnot přiřazených jednomu nebo více atributům. Nemusí se jednat pouze o číselnou nebo textovou hodnotu, může to být i obrázek, video, zvuková stop aritmetická operace apod.

Klíč

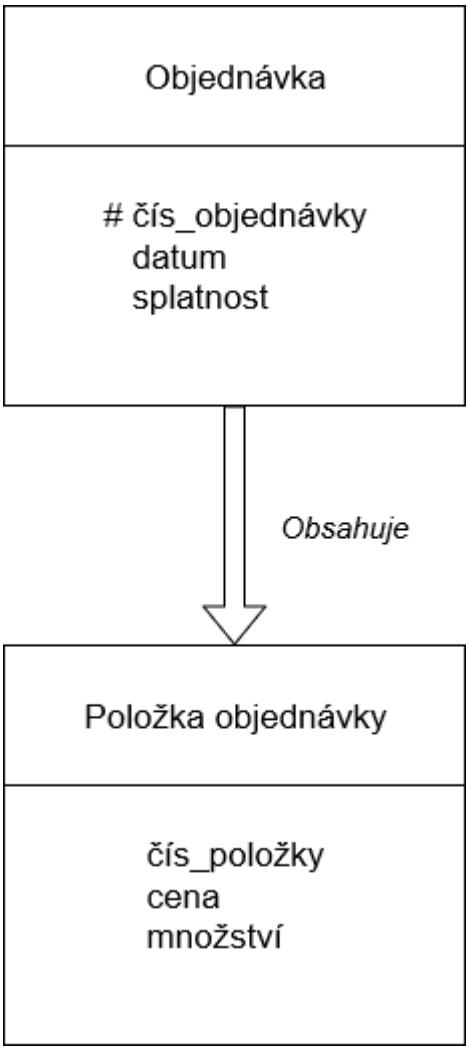
Klíč je jedním nebo několika atributy identifikujícími výskyty konkrétní entity. Rozeznáváme několik druhů klíčů. Jednoduchý klíč slouží k identifikaci entity pomocí jediného atributu. Složený klíč využívá více atributů k identifikování jedné entity. Sekundárních klíčů může mít entita několik, nejedná se však o jedinečný identifikátor. Z logiky věci tedy vyplývá, že v případě kandidátního klíče se jedná o jedinečný identifikátor výskytu dané entity. Platí obecná definice, že I je kandidátním klíčem entity E za určitých okolností:

- podmínka jedinečnosti – neexistují dva výskyty entity E, které mají stejnou hodnotu kandidátního klíče,
- podmínka neredukovatelnosti – pokud dojde k vypuštění jakékoliv části kandidátního klíče I, podmínka jedinečnosti přestane platit.

Takovýto jedinečný kandidátní klíč dané entity se stává klíčem primárním. Kandidátní klíč, který nenabyl statusu primární klíč, se stává klíčem alternativním. Rovněž pro volbu primárního klíče existuje řada doporučení:

- minimální množství atributů,
- změna hodnot není pravděpodobná,
- nejméně pravděpodobná skutečnost, že v budoucnu ztratí svoji jedinečnost,
- nejmenší počet znaků (u textových atributů) nebo nejmenší maximální hodnota (u číselných atributů),
- nejjednodušší použití ze strany uživatele. [7,8]

Graficky se primární klíč označuje symbolem # s doplněním názvem atributu viz obr. 3. Alternativní klíč zůstává bez označení. Existují rovněž entity, které nemají svůj vlastní klíč a jsou tedy závislé na primárních klíčích jiných entit – tyto případy se označují jako silné a slabé entity viz obr 4.



Obrázek 4: Silné a slabé entity [4].

Silná entita není svým primárním klíčem závislá na existenci jiné entity a v případě slabé entity neexistuje žádný její atribut, který by mohl sloužit jako jedinečný identifikátor. V grafické podobě je rozdíl mezi silnou a slabou entitou v neuvedení symbolu primárního klíče a vazba mezi nimi je popsána zdvojenou čarou. [7,8]

1.3 Logický datový model

Jedná se o schéma, které člení data do druhů a skupin. Současně také vymezuje vztahy mezi daty (tabulkami). Snaží se zachytit povahu procesů, které jsou následně důležité pro správnou organizaci dat v databázi. Logický datový model bývá nutnou podmínkou pro konstrukci fyzického datového modelu.

Při tvorbě logického modelu je možné využít několik rozdílných metodik – hierarchické modelování, síťové modelování, relační modelování, objektové modelování a relačně-objektové modelování.

Hierarchická koncepce

Jedná se o nejstarší aplikačně rozšířenou databázovou koncepci. Podstatou této koncepce je modelování dat do stromových struktur, kdy jsou uzly vyjadřující datové entity spojeny do hierarchie podle kardinality 1:N (jeden výskyt uzlu vyšší úrovně se vztahuje k N výskytům uzlu nižší úrovně apod.). Vykazuje ale některé nedostatky při modelování reality.

Síťová koncepce

Navazuje na hierarchickou koncepci, jde v podstatě o její rozšíření. Na rozdíl od hierarchického modelu poskytuje navíc vztahy o kardinalitě N:M.

Relační koncepce

Hlavním rysem relačního modelování, díky kterému je v dnešní době dominantní, je její jednoduchost a přehlednost. Od konceptuálního modelování přejímá některé datové struktury, jako jsou atribut, doména a klíč. V průběhu let se objevila celá řada nejrůznějších definic pojmu „relace“ přičemž nejsnadněji ji lze popsat jako tabulku.

Samotná databáze je potom kolekce relací, které jsou reprezentovány tabulkami (všechny informace jsou v tabulkách). Databázová relace je tedy vybavena pomocnou strukturou jménem relace, názvy atributů a definicí domén. Každá tabulka má primární klíč. Relační modelování využívá systém řízení báze dat (SŘBD). [9]

Objektové modelování

Objektové modelování je rozšířením relačního modelování. Jde o způsob nazírání na vznikající systém pomocí zjednodušené abstrakce reálného světa. Základním stavebním prvkem je objekt (entita), která v sobě zahrnuje jak datovou strukturu popisující určitou entitu, tak i pravidla chování této entity. Každý objekt dokáže provádět určité činnosti a komuni-

kovat s okolím, aniž by se vyžadovala znalost způsobu, kterým vnitřně pracuje. Pro každý objekt se uvádí čtyři charakteristické aspekty, tedy jedinečnost, zatříditelnost, mnohotvářnost a dědičnost. [10]

Relačně-objektová koncepce

Jedná se v podstatě o relační databáze obohacené o objektové prvky. V praxi není příliš využitelná pro aplikace s bohatě strukturovanými daty. [4]

1.4 Fyzický datový model

Představuje nejnižší míru abstrakce bez možnosti jakéhokoliv dalšího zjednodušení. Předchozí datové úrovně se přemění do daného programovacího jazyka. V této fázi vývoje je model již závislý na konkrétních specifikách použité databázové platformy. Implementační úroveň tedy definuje formu realizace modelu popsanou v konceptuální a logické úrovni. [11]

2 INFORMAČNÍ BEZPEČNOSTNÍ POLITIKA

Informační bezpečnostní politika se vztahuje na veškeré činnosti organizace v rámci působnosti Systému řízení bezpečnosti informací (ISMS) a týká se tedy informací, informačních systémů (IS), sítě, fyzického prostředí a pracovníků, kteří uvedené činnosti zajišťují. Dále obsahuje definice základních principů, odpovědnosti a pravomocí. Výstupem je dokument s názvem Bezpečnostní politika informačních systémů. Hlavními cíli jsou tedy:

- definovat hlavní cíle při ochraně informací,
- stanovit způsob, jak bezpečně je řešit,
- určit pravomoci a odpovědnosti. [12]

2.1 Terminologie

Oblast bezpečnosti informací obsahuje celou řadu důležitých pojmů a definic. Pro správně pochopení problematiky je nutné definovat alespoň ty základní.

Aktivum

Rozumíme všechny hmotné a nehmotné statky, vše co má pro majitele informačního systému nějakou hodnotu. Za nejcennější aktiva se považují především data a informace, jejich zneužití, ztráta nebo modifikace, by organizaci nebo určité osobě způsobily určitou škodu. Aktiva dělíme na hmotná a nehmotná:

- Hmotná aktiva – jsou tvořena uživatelskou technologií, především výpočetní technikou (počítače, servery, disková pole), komunikačními technologiemi (strukturovaná kabeláž, aktivní síťové prvky). Hodnotu těchto aktiv lze zpravidla přesně stanovit v závislosti na jejich pořizovací ceně.

Nehmotná aktiva – představují programové vybavení a data. Patří sem operační systémy, aplikační programy, programové nástroje pro správu a řízení informačního systému. Další nedílnou součástí nehmotných aktiv je know-how organizace. Nejvýznamnější hodnotu nehmotných aktiv představuje datová základna. [12]

Algoritmus

Můžeme definovat jako konečnou posloupnost či sekvenci pravidel, která jsou aplikována na konečnou množinu dat, a umožňuje řešit třídu problémů podobného typu. Tyto sady pravidel jsou typické pro jisté informační výpočty nebo činnosti. [24]

Bezpečnost

Jedná se o stav, kdy je systém schopen odolávat známým a předvídatelným vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně i celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí. Je to tedy míra stability systému a jeho primární a sekundární adaptace. [13]

Bezpečnostní analýza IS

Také analýza rizik, hrozeb, představuje odbornou analýzu informačního systému s cílem zjistit rizika a navrhnout protiopatření pro maximální zabezpečení zkoumaného IS. [12]

Data

Vhodným způsobem vyjádřená (zakódovaná) zpráva, která je srozumitelná příjemci (může být člověk nebo počítač) a přizpůsobená k dalšímu zpracování. Bezprostředně odráží zkoumanou skutečnost a představují nejnižší prvek informačního systému (primární data). Procházejí dalším zpracováním (sekundární data) například v počítači a po následné analýze se stávají podkladem pro formulace empirických tvrzení (faktů). Je možno je uchovávat na datových nosičích.

Data lze označit za základní zdroj informací, sama o sobě ale nejsou použitelná. Použitelné jsou za předpokladu, že jsou organizované nebo se s nimi zachází tak, aby se stala informacemi. [14]

Dostupnost

Představuje zachování odpovídajícího přístupu (a to i v případě havárie mateřského systému přechodem na záložní systémy) k informacím nebo službám v souladu s příslušným oprávněním (přístupová práva uživatele). [14]

Důvěrnost

Vlastnost, že informace není dostupná nebo není odhalená neautorizovaným jednotlivcům, entitám nebo procesům. [14]

Hrozba

Je skutečnost, událost, síla, okolnost, osoby, jejichž působením může dojít k poškození, zničení, ke ztrátě důvěrnosti nebo hodnoty aktiva. Hrozba je tedy jakékoliv nebezpečí,

známé, reálné nebo potenciální, související s rozvojem informačních technologií, které ohrožuje IS, nebo data v něm obsažená. [12]

Informace

Jedná se o význam přisouzený datům. Je to, co vyplývá z analýz, zpracování a prezentace dat v takové formě, která bude vhodná pro rozhodovací proces. Informace je subjektivní a existuje jen ve vztahu příjemce – uživatel.

Informace se rovněž stávají zbožím, mají jistou cenu, hodnotu, která závisí na mnoha faktorech. Lze ji kupovat, prodávat, takže potřebujeme posoudit hodnotu informace. Důležitá je vnitřní hodnota zprávy, její novota pro příjemce. Proto je tedy cennější takové sdělení, které přináší manažerovi, spolupracovníkovi apod. něco nového, co dosud nevěděl a může užít ke své činnosti. [15]

Informační a komunikační technologie (ICT)

Tento pojem zahrnuje veškeré informační technologie (IT) využívané pro komunikaci a práci s informacemi. Jedná se o vzájemnou komunikaci jednotlivých počítačů či uzavřených sítí. [15]

Informační bezpečnost

Chápeme ji jako zodpovědnost za ochranu informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot. [12]

Informační systém

Je to soubor prvků, které jsou spojeny vzájemnými vztahy, vazbami. Prvky informačního systému tvoří místa transformace dat a informací jako výpočetní technika – hardware (HW), lidé, programy – software (SW) apod. [15]

Integrita

Vlastnost, která potvrzuje a zaručuje neporušenost dat v průběhu jejich přenosu od zdroje k cíli. [14]

Protiopatření

Je jakákoliv činnost, technické zařízení, proces, mechanizmus, nebo cokoliv, co chrání IS a jeho části (aktiva) před působením konkrétních hrozeb nebo hrozby. Protiopatření může

chránit hrozby před působením hrozby úplně, nebo jen zmírňovat její působení a vzniklé škody. [12]

Riziko

Jedná se o pravděpodobnost, s jakou bude daná hodnota (aktivum) zničena, nebo poškozena působením konkrétní hrozby. Působí na slabou stránku této hodnoty. Je to míra ohrožení konkrétního aktiva. [12]

Zranitelnost

Je nedostatek, nebo slabina celého bezpečnostního systému nebo jeho části, která může být zneužita hrozbou tak, že dojde k poškození nebo zničení hodnot – aktiv. Každé aktivum je tedy zranitelné a jeho hodnotu ohrožují různé vlivy. V každém IS existují zranitelná místa – prvky, které jsou využitelná pro útočníka k útoku na data, nebo celý systém. Mohou to být slabiny SW, aplikace, ale i lidské (úmyslné i neúmyslné) chyby, neznalost, podcenění bezpečnosti. [12]

2.2 Bezpečnost informací

Zabezpečení IS připomíná zabezpečení ochrany významného objektu. Hlavní prioritou bezpečnosti informací je vyvážená ochrana důvěrnosti, integrity a dostupnosti dat. Pro maximální efektivitu je nezbytná kooperace bezpečnosti informační s personální, majetkovou a dalšími typy zabezpečení. Snahou a cílem provozovatele IS je co nejvyšší bezpečnost systému, který zaručuje minimální úniky, či možnost zneužití informací. [12,27]

Je nezbytné na ni pohlížet jako na elementární předpoklad úspěšných a důvěryhodných vztahů s klienty, obchodními partnery, zaměstnanci. Všechny osobní údaje, se kterými se pracuje, je nutné shromažďovat, zpracovávat a uchovávat v centrální databázi s vysokou úrovní zabezpečení, včetně komunikace mezi interními a externími počítači a serverem. Rovněž je důležité zabezpečit procesy, při kterých probíhá přenos citlivých dat.

Jak již bylo zmíněno výše, na informace je třeba se dívat jako na aktiva, které mají pro danou organizaci určitou hodnotu. Rovněž mohou existovat v rozdílných podobách - vytištěné, napsané na papíře, zachycené na film či v elektronické podobě.

Informační bezpečnosti lze dosáhnout implementací soustavy opatření, které mohou existovat například v podobě pravidel, natrénovaných postupů. Procedur, organizační struktury a programových funkcí

V jednoduchosti je informační bezpečnost v podstatě ochrana proti možným nebezpečím, minimalizuje rizika, obsahuje komplex administrativních, logických, technických a fyzických opatření pro prevenci, detekci a opravu nesprávného použití systému informací. [16]

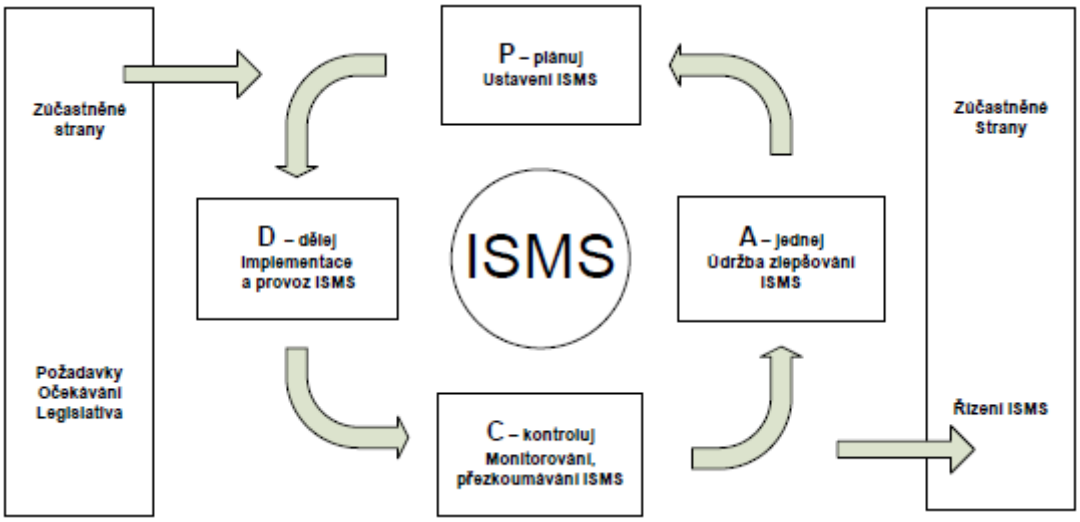
2.3 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací je překladem z anglického názvu Information Security Management System, vystupuje pod zkratkou ISMS a je součástí řízení organizace. Je založený na přístupu k rizikům činností, který je zaměřen na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbě a zlepšování bezpečnosti informací. Jedná se v podstatě o soubor kontrol, které organizace provádí, aby chránila své vlastní aktiva nebo další aktiva, za které zodpovídá s cílem eliminovat jejich případnou ztrátu či poškození:

- identifikováním aktiv, které se mají chránit,
- zvolením a řízením možných rizik informační bezpečnosti,
- zavedením opatření a jejich kontrolou.

Tento systém může být zaveden pro jednotlivou organizační složku společnosti, IS či jeho část nebo pro celou organizaci. ISMS postihuje tyto základní okruhy:

- IT bezpečnost,
- komunikační, personální, fyzická a administrativní bezpečnost,
- dokumentace,
- bezpečnostní funkce a mechanismy. [17,18]



Obrázek 5: Procesní model ISMS [16]

2.4 Metodiky

Nezbytným předpokladem pro zavedení nové koncepce řízení informatiky je podpora v podobě různých standardů, nejlepších zkušeností nebo metodik. Existuje řada metodik na tuto problematiku, ale dvě vyčnívají nejvíce – COBIT a ITIL. Jsou obecněji zaměřené a kromě oblasti řízení bezpečnosti se zabývají i dalšími aspekty řízení informatiky organizací. [14]

2.4.1 ITIL

Information Technology Infrastructure Library neboli ITIL, představuje soubor knih (nikoliv norem), který obsahuje popis způsobu procesního řízení služeb včetně infrastruktury IT, které jsou jejím prostřednictvím vykonávány. Koncentruje se na plánování, vytváření, modifikaci, dodávku, správu, analýzu a použití služeb IT.

Cílem této metodiky je poskytnutí uceleného souboru tzv. nejlepších zkušeností pro oblast řízení služeb IT a souvisejících procesů.

Tato metodika považuje útvar informatiky za poskytovatele služeb a předjímá, že by se měl změnit na obchodní útvar, který poskytuje ostatním útvarům informatické služby. [14]

Metodika ITIL se vyznačuje několika charakteristickými znaky:

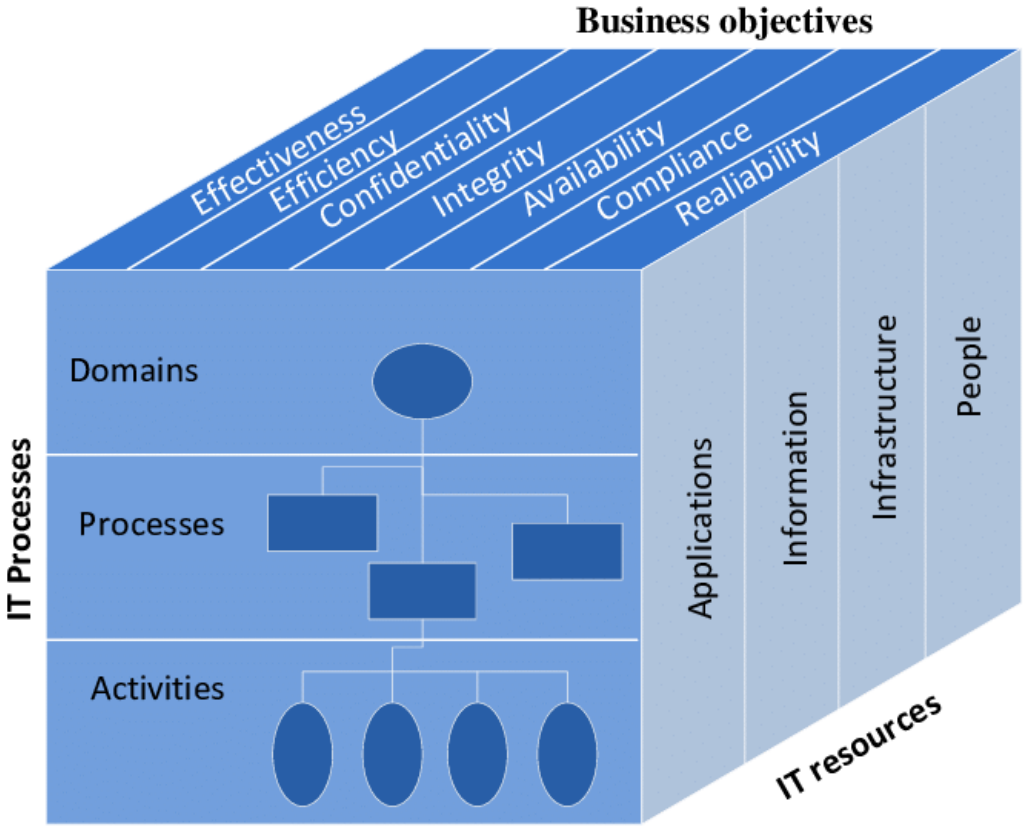
- **procesním přístupem** – každý proces předpokládá, že je určen jeho cíl a má přiděleného vlastníka procesu, definované vstupy, výstupy a aktivity,
- **nejlepšími zkušenostmi –** obsahuje shrnutí nejlepších zkušeností z praxe. S rostoucím množstvím implementací a tím analogicky lidí znalých této problematiky, se otevírá prostor pro její další zdokonalování,
- **respektováním individuality –** metodika poskytuje návod, co by se mělo udělat, ale nikoliv jakým způsobem by toho mělo být dosaženo, tudíž nabízí organizacím dostatečnou volnost,
- **zákaznickou orientací –** zvyšování produktivity práce zaměstnanců pomocí zvyšování jejich spokojenosti,
- **jednotnou terminologií –** jednotná terminologie znamená jednoduchou a jasnou komunikaci a eliminuje tudíž možné problémy vyplývající ze špatné komunikace,

- **nezávislostí na platformě –** ITIL je rámec, jež definuje hranice, pravidla, vazby a tím organizaci dává dostatečnou volnost. Nezáleží na tom, jaká informační a komunikační infrastruktura je řízena a ani na službách, které jsou touto infrastrukturou poskytovány. [14]

2.4.2 COBIT

V případě metodiky COBIT (Control Objectives for Information and Related Technology) se jedná o sadu všeobecně přijímaných procesů, návodů pro hodnocení ukazatelů a nejlepších praktických zkušeností, která má za cíl pomoci organizaci maximalizovat užitek plynoucí z informačních technologií. [14]

Hlavní snahou metodiky COBIT je jasně strukturovat vysoce složitý systém řízení IT tak, aby byla tato struktura srozumitelná pro řídící pracovníky a uživatele bez detailních znalostí IT. Metodika dovoluje těmto pracovníkům sestavit vhodná objektivní kritéria, podle kterých bude možné posuzovat úspěšnost či neúspěšnost jednotlivých oblastí IT. [17]



Obrázek 6: Kostka COBIT [19]

Požadavky na informace (informační kritéria) jsou v COBIT strukturovány do následujících skupin:

Efektivita (Effectiveness)

Definuje požadavky na včasné doručování relevantních informací ve správném, konzistentním a použitelném tvaru. [17]

Účinnost (Effiency)

Definuje požadavky na zpracování informací (nejekonomičtějším a neproduktivnějším způsobem) prostřednictvím optimálního využívání zdrojů informatiky. [17]

Důvěryhodnost (Confidentiality)

Definuje požadavky zahrnující oblast důležitých informací proti neautorizovanému použití (prozrazení). [17]

Integrita (Integrity)

Definuje požadavky týkající se přesnosti a kompletnosti informace ve vztahu k požadavkům podnikání a jeho očekáváním. [17]

Dostupnost (Availability)

Definuje požadavky vztahující se k dostupnosti informace pro podnikání (nyní, ale i v budoucnu) a týkající se také ochrany potřebných zdrojů (např. datových, technologických). [17]

Soulad (Compliance)

Definuje požadavky týkající se udržování souladu se zákony, regulacemi, směrnicemi a kontraktačními podmínkami, které se týkají procesů podnikání (hlavních podnikových procesů). [17]

Spolehlivost (Reliability)

Definuje požadavky vztahující se k přínosu informace pro rozhodování manažerů.

Tato informační kritéria vytváří jednu osu kostky COBIT. Druhá osa se skládá ze zdrojů IT (aplikace, informace, infrastruktura a lidé). Třetí osa kostky reprezentuje IT procesy (aktivity, procesy a domény). [17]

Domény (Domains)

Z kostky COBIT je zřejmé, že jsou definované různé úrovně podrobnosti. Nejobecnější jsou definice domén, které metodika rozděluje na:

- plánování a organizace,
- akvizice a implementace,
- dodávka a podpora,
- sledování a hodnocení. [14]

Procesy (Processes)

V rámci každé domény jsou spravovány procesy. Procesy jsou také někdy označována jako High Level Control Objectives a je jich celkem 34. [14]

Aktivity (Activities)

Každý proces je tvořen tzv. detailními kontrolními cíli. Je jich celkem 214. [14]

Struktura IT procesů vytváří v metodice COBIT „smyčku“, která odpovídá základním prvkům „životního cyklu“ IS. Životní cyklus kompletně pokrývá celý vývoj IS, který se skládá z jednotlivých etap navazujících na sebe. Každý IS lze popsat pomocí životního cyklu, jehož základními etapami je zachycení požadavků na systém, tvorba konceptuálního, logického a fyzického datového modelu, implementace, zavedení, testování, udržování systému a jeho provoz. V některých případech i jeho stažení z užívání. [17]

2.4.3 CRAMM

Metodika CRAMM (CCTA Risk Analysis and Management Method) je soubor SW nástrojů pro zavádění a podporu ISMS, pro zavádění identifikace a ohodnocení aktiv, analýzy rizik informačních systémů a sítí, k návrhu bezpečnostních opatření, určování havarijních požadavků na IS a k návrhům na řešení havarijních situací.

Pokrývá komplexně všechny fáze řízení rizik od samotné analýzy rizik až k návrhu protiopatření, včetně generování výstupů pro bezpečnostní dokumentaci.

Existují i specializované programy jako například CRAMM metodika, CRAMM express, CRAMM expert.

Metodika CRAMM plně podporuje proces zavádění ISMS v souladu s normou ISO/IEC 27001:2005. Dále vytváří a neustále aktualizuje kompletní bezpečnostní dokumentaci celého systému pro přípravu na certifikaci podle ISO/IEC 27001. [20, 17].

2.5 Normy ČSN ISO/IEC 2700x

Jedná se o sadu norem z oblasti informační bezpečnosti. V práci jsou uvedené pouze některé z nich.

ISO 27000 – slovník a celkový přehled ISMS

Norma poskytuje základní informace o modelu pro vytvoření a provozování systému řízení bezpečnosti informací. Podává informace o souboru norem zaměřených na ISMS. [16]

ISO 27001 – Specifikace pro systémy řízení bezpečnosti informací

Norma slouží jako základ pro posouzení ISMS pro organizaci jako celek nebo její část. Specifikuje požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování dokumentace ISMS v kontextu podnikatelských rizik organizace. Dále specifikuje požadavky na zavedení nástrojů řízení bezpečnosti, upravené podle potřeb jednotlivých organizací nebo jejich částí. [16]

ISO 27002 – Návod na implementaci opatření

Tato norma obsahuje návod pro zavedení a provoz ISMS. Poskytuje návody a všeobecné principy na návrh, implementaci, udržení a zlepšení ISMS v rámci organizace. Doporučení této normy představují všeobecné postupy vzhledem ke schváleným cílům řízení informační bezpečnosti. [16]

ISO 27003 – Návod na zavedení ISMS v souladu s ISO/IEC 27001:2005

Norma obsahuje především návod k implementaci ostatním norem série 2700x a je určena k využití ve všech typech organizací, které mají v úmyslu zavést ISMS podle ISO/IEC 27000:2005. [16]

ISO 27004 – Metriky ISMS

Norma je pro organizace pomůckou k měření a prezentaci efektivity jejich systémů řízení bezpečnosti informací, zahrnující řídící procesy definované v ISO/IEC 27001:2005 a opatření ISO/IEC 27002:2005. Norma byla publikována v prosinci roku 2009. [16]

ISO 27005 – Management rizik bezpečnostních informací

Norma poskytuje návody na řízení bezpečnostních rizik v oblasti ISMS. Norma svým obsahem podporuje požadavky stanovené v normě ISO/IEC 27001:2005. Obsahuje návody na implementaci procesů zaměřených na management rizik. Přístup napomáhá úspěšné

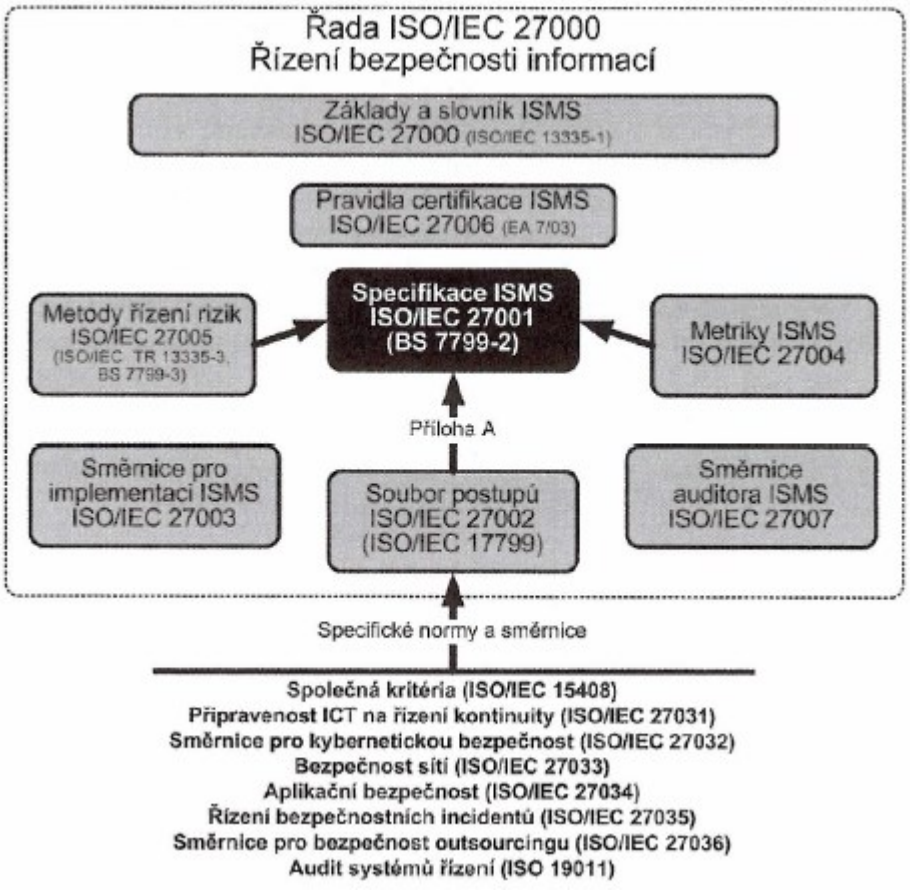
implementaci a naplnění požadavků ISO/IEC 27001:2005 v oblasti řízení rizik. Součástí normy jsou rovněž přílohy hrozeb, zranitelností, rizik atd. [16]

ISO 27006 – Návod na implementaci opatření

Norma specifikuje požadavky a současně poskytuje návody pro orgány zabývající se auditováním ISMS a certifikací těchto systémů řízení. Jejím účelem je podpora orgánů provádějících akreditaci certifikačních orgánů provádějící vlastní certifikaci ISMS. [16]

ISO 27008 – Doporučení pro auditování ISMS tzv. „technický audit“

Doplňuje normu pro auditování ISO/IEC 27007. Norma zpestřuje a konkretizuje auditování kontrol bezpečnosti informací oproti ISO/IEC 27007, která se zaměřuje na auditování managementu systému. [16]

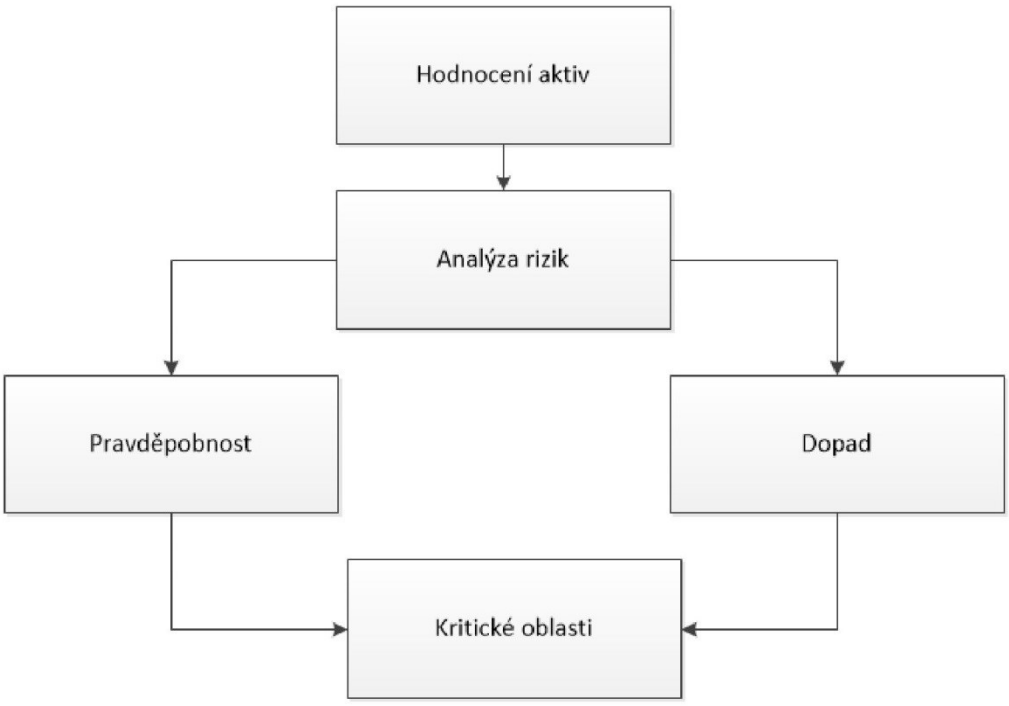


Obrázek 7:Normy řady ISO/IEC 27000 [14]

3 ANALÝZA RIZIK

Při analýze bezpečnosti IS je cílem prověřit aktuální stav bezpečnosti, odhalit slabá místa a najít nejvhodnější opatření k jeho odstranění. Výsledkem analýzy je podrobná dokumentace o bezpečnostní situaci IS organizace. Ochrana a bezpečnost informací ovšem nezahrnuje jen HW část. Zahrnuje rovněž veškeré činnosti a subjekty, které s informacemi přicházejí do styku a to jak s informacemi v elektronické, tak papíroví a jiné podobě. Z tohoto důvodu je třeba při analýze neopomenout a významně se zabývat lidským faktorem, neboť opomenutí něčeho v této oblasti se stává místem informačního úniku. Tohoto pak mohou využít jak neloajální zaměstnanci, tak i další pracovníci, kteří vůbec nemusejí být specialisté v oblasti informatiky.

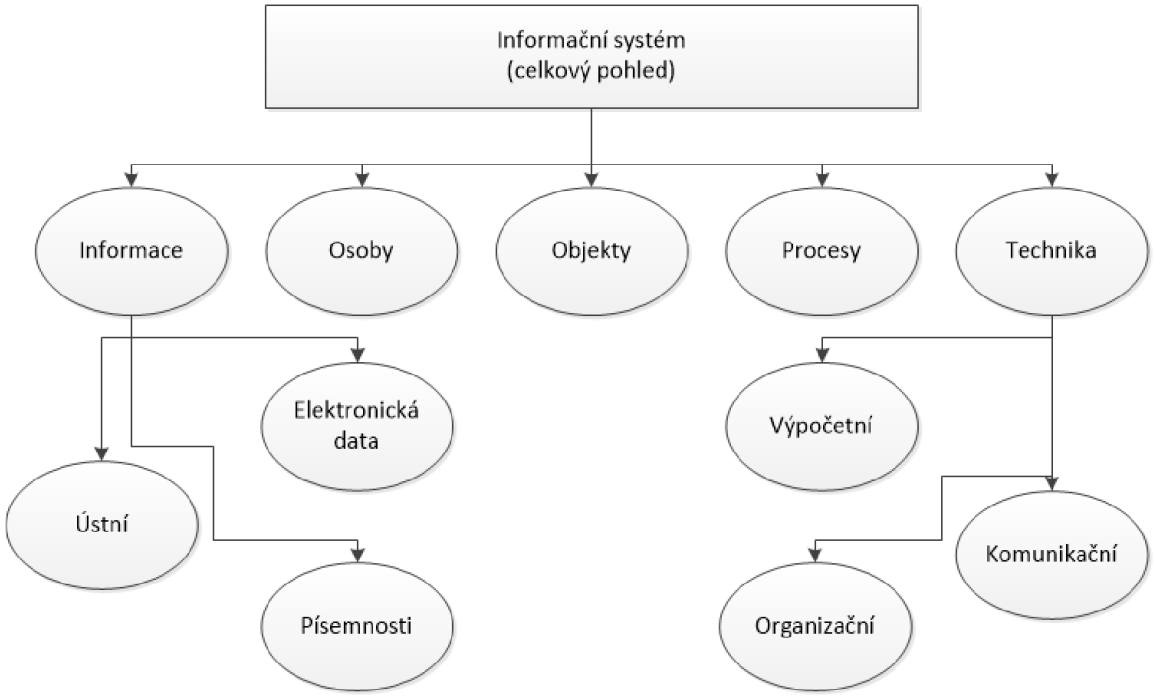
Aktivity dané organizace jsou nutně spojeny s podnikatelským rizikem. Podnikatelské riziko je definováno jako nebezpečí, že určitá událost nebo akce negativně ovlivní schopnost organizace dosahovat svých cílů a naplnit svoji strategii. [12]



Obrázek 8: Analýza rizik [12]

Při tvorbě bezpečnostního systému řízení rizik IS je analýza rizik nezbytná. Teprve na jejím základě lze jasně určit, které z kontrolních mechanismů jsou nezbytné a naopak které nadbytečné. Je rovněž důležité si uvědomit, že analýza rizik poskytuje dané aktuální in-

formace pouze v jistém časovém horizontu. Proto je třeba s ohledem na rychlý vývoj informačních technologií analýzy s určitou pravidelností aktualizovat. [12]



Obrázek 9: Rozsah analýzy rizik v informačních systémech [12]

Analýza rizik slouží ke stanovení míry rizika. Dle ohodnocení aktiv probíhá analýza hrozby, u kterých se stanoví míra pravděpodobnosti výskytu. Výsledkem je pak tedy seznam hrozeb. Pro hrozby, které ohrožují daný podnik, se navrhují bezpečnostní opatření, která zvyšují míru bezpečnosti aktiva. Analýza rizik obsahuje tyto kroky: [21]

- **stanovení hranice analýzy rizik** – zde je zapotřebí určit, která aktiva budou do analýzy zahrnuta a která ne. Tento krok je jednoznačně dá výsledný rozsah analýzy rizik.
- **identifikace aktiv** – vytváří soupis všech identifikovaných aktiv uvnitř definované hranice pro analýzu rizik,
- **stanovení hodnoty seskupování aktiv** – při stanovení hodnot aktiv lze vycházet z jednotlivých hledisek. Tyto hlediska se rozdělují na zkoumání nákladových nebo výnosových charakteristik aktiva. Používají se charakteristiky, které odpovídají vyšší hodnotě pro podnik.

- **identifikace hrozeb** – zde se vyhledávají hrozby, pro které musí být v dalších krocích nalezeno správné protiopatření. Výběr je třeba provádět tak, aby hrozby ohrožovaly alespoň jedno z identifikovaných aktiv.
- **analýza hrozeb a zranitelnosti** – každá identifikovaná hrozba musí být ohodnocena vůči všem skupinám aktiv, které byly předchozími kroky vytvořeny. Je potřeba, aby pro aktiva, u kterých se mohou dané hrozby uplatnit, byla určena úroveň hrozby vůči aktivu a také úroveň zranitelnosti aktiva vůči hrozbě
- **pravděpodobnost jevu** – v tomto kroku je potřeba zvážit pravděpodobnost výskytu hrozby. Je tedy potřeba tyto identifikované hrozby doplnit pravděpodobností jejich výskytu a tuto hodnotu brát v potaz při vytváření protiopatření. Je také potřebné zkoumat, zda se jedná o náhodné nebo nenáhodné jevy.
- **Měření rizika** – výše rizika vyplývá z hodnoty aktiva, úrovně hrozby a zranitelnosti aktiva. [22]

Hodnocení rizik je pro každou organizaci zcela individuální záležitost. Především je nutné vybrat metodiku pro identifikaci a ocenění rizik a definovat kritéria, na základě kterých se bude rozhodovat o tom, kdy je dané riziko pro organizaci přijatelné a kdy není. Analýza rizik je základním procesem pro ISMS. Je to jedna z nejdůležitějších etap pro stanovení bezpečnostní politiky organizace. Jedná se o proces porovnávání odhadovaných rizik proti přínosu nebo a/nebo ceně možných bezpečnostních opatření. Význam důsledného provedení analýzy rizik je zásadní. Mezi metody podrobné analýzy patří:

- matice s předdefinovanými hodnotami,
- odhady četnosti a možné změny rizik,
- rozlišení mezi riziky, které je a které není možné tolerovat,
- zařazení hrozeb podle míry rizika,
- analýza rizik využívající matice aktiv, hrozeb a zranitelnosti. [14]

4 CÍL PRÁCE A POUŽITÉ METODY

V této kapitole jsou popsány cíle diplomové práce s použitými metodami v praktické části práce.

Cílem práce bylo vytvoření konceptuálního datového modelu mobilní aplikace pro analýzu rizik v oblasti bezpečnosti informací. Součástí datového modelu bude rovněž grafický návrh s popisem funkčnosti jednotlivých kroků, které tvoří kostru aplikace. Jedná se o přihlášení do aplikace, funkcionalitu úvodní obrazovky, vytvoření profilu, návrh bezpečnostních opatření, nahrání profilu, smazání profilu a funkce náhledu.

Práce se zaměřuje na ověření možnosti vytvoření konceptuálního datového modelu aplikace pro analýzu rizik v rámci mobilního operačního systému Android.

K naplnění cílů vymezených v rámci této práce byly využity následující vědecké metody:

- **Modelování -** model je zjednodušený obraz skutečnosti. Modelováním pak rozumíme aplikaci různých druhů modelů na řešení dané problematiky. Tato metoda byla využita pro vytvoření praktické části práce v kapitole č. 6 a 7.
- **Simulace -** napodobování skutečné situace situací modelovou. Metoda simulace je částečně využita v 7. kapitole práce.
- **Analýza -** je proces reálného nebo myšlenkového rozkladu zkoumaného objektu na dílčí části, které se následně stávají předmětem dalšího zkoumání. Jde o rozbor vlastností, vztahů, faktů postupující od celku k částem. Analýza předpokládá, že v každém jevu je určitý systém a platí v něm ustálené zákonitosti fungování systému. Tato metoda je využita v kapitolách č. 1, 2 a 3.
- **Syntéza -** je myšlenkové spojení poznatků získaných analytickými metodami v celek. Syntéza je základem pro pochopení vzájemné souvislosti jevů. Syntéza je sumarizací poznatků vedoucí k získání nových poznatků, vztahů a zákonitostí ve kvalitativně vyšší úrovni. Tato vědecká metoda byla využita v kapitolách č. 5 a 6.

II. PRAKTICKÁ ČÁST

5 APLIKACE ARBIN

Tato kapitola stručně charakterizuje funkce a možnosti mnou navržené aplikace pro analýzu rizik v oblasti bezpečnosti informací neboli ARBIN. Aplikace využívá metodu matice zranitelnosti a matice míry rizika, do kterých jsou zaneseny hodnoty dle předchozího identifikování a ohodnocení vytipovaných aktiv a hrozeb uživatelem.

U výpočtu hodnoty aktiva je využit součtový algoritmus, kde je součet hodnot jednotlivých kritérií dělený jejich počtem. Na základě teoretických východisek (metodika COBIT a technické normy informační bezpečnosti ISO/IEC 2700x) jsem do výpočtu zahrnul celkem šest kritérií, podle kterých se hodnota aktiva určí.

$$\frac{Dv + Ds + In + Au + Od + Sp}{6}$$

Kde:

Dv – důvěrnost,

- ztráta důvěrnosti může vést ke ztrátě důvěry vůči zákazníkům, právní odpovědnosti, finanční ztrátě apod.

Ds – dostupnost,

- ztráta dostupnosti může vést k neschopnosti vykonávat kritické činnosti.

In – integrita,

- ztráta integrity může vést k přijetí nesprávných rozhodnutí.

Au – autenticita,

- ztráta autenticity může vést k použití neplatných dat, která vedou k neplatným výsledkům.

Od – odpovědnost,

- ztráta odpovědnosti může vést k podvodu, špionáži, krádeži.

Sp – spolehlivost,

- ztráta spolehlivosti může vést k nespolehlivým dodavatelům, demotivaci zaměstnanců.

Pro hodnocení těchto šesti kritérií je stanovena škála 1 – 5, přičemž 1 je nejnižší a 5 je nejvyšší.

Výsledný výpočet je zaokrouhlován na celá čísla. Tato hodnota aktiva, označovaná písmenem „A“. Váhu hodnoty aktiva lze nalézt v tabulce pro hodnocení aktiv.

Tabulka 1: Hodnocení aktiv [Vlastní]

Hodnota aktiva	Popis	Dopad
1	Nevýznamné	Nemá dopad na chod organizace
2	Méně významné	Minimální dopad na organizaci
3	Významné	Znatelný dopad na organizaci, možnost omezení jejího chodu a finanční ztráty
4	Cenné	Velký dopad na organizaci, omezení jejího chodu a finanční ztráta
5	Velmi cenné	Existenční potíže

Dalším krokem je určení pravděpodobnosti identifikovaných hrozeb. Tato škála udává hodnotu 1 jako nejmenší pravděpodobnost hrozby a hodnotu 5 jako nejvyšší pravděpodobnost hrozby.

Tabulka 2: Hodnocení hrozeb [Vlastní]

Hodnota	Popis
1	Velmi malá pravděpodobnost hrozby
2	Malá pravděpodobnost hrozby
3	Střední pravděpodobnost hrozby
4	Vysoká pravděpodobnost hrozby
5	Velmi vysoká pravděpodobnost hrozby

V matici zranitelnosti se určí zranitelnost pro každou konkrétní dvojici aktivum – hrozba, přičemž hodnota 1 je nejnižší a hodnota 5 nejvyšší zranitelnost. V případě, že hrozba nemůže využít zranitelnosti k poškození aktiva, se pole zanechá prázdné.

Výsledná míra rizika se promítne v matici míry rizika, kde jsou jednotlivé hodnoty barevně podbarveny a jejich výpočet vychází ze vzorce:

$$A \times P \times Z$$

Kde:

A – hodnota aktiva.

P – pravděpodobnost hrozby.

Z – zranitelnost.

Součin těchto tří parametrů vytvoří hodnotu, která se dělí do 5 kategorií, tato hodnota se pohybuje od 0 do 125.

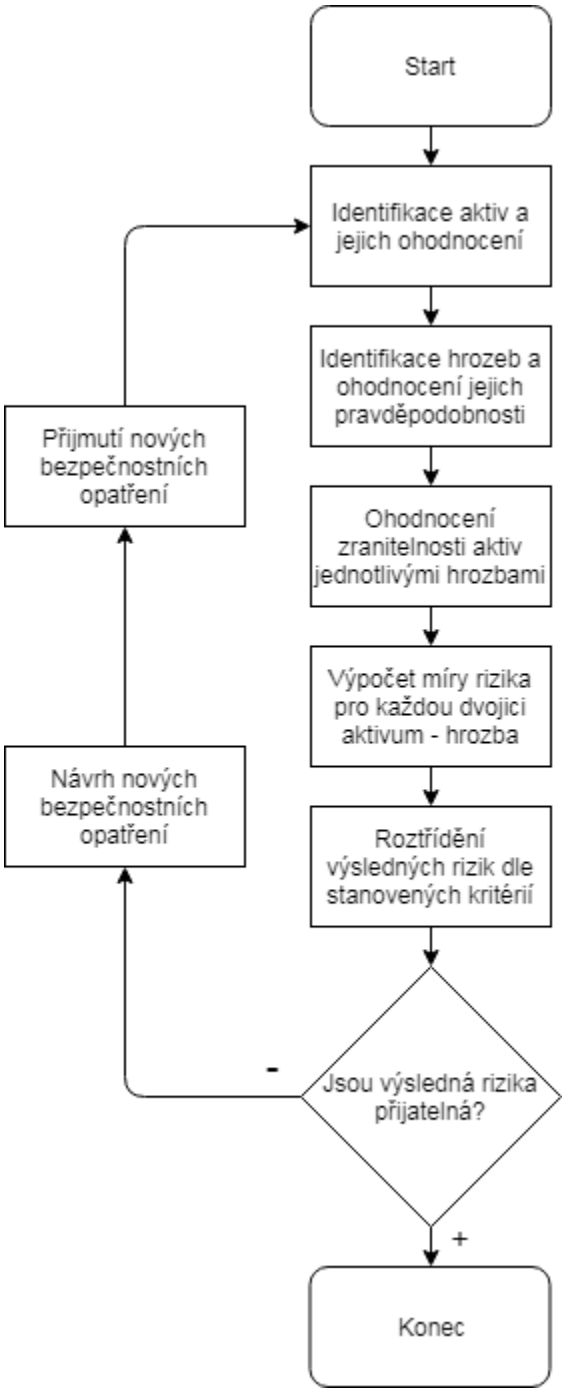
Tabulka 3: Hodnocení míry rizika [Vlastní]

Hodnota	Míra rizika
0 – 10	Bezvýznamné riziko
11 – 20	Akceptovatelné riziko
21 – 40	Mírné riziko
41 – 70	Nežádoucí riziko
71 – 125	Nepřijatelné riziko

Další možnosti aplikace je navrhnutí bezpečnostních opatření dle výsledků z matice míry rizik. Tyto opatření se navrhují pro konkrétní dvojici aktivum – hrozba a je možno na jejich základě upravit jakoukoliv hodnotu parametru, který je obsažen ve výpočtu. V případě přijmutí navrhnutého bezpečnostního opatření dojde k přepočtu vzorců a stanovení nové míry rizika. Posloupnost těchto kroků lze vidět na obrázku č. 10.

6 KONCEPTUÁLNÍ DATOVÝ MODEL APLIKACE

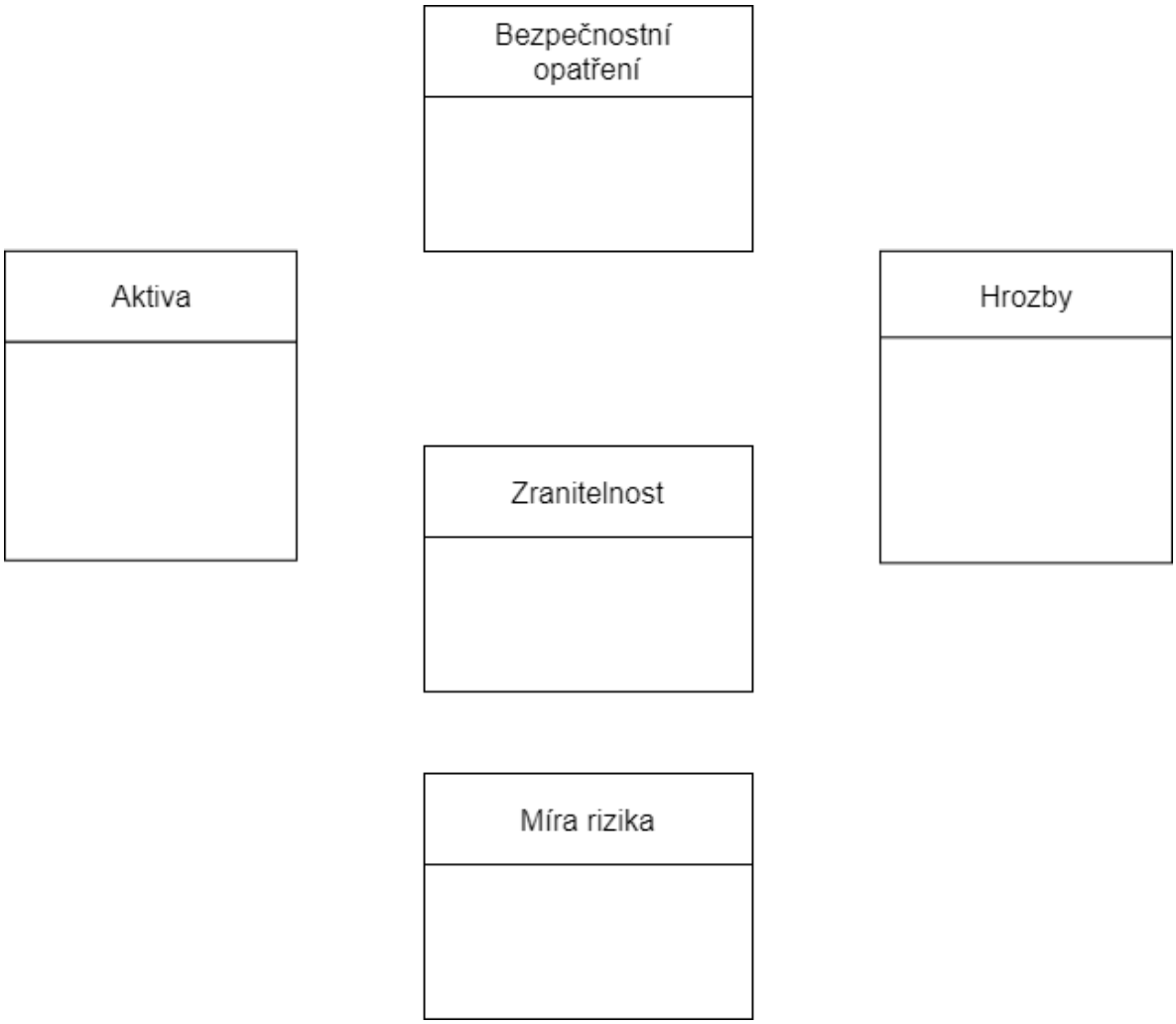
Tvorba konceptuálního datového modelu vycházela z analýzy dostupných dokumentů popsaných v teoretické části. Na jejich základě bylo možné definovat jednotlivé entity včetně dalších stavebních konstruktů, nezbytných pro tvorbu konceptuálního datového modelu. Při tvorbě konceptuálního datového modelu bylo využito metody E-R diagramu a tabulek obsahujících výčet jeho atributů.



Obrázek 10: Proces analýzy rizik za využití aplikace ARBIN [Vlastní]

6.1 Definování entit

Pro potřeby vytvoření datového modelu na konceptuální úrovni bylo definováno celkem pět entit, tyto entity jsou graficky znázorněny na obr. č. 11. Jedná se tedy o entity aktiva, hrozby, zranitelnost, míra rizika a bezpečnostní opatření.



Obrázek 11: Vymezení entit [Vlastní]

6.2 Definování atributů a klíčů

Atributy pro konkrétní entity byly vybrány na základě analýzy teoretických poznatků z 2. kapitoly této práce. Seznam atributů byl podle jednotlivých entit sestaven do tabulek společně se zkratkami. Součástí je rovněž i následné definování klíčů entit viz obr. č. 12.

Tabulka 4: Vymezení atributů pro entitu aktiva [Vlastní]

Entita	**Aktiva**
Atributy	**Zkratky atributů**
#ID_aktiva	#ID
Typ_aktiva	typ_a
Důvěrnost	dv
Integrita	in
Dostupnost	ds
Autenticita	au
Odpovědnost	od
Spolehlivost	sp

Tabulka 5: Vymezení atributů pro entitu hrozby [Vlastní]

Entita	**Hrozby**
Atributy	**Zkratky atributů**
#ID_hrozby	#ID
Typ_hrozby	typ_h
Pravděpodobnost	prav

Tabulka 6: Vymezení atributů pro entitu zranitelnost [Vlastní]

Entita	**Zranitelnost**
Atributy	**Zkratky atributů**
ID_zranitelnost	ID
#ID_aktiva	#ID
#ID_hrozby	#ID
Zranitelnost	zran

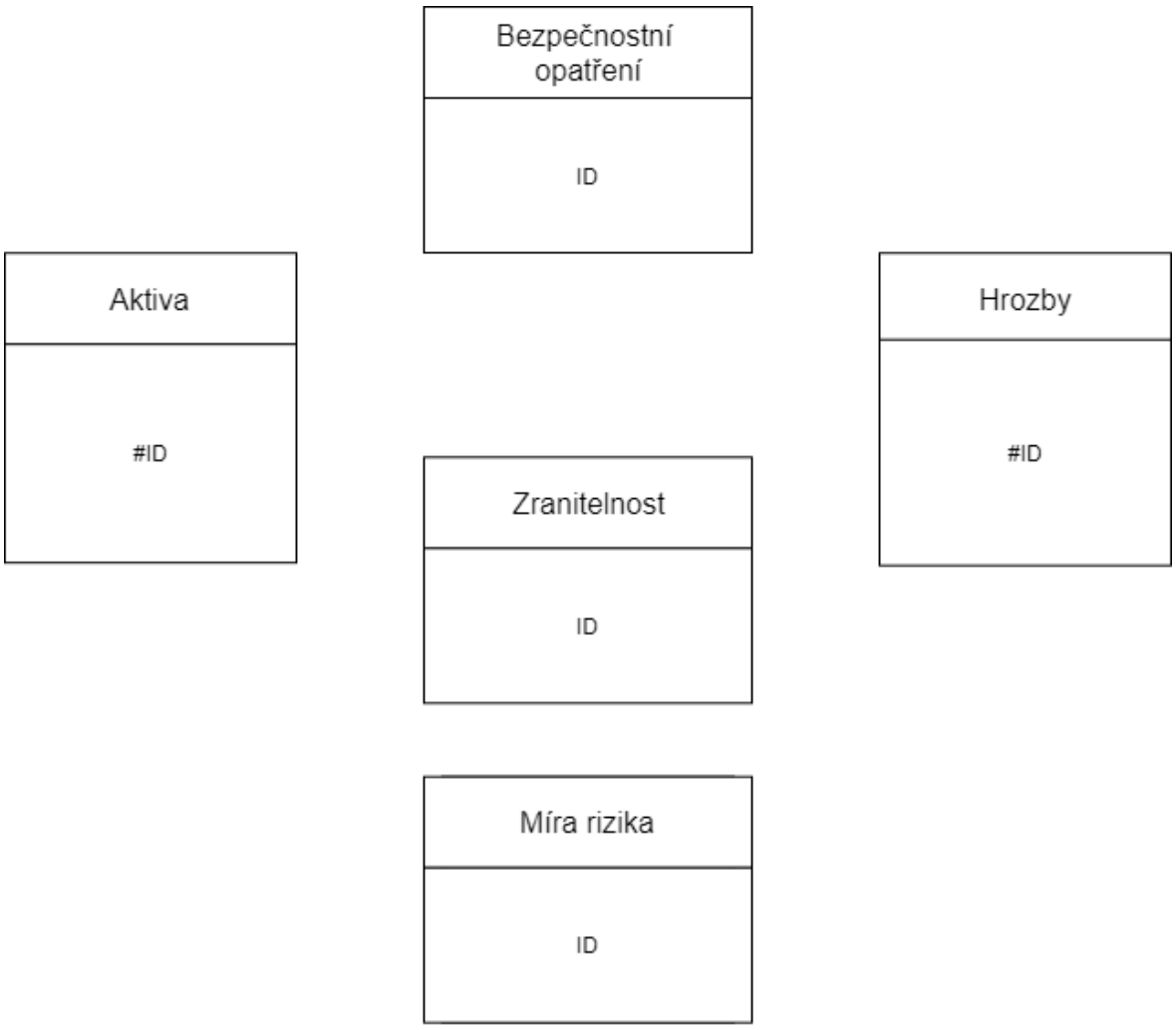
Tabulka 7: Vymezení atributů pro entitu míra rizika [Vlastní]

Entita	**Míra rizika**
Atributy	**Zkratky atributů**
ID_míra_rizika	ID
#ID_aktiva	#ID
#ID_hrozby	#ID
Hodnota_aktiva	hod_ak
Výsledná_míra_rizika	vys_mr

Tabulka 8: Vymezení atributů pro entitu bezpečnostní opatření [Vlastní]

Entita	**Bezpečnostní opatření**
Atributy	**Zkratky atributů**
ID_bezpečnostní_opatření	ID
#ID_aktiva	#ID
Typ_bezpečnostní_opatření	typ_bo

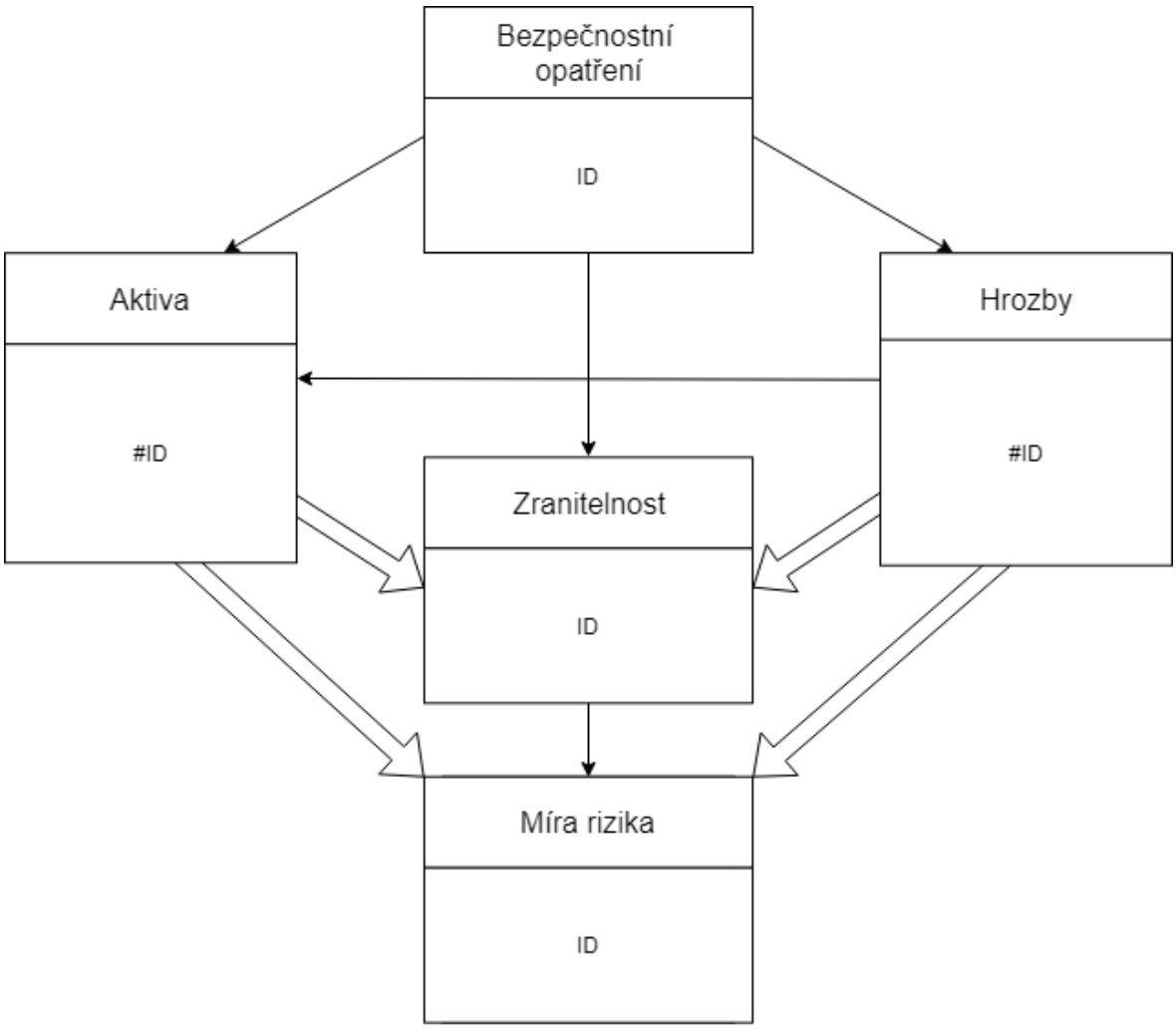
V rámci E-R diagramu byl primární klíč definován u entit aktiva a hrozby. Primární klíč entity aktiva se nachází v podobě cizího klíče rovněž u entity zranitelnost, míra rizika a bezpečnostní opatření. Primární klíč entity hrozby se nachází v podobě cizího klíče u entit zranitelnost a míra rizika. Všechny klíče jsou prezentovány v podobě identifikačního čísla viz obr. č. 12.



Obrázek 12: Vymezení klíčů [Vlastní]

6.3 Definování vztahů

V řadě třetím krokem v procesu tvorby konceptuálního datového modelu je vymezení vztahů mezi jednotlivými entitami. Dle výše napsané 1. kapitoly rozeznáváme u E-R diagramu silné a slabé entity. Mezi silné entity jsou zařazeny entity aktiva a hrozby, naopak mezi slabé patří entity zranitelnost, míra rizika a bezpečnostní opatření viz obr. č. 13.



Obrázek 13: Vymezení vztahů [Vlastní]

6.4 Definování domén

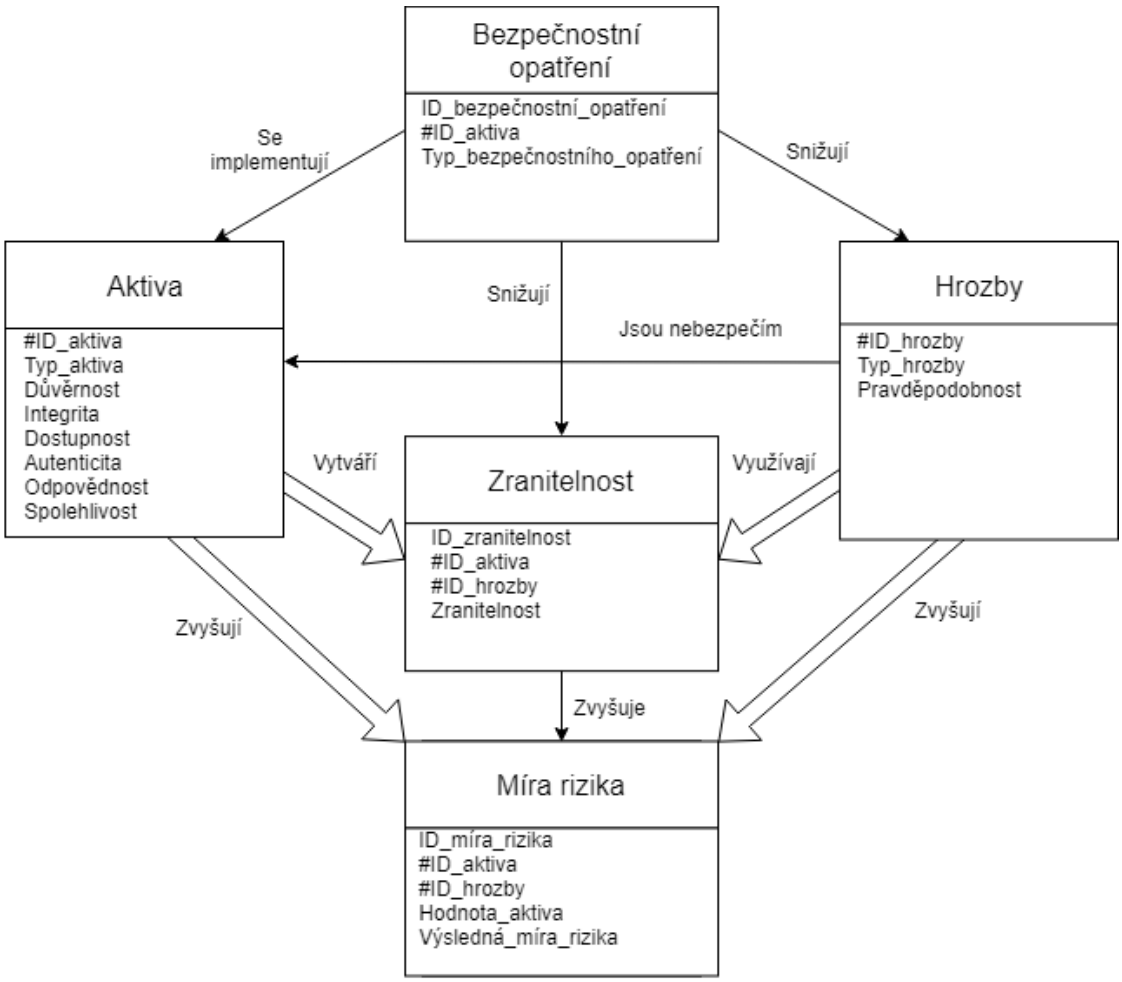
Finálním krokem před integrací dílčích části konceptuálního datového modelu je stanovení a definování domén pro již existující atributy jednotlivých entit. Jelikož bylo celkově navrženo relativně malé množství atributů pro tento model, jsou všechny domény znázorněny v tabulce č. 9 společně s jednotlivými atributy daných entit. Prázdné rámečky jsou vyplňované samostatně uživatelem (mimo ID).

Tabulka 9: Vymezení domén [Vlastní]

Entita	Atribut	Doména
Aktiva	#ID_aktiva	
	Typ_aktiva	
	Důvěrnost	1/2/3/4/5
	Integrita	1/2/3/4/5
	Dostupnost	1/2/3/4/5
	Autenticita	1/2/3/4/5
	Odpovědnost	1/2/3/4/5
	Spolehlivost	1/2/3/4/5
Hrozby	#ID_hrozby	
	Typ_hrozby	
	Pravděpodobnost	1/2/3/4/5
Zranitelnost	ID_zranitelnost	
	#ID_aktiva	
	#ID_hrozby	
	Zranitelnost	1/2/3/4/5
Míra rizika	ID_míra_rizika	
	#ID_aktiva	
	#ID_hrozby	
	Hodnota_aktiva	$\frac{Dv + Ds + In + Au + Od + Sp}{6}$
	Výsledná_míra_rizika	$A \times P \times Z$
Bezpečnostní opatření	ID_bezpečnostní_opatření	
	#ID_aktiva	
	Typ_bezpečnostní_opatření	

6.5 Integrace dílčích částí modelu

V závěrečném kroku návrhu konceptuálního datového modelu se dílčí části sloučí do jednoho modelu. E-R diagram byl doplněn o výčet atributů jednotlivých entit a v případě vztahů o legendu upravujících vazby mezi entitami. Po realizaci tohoto kroku je konceptuální model dokončen a připraven k logickému modelování.



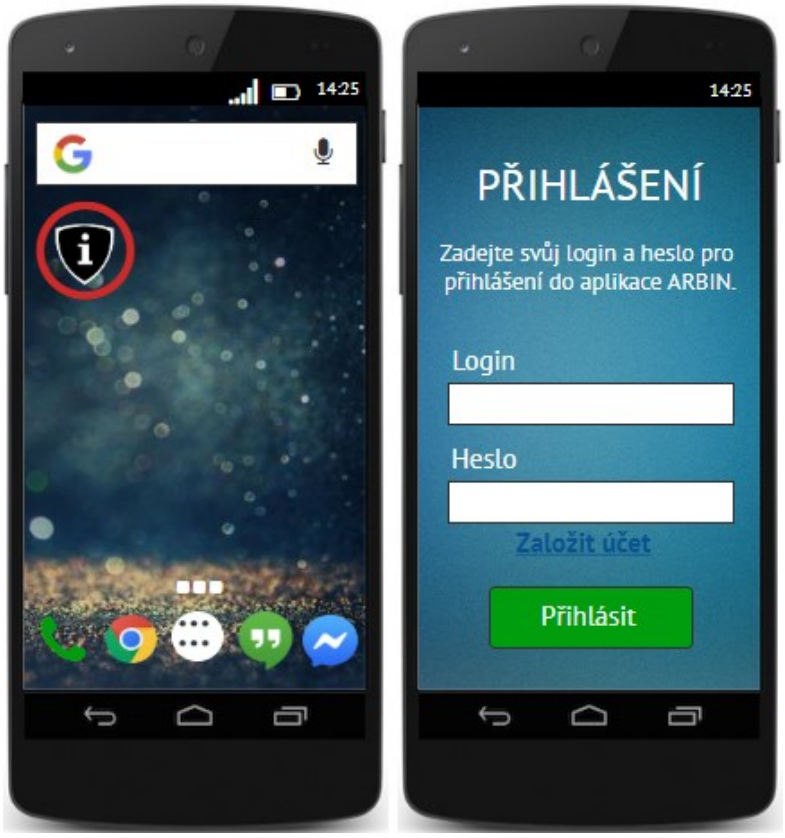
Obrázek 14: Návrh konceptuálního datového modelu [Vlastní]

7 NÁVRH UŽIVATELSKÉHO ROZHRANÍ

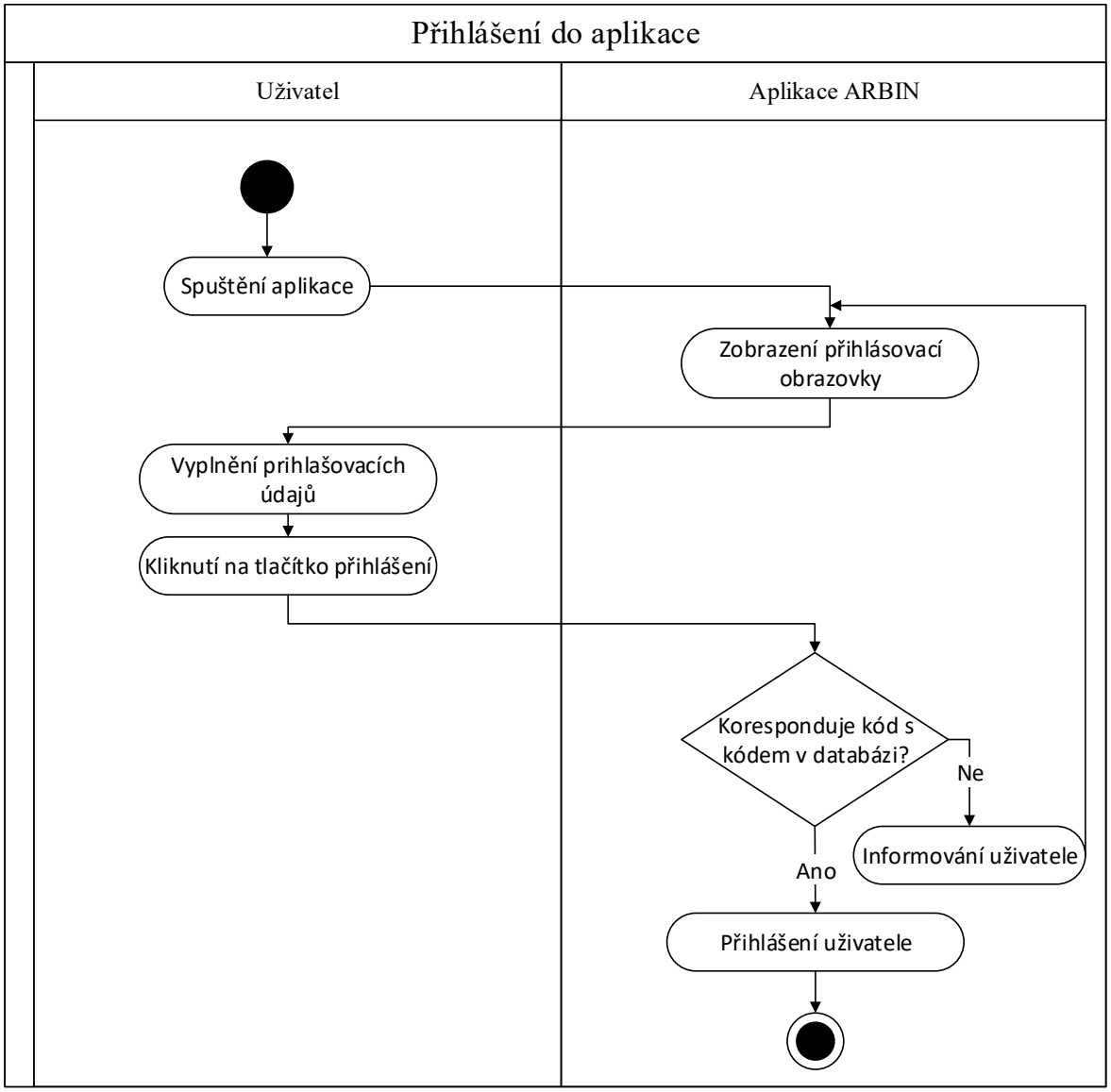
Obsahem této kapitoly je grafická vizualizace jednotlivých segmentů navrhované aplikace z pohledu uživatele, včetně schématu a popisu jejich funkčnosti.

7.1 Přihlášení

Po spuštění aplikace (zvýrazněná červeným kruhem) se zobrazí přihlašovací stránka. Stránka obsahuje dvě editovatelné položky „Login“ a „Heslo“ a možnost „Založit nový účet“ viz obr. č. 15. Po zadání údajů a stisknutí tlačítka „přihlásit“ se zobrazí hlavní menu aplikace. Schéma přihlášení do aplikace lze vidět na obr. č. 16.



Obrázek: 15 Obrazovka přihlášení do aplikace [Vlastní]



Obrázek 16: Schéma přihlášení do aplikace [Vlastní]

7.2 Úvodní obrazovka

Úvodní obrazovka obsahuje tzv. Action bar, neboli horní panel s názvem „Hlavní menu“. Kliknutím na tuto možnost se otevře horní panel (obr. č. 17) s položkami „Číselníky“, „Nápověda“, „O aplikaci“ a „Ukončit“.

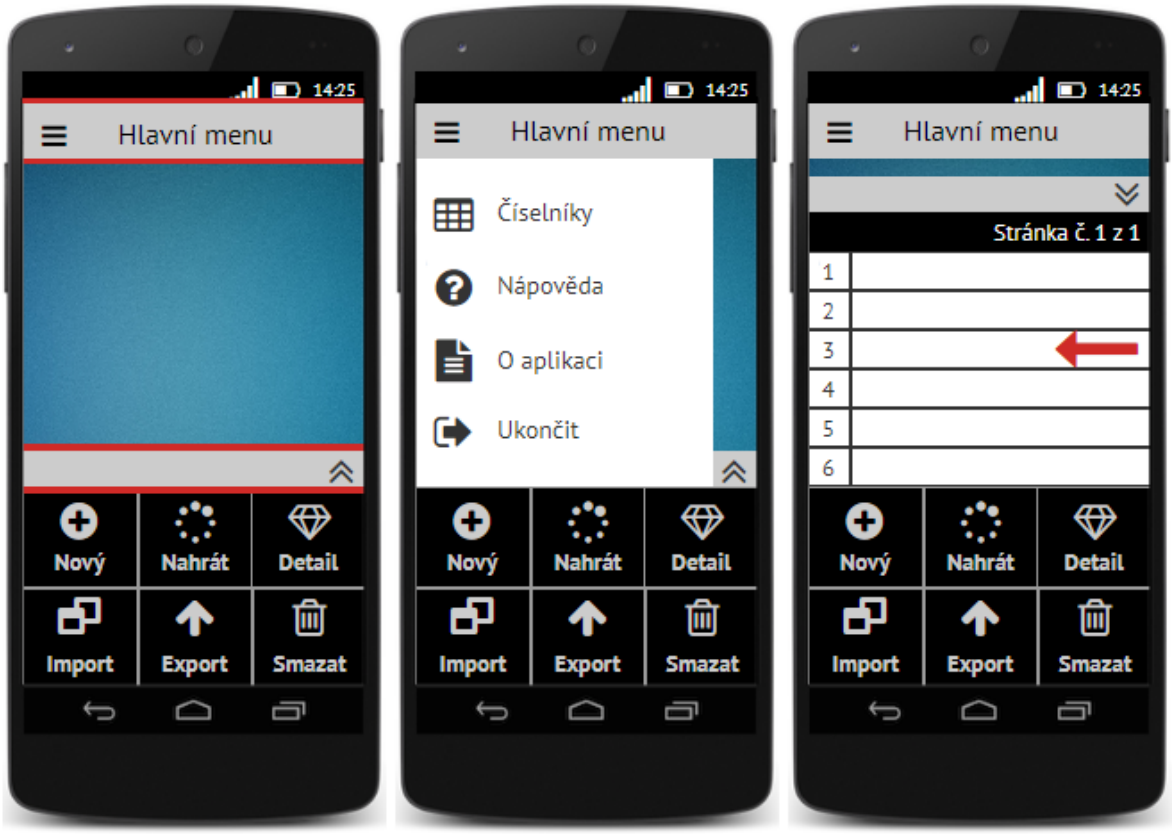
Položka „Číselníky“ obsahuje tabulky hodnot jednotlivých parametrů. Tyto číselníky se zde nacházejí celkem čtyři, tedy číselníky pro aktiva (A), hrozby (H), míru rizika (R) a ostatní (O - zde jsou definovány hodnoty pro zranitelnost a hodnoty pro kritéria hodnotící aktiva). Tyto číselníky označené zkratkami se nachází na levé straně obrazovky, po kliknutí se daný číselník dostane do popředí, přičemž se aktualizuje tabulka. Číselníky charakte-

rizuje ikonka s tabulkou, která slouží při aktivaci pro rychlou nápovědu při hodnocení jednotlivých parametrů (červeně zvýrazněná). Graficky jsou znázorněny na obr. č. 18.

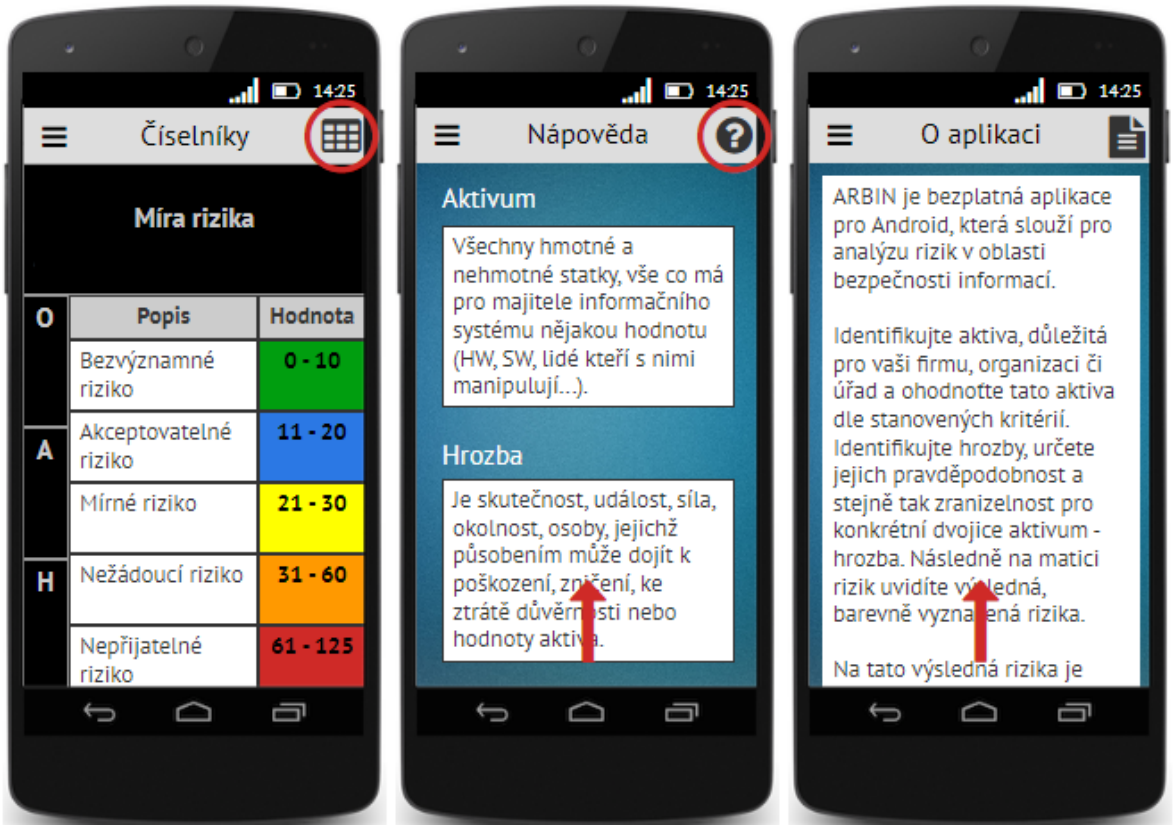
Položka „Nápověda“ obsahuje základní informace a terminologii pro správně pochopení kontextu problematiky. Charakterizuje ji ikonka s otazníkem, která slouží pro rychlou nápovědu při pozdějším vývoji vlastní analýzy (červeně zvýrazněná). Provedením gesta ve směru šipky lze položku posouvat. Graficky je znázorněny na obr. č. 18.

Položka „O aplikaci“ poskytuje popis samotné aplikace, k čemu slouží, k jakým účelům je ji možné využít a celkově popisuje její funkčnost. Provedením gesta ve směru šipky lze položku posouvat. Graficky je tato obrazovka znázorněna na obr. č. 18.

Položka „Ukončit“ slouží k ukončení aplikace a návratu na domovskou obrazovku.



Obrázek 17: Obrazovka otevření hlavního panelu [Vlastní]



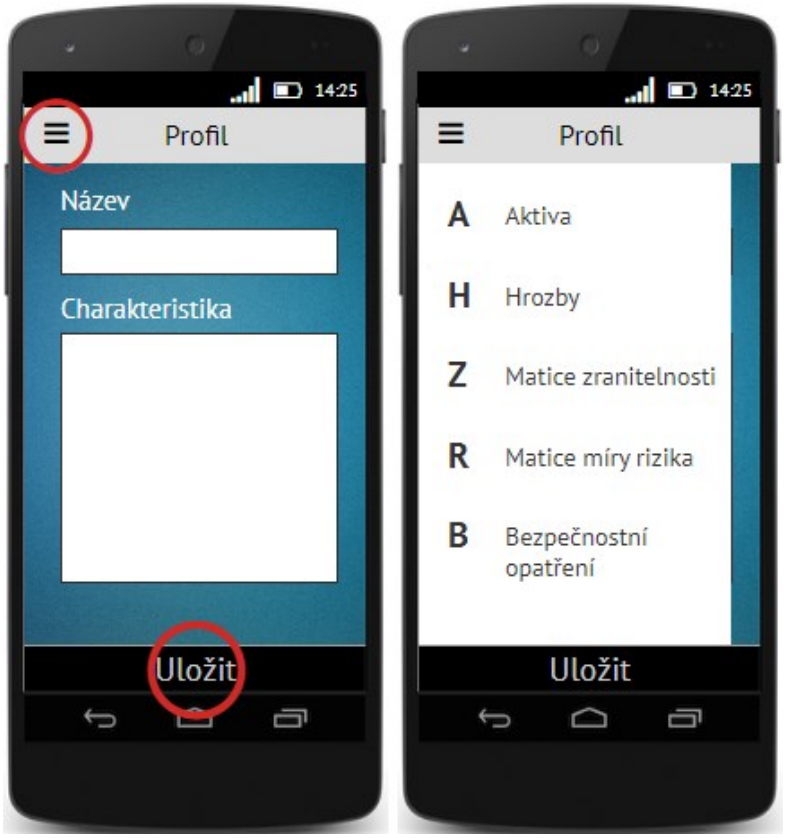
Obrázek 18: Obrazovka číselníky, nápověda, o aplikaci [Vlastní]

Další aktivitou na úvodní obrazovce je vysouvací panel s přehledem profilů nacházející se nad spodním menu (zvýrazněno červenou barvou). Graficky je zviditelněný dvojitou šipkou. V tomto panelu je možné označit jednotlivé profily a provádět s nimi činnosti z nabídky spodního menu. Mezi jednotlivými stránkami lze listovat provedením gesta ve směru šipky viz obr. č. 17.

Posledním výrazným prvkem uživatelského rozhraní úvodní obrazovky je spodní menu, které je rozděleno na šest polí. Každé z těchto polí má svoji specifickou funkci. Tyto funkce je možné aktivovat až po vybrání příslušného profilu (kromě položky „Nový“). Konkrétně tedy obsahuje položku „Nový“ pro vytvoření nového profilu, položku „Nahrát“ pro nahrání a úpravu již existujícího profilu, položku detail pro rychlý náhled na profil, položku „Import“ pro importování profilů vytvořených jinými uživateli, položku „Export“ pro exportování profilu do jiného formátu. Poslední položkou je „Smazat“, která slouží k vymazání nechtěných profilů.

7.3 Založení nového profilu

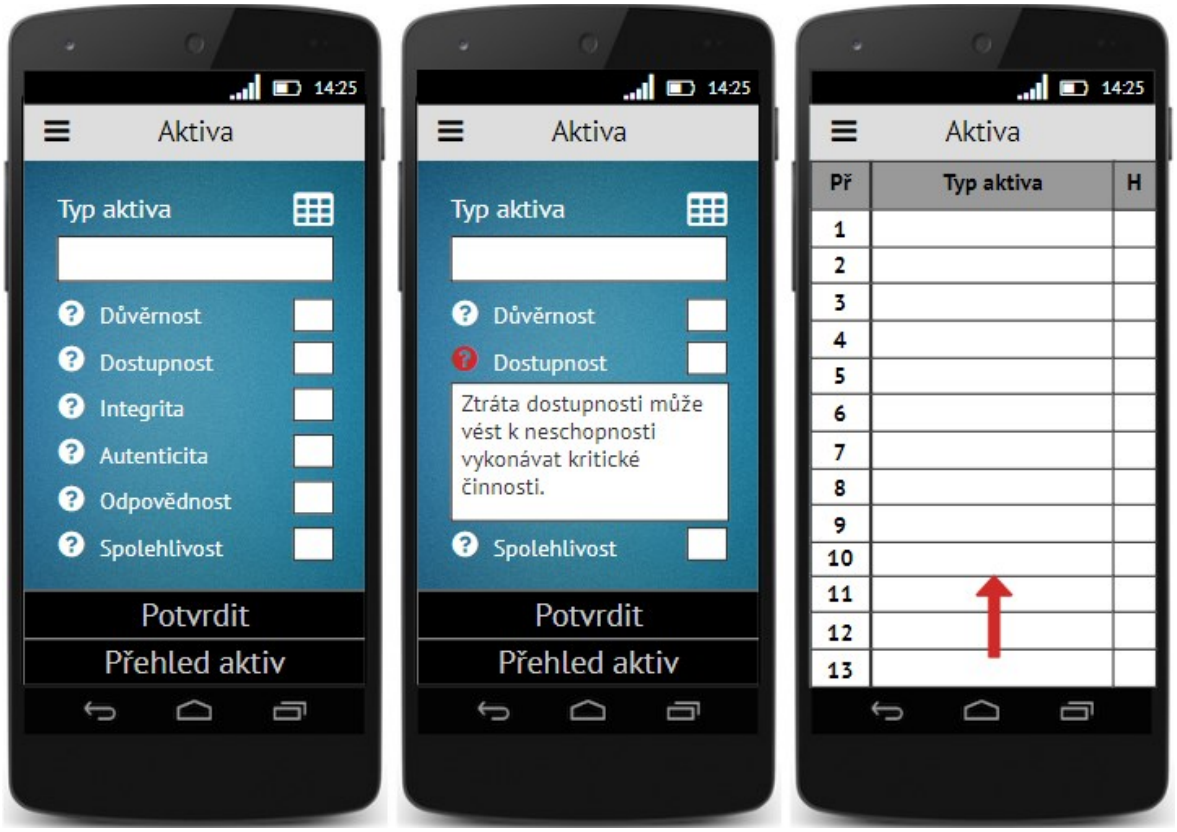
Po kliknutí na tlačítko „Nový“ na úvodní obrazovce spodního menu (viz obr. č. 17) se zobrazí fragment „Profil“ s dvěma editovatelnými položkami. Položka „Název“ slouží k pojmenování celého profilu (analýzy) a položka „Charakteristika“ ke stručnému popisu. Ve spodní části obrazovky se nachází pole „Uložit“, které po kliknutí uloží dokončený či rozpracovaný profil a navrátí uživatele na úvodní obrazovku (červeně zvýrazněno). Došlo k změně funkcí v horním panelu, přičemž tedy po kliknutí (červeně zvýrazněno) se otevře nabídka pěti možností, viz obr. č. 19. Schéma vytváření nového profilu je kvůli velikosti rozděleno do dvou částí viz obr. č. 21 a 22.



Obrázek 19: Obrazovka založení nového profilu [Vlastní]

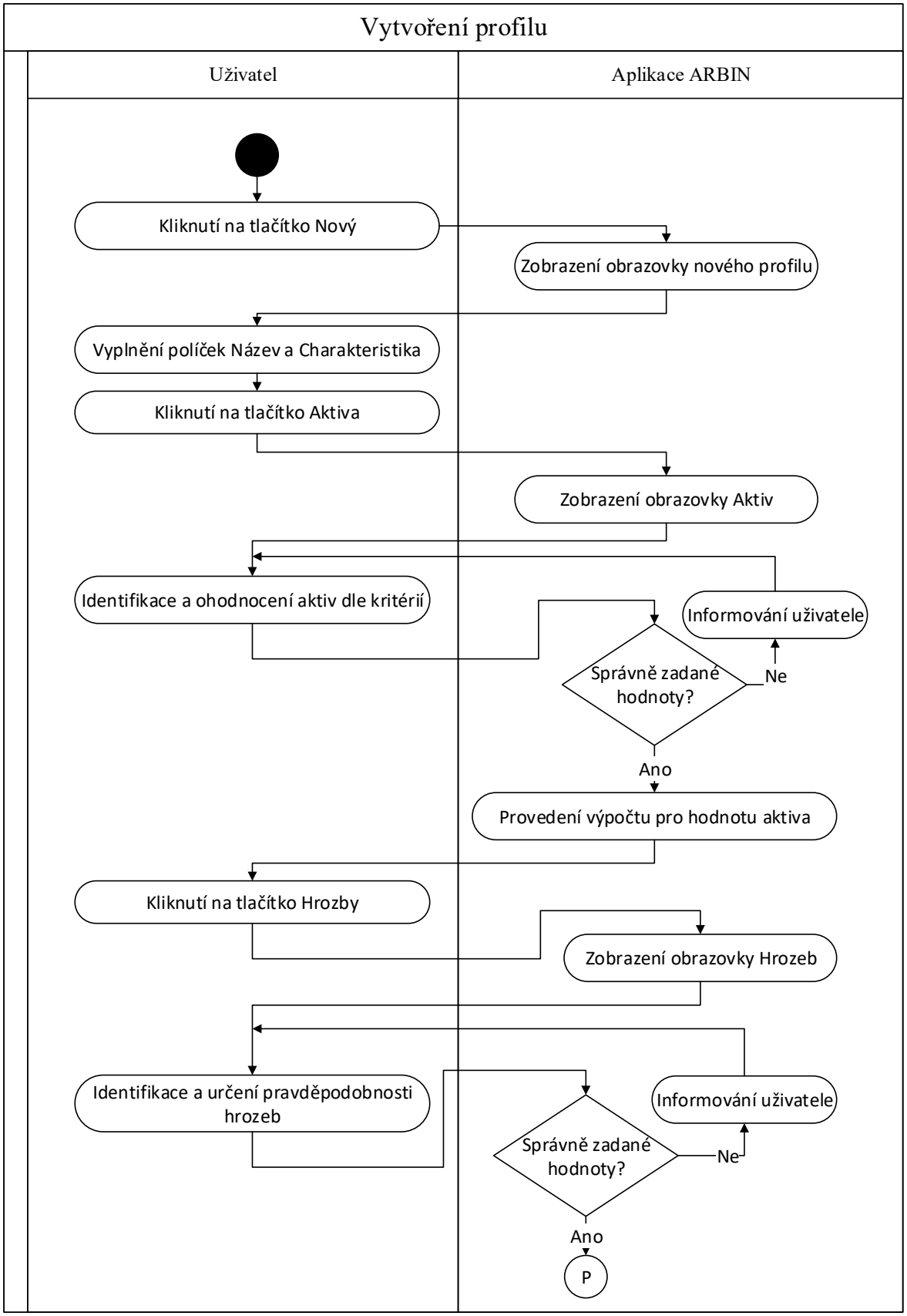
Na fragmentu „Aktiva“ se nachází celkem sedm editovatelných položek. Položka „Typ aktiva“ udává konkrétní aktivum, které se v následných krocích hodnotí. Dalších šest editovatelných položek jsou hodnotící kritéria aktiva (důvěrnost, dostupnost, integrita, autenticita, odpovědnost, spolehlivost), přičemž před každým názvem se nachází ikonka pro rychlou nápovědu. Další ikonkou, kterou je možné aktivovat je ikonka pro rychlé zobraze-

ní číselníků, která bude popsána dále. Po vyplnění těchto polí musí uživatel kliknout na možnost „Potvrdit“. Celá karta konkrétního aktiva se tímto uloží. Celkový přehled vytvořených aktiv lze zobrazit po kliknutí na položku „Přehled aktiv“, která se nachází ve spodní části obrazovky. Tento fragment tedy obsahuje tabulku rozdělenou na tři části, pořadí (Př), typ aktiva a hodnotu aktiva (H), která se automaticky vypočítá na základě ohodnocených kritérií dle rovnice uvedené v kapitole č. 5. Provedením gesta ve směru šipky lze přehled posouvat viz obr. č. 20.

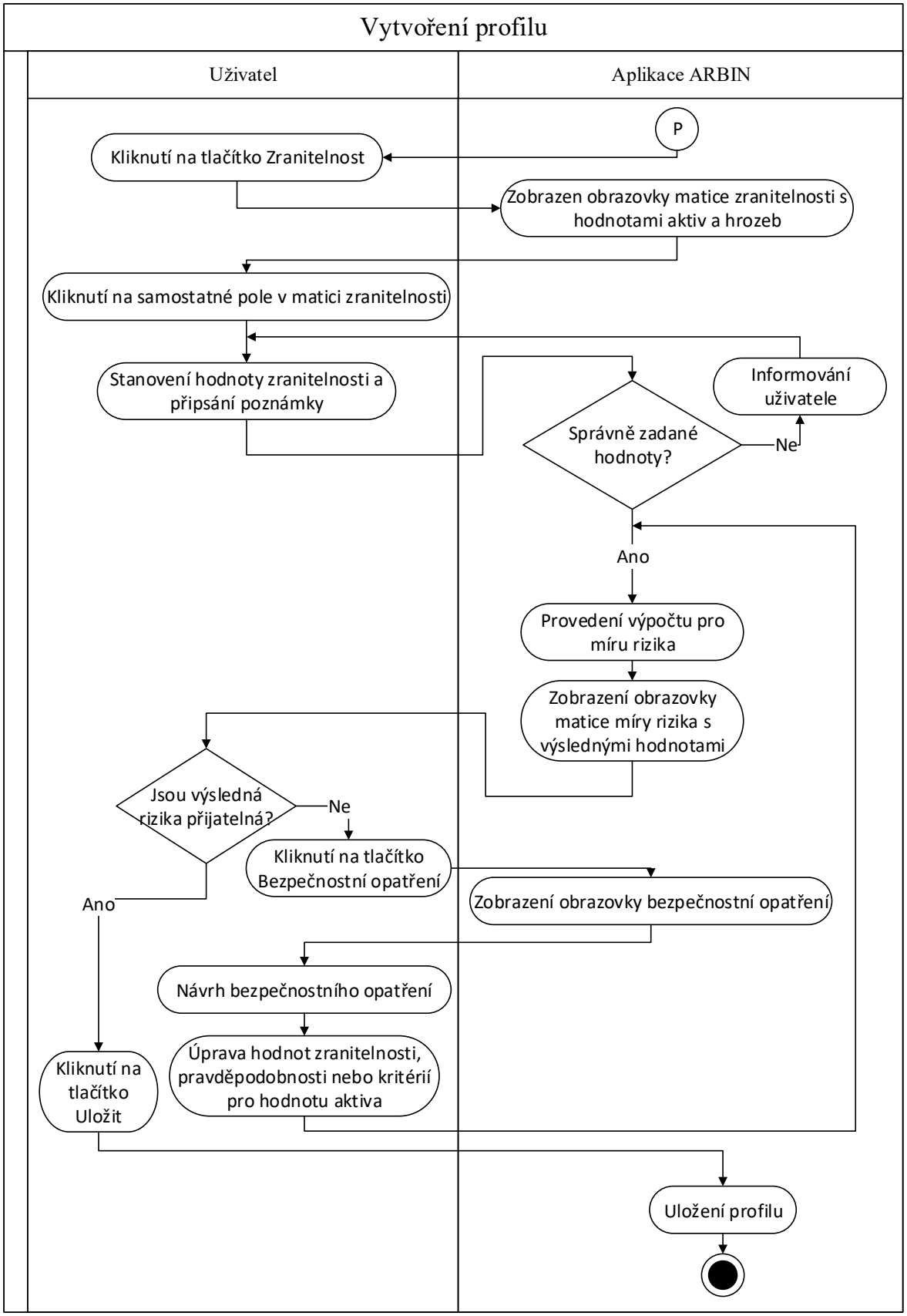


Obrázek 20: Obrazovka hodnocení aktiv [Vlastní]

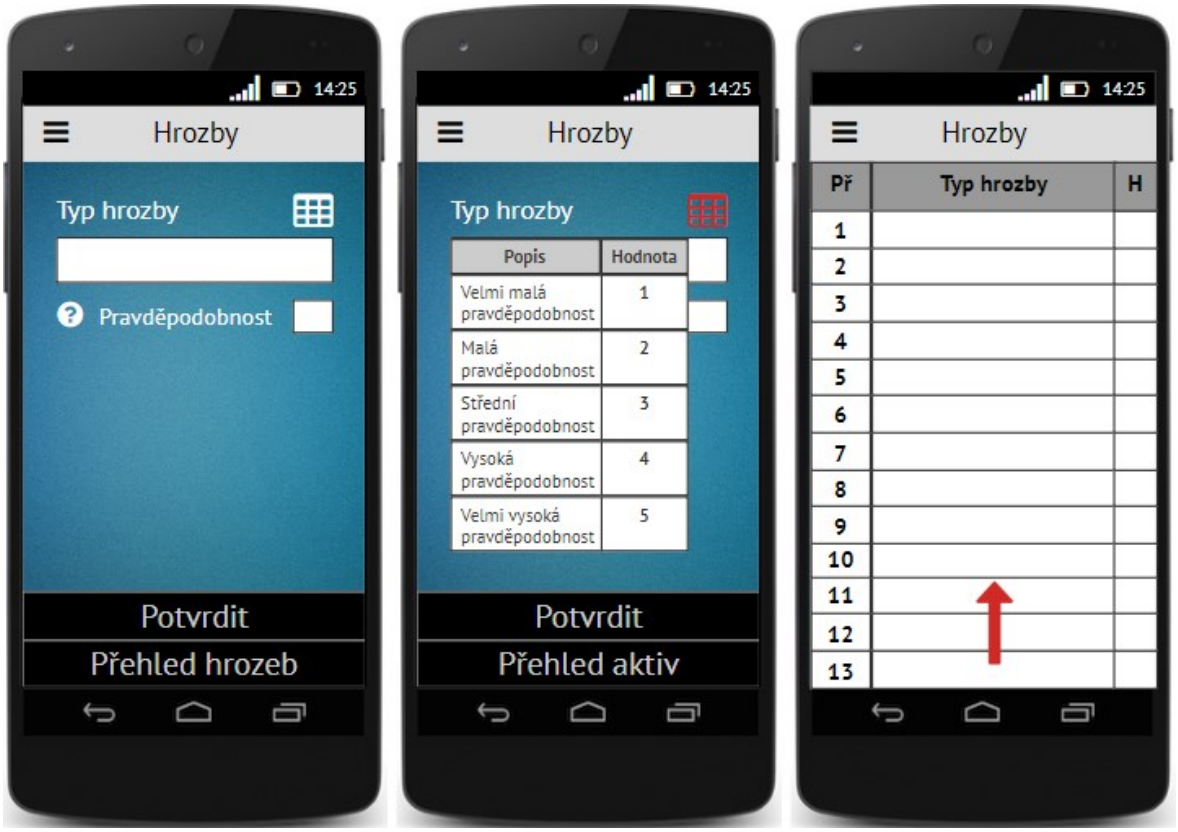
Dalším krokem po identifikování a ohodnocení aktiv je identifikace hrozeb a určení jejich pravděpodobnosti. Na fragmentu „Hrozby“ se nachází dvě editovatelné položky, tedy „Typ hrozby“ udává konkrétní hrozbu a druhou položkou je volné pole pro určení pravděpodobnosti hrozby. Fragment obsahuje rovněž dvě aktivující ikonky, jednou je rychlá nápověda a druhou je ikonka pro rychlé zobrazení číselníků (aktivace této ikonky je červeně vyznačena). Posloupnost činností a funkcí tohoto kroku je založená na stejném principu jako v případě kroku předchozího (identifikace a hodnocení aktiv). Graficky jsou tyto kroky znázorněny na obr. č. 23.



Obrázek 21: Schéma založení profilu I [Vlastní]

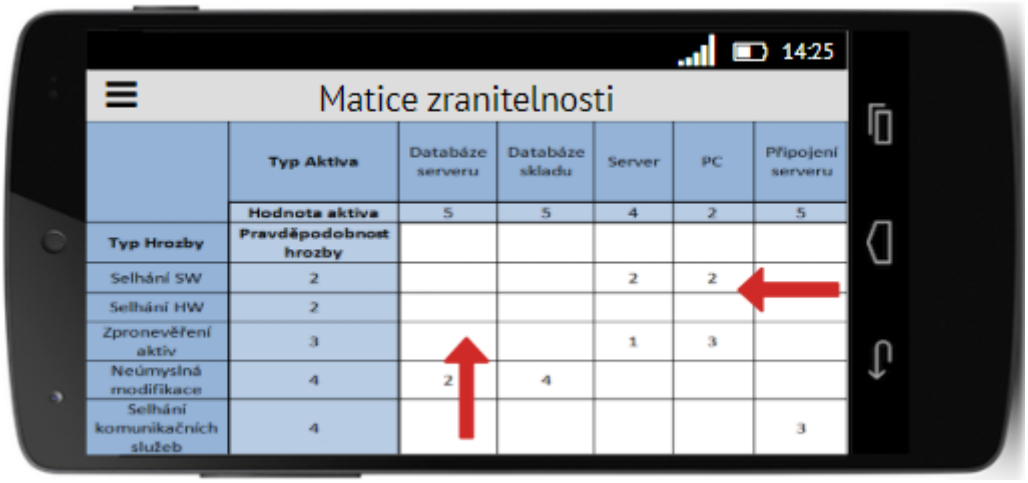


Obrázek 22: Schéma založení profilu II [Vlastní]



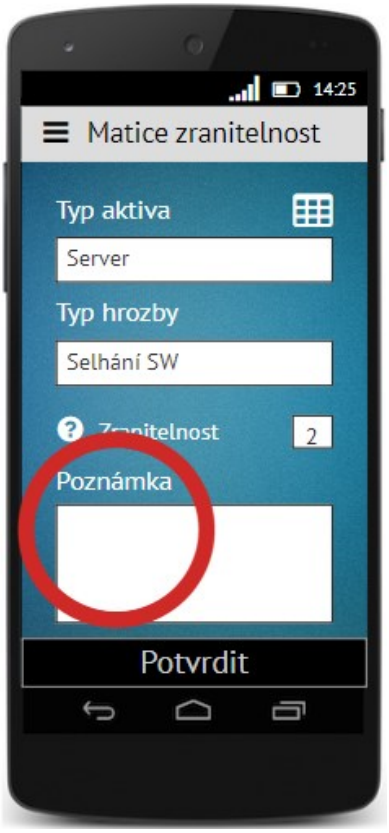
Obrázek 23: Obrazovka pro hodnocení hrozeb [Vlastní]

Na fragmentu „Matice zranitelnosti“ se automaticky vygeneruje matice na základě předešlých kroků. V jednotlivých polích matice pak uživatel hodnotí možnost využití zranitelnosti konkrétní hrozby vůči danému aktivu. V případě, že hrozba nemůže zneužít zranitelnosti, se pole nechává prázdné. Provedením gesta ve směru šipky lze matici posouvat viz obr. č. 24. Pro nastínění funkcionality byla matice doplněna o fiktivní údaje a stejně tak budou i další kroky.

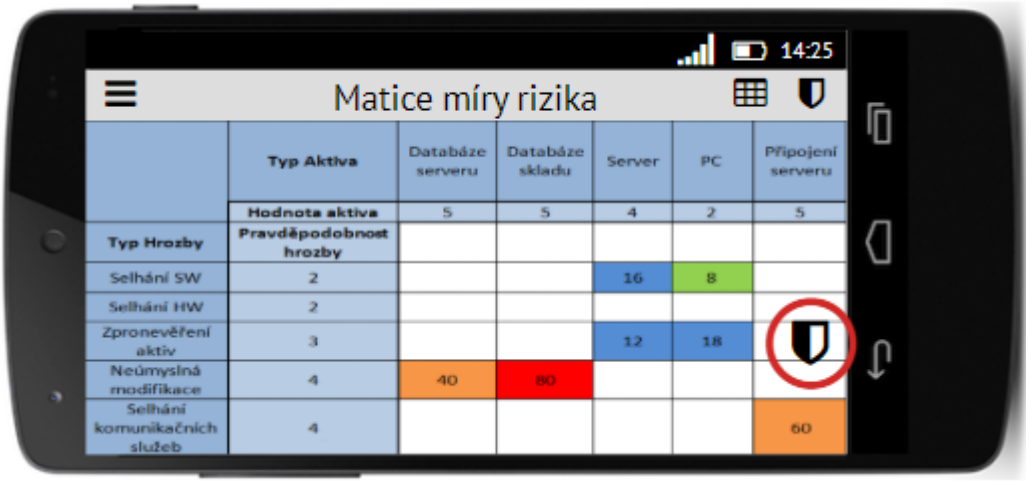


Obrázek 24: Obrazovka matice zranitelnosti [Vlastní]

Kliknutím na konkrétní pole v matici zranitelnosti se uživatel přesune na fragment „Zranitelnost“. Zde se nachází celkem čtyři pole, z toho dvě jsou editovatelné. Položky „Typ aktiva“ a „Typ hrozby“ jsou generovány dle předchozího kroku. Položka „Zranitelnost“ je doplňována uživatelem a stejně tak položka „Poznámka“ (červeně zvýrazněná), která slouží pro objasnění přiřazení konkrétní hodnoty zranitelnosti. Rovněž se na tomto fragmentu vyskytuje ikonka pro rychlé zobrazení číselníků. Po vyplnění údajů klikne uživatel na položku „Potvrdit“, čímž se dostane opět na obrazovku matice zranitelnosti (obr. č. 24) a může pokračovat vyplněním dalšího pole. Graficky je tento krok znázorněn na obr. č. 25.



Obrázek 25: Obrazovka hodnocení zranitelnosti [Vlastní]

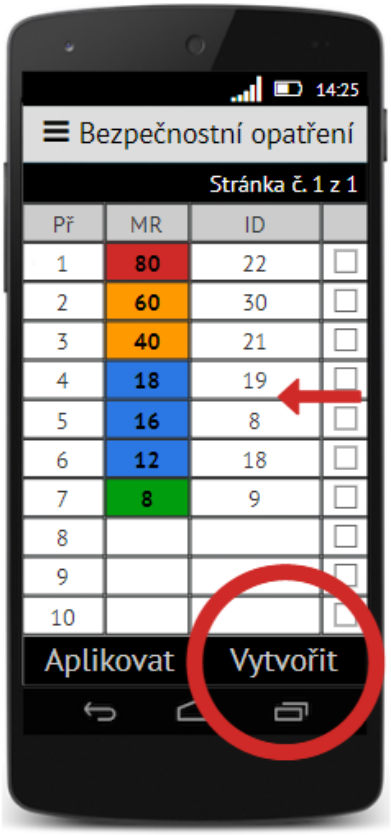


Obrázek 26: Obrazovka matice míry rizika [Vlastní]

Na obrazovce „Matice míry rizika“ jsou vidět výsledné hodnoty po provedení výpočtu uvedeného v kapitole č. 5 a dále jsou tyto výsledky barevně zvýrazněny dle velikosti nabytých hodnot. Uživateli je nabízena možnost, prostřednictvím ikonky štítu (červeně zvýrazněný), vytvoření bezpečnostních opatření. V horním panelu se nachází dvě ikonky, ikonka tabulky slouží pro rychlé zobrazení číselníků a ikonka štítu pro aktivaci vytvořených bezpečnostních opatření viz obr. č. 26. V případě že uživatel nemá zájem o vytvoření bezpečnostních opatření, může být tento krok rovněž posledním. V tomto případě se uživatel vrátí na fragment „Profil“ a dokončí celý proces kliknutím na tlačítko „Uložit“ (obr. č. 19).

7.4 Navrhnutí a přijmutí bezpečnostních opatření

Po kliknutí na ikonku štítu (červeně zvýrazněno na obr. č. 26) se zobrazí fragment přehledu bezpečnostních opatření. Tato tabulka je rozdělena celkem do čtyř sloupců, přičemž v prvním sloupci je uvedeno pořadí, ve druhém je barevně zvýrazněná hodnota míry rizika, ve třetím sloupci je ID (identifikační číslo) míry rizika, podle které se při následném kroku dohledají všechny potřebné údaje. Poslední sloupec slouží k vybrání konkrétního řádku. Mezi jednotlivými stránkami přehledu lze listovat provedením gesta ve směru šipky. Po tom co uživatel zatrhne konkrétní pole, stiskne tlačítko „Vytvořit“ (červeně zvýrazněno), které ho přesune do dalšího kroku. Druhou možností je tlačítko „Aplikovat“, které po vytvoření a označení konkrétních řádků přenese nové hodnoty do matice míry rizika. Graficky je tento krok znázorněn na obr. č. 27.

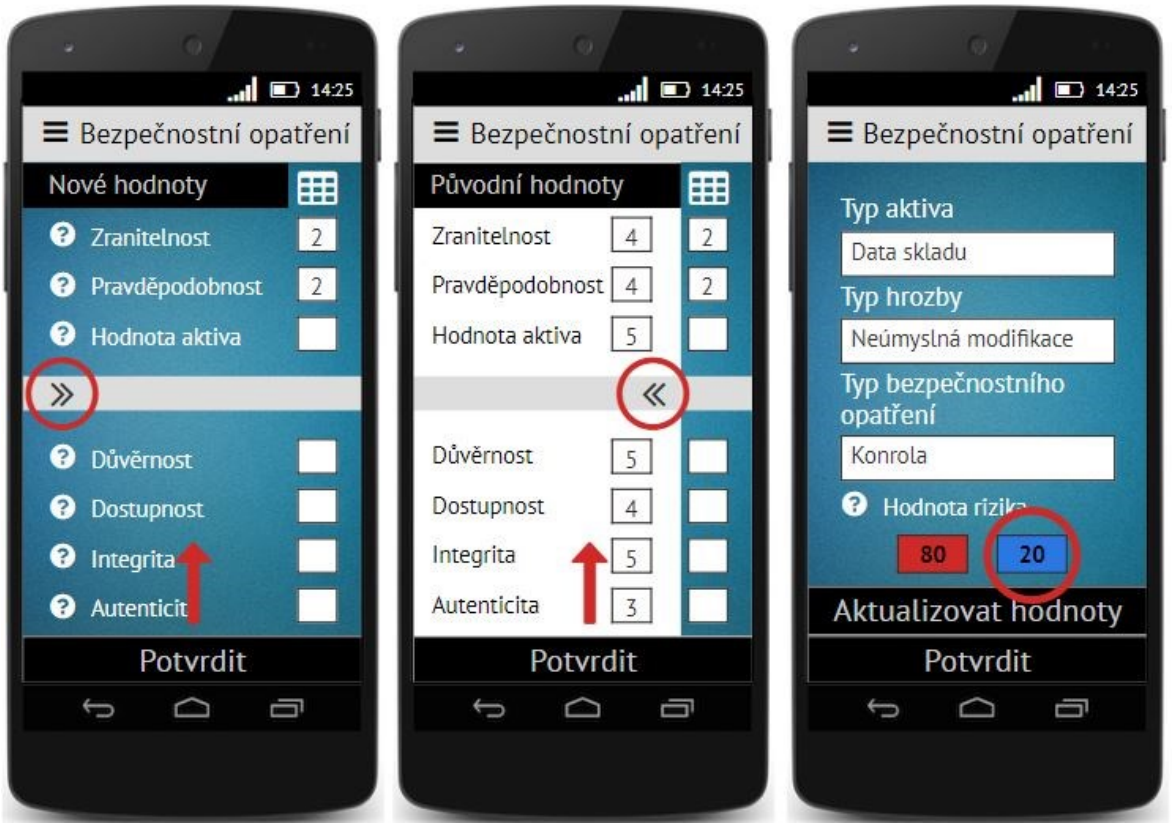


Obrázek 27: Obrazovka přehledu bezpečnostních opatření [Vlastní]

Po kliknutí na tlačítko „Vytvořit“ se uživatel dostane na fragment, kde vytváří vlastní návrh bezpečnostního opatření. Nachází se zde celkem pět polí, ale pouze jedno z nich je editovatelné. Do pole „Typ aktiva“, „Typ hrozby“ a dvou polí pro hodnotu rizika jsou hodnoty generovány automaticky na základě předchozích kroků. Uživatel tedy vyplní pouze položku „Typ bezpečnostního opatření“. Další dvě pole slouží pro zobrazení aktuální míry rizika (pole vlevo, červeně podbarvené) a druhé pole slouží pro zobrazení míry rizika po úpravě hodnot, které mají odrážet účinnost daného navrhovaného opatření. Tyto pole se pro větší přehlednost podbarvují na základě stanovené hodnoty míry rizika). Rovněž jsou obě hodnoty automaticky generovány, tudíž je uživatel nevyplňuje. Pro zadání výše zmíněných hodnot musí uživatel kliknout na tlačítko „Nové hodnoty“ (červeně zvýrazněno) viz obr. č. 28.

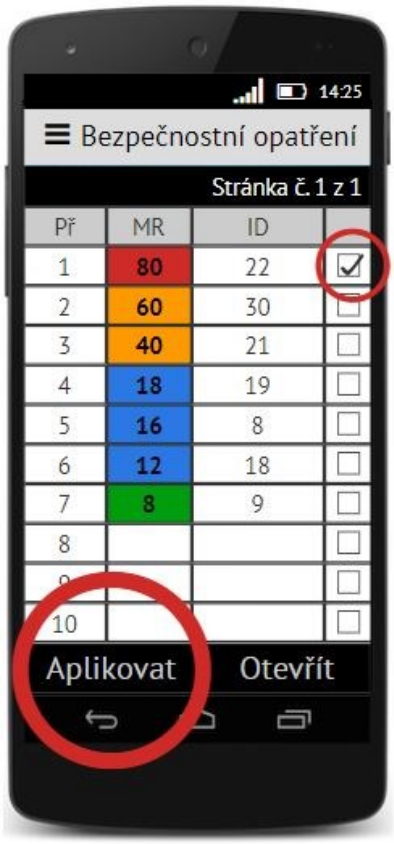
Obrázek 28: Obrazovka návrhu bezpečnostního opatření [Vlastní]

Po kliknutí na tlačítko „Nové hodnoty“ (viz obr. č. 28) se uživateli zobrazí fragment, kde má možnost upravit původní hodnoty zadané v předchozích krocích. Nachází se zde všechny hodnotící parametry. Všechny položky jsou editovatelné až na položku „Hodnota aktiva“, kterou lze upravit pouze prostřednictvím změny hodnotících kritérií, jenž se nachází ve spodní polovině obrazovky. Gestem ve směru šipky lze obrazovku posunovat. Při potažení levého okraje směrem do středu obrazovky se zobrazí postranní panel s původními hodnotami. Tyto položky jsou needitovatelné a slouží pouze pro informování uživatele. Potažením ve směru šipky lze tento postranní panel zavřít. Stejně jako v předchozích krocích může uživatel využít možnost rychlé nápovědy či rychlého zobrazení číselníků kliknutím na příslušnou ikonku. Po úpravě daných hodnot uživatel klikne na tlačítko „Potvrdit“, čímž dojde k přepočtu nové míry rizika. Uživatel se vrátí na předchozí obrazovku a zde je již přepočítaná hodnota míry rizika (modře podbarvená a zvýrazněná červeným kruhem). Graficky je tento krok zobrazen na obr. č. 29.



Obrázek 29: Obrazovka zadání nových hodnot [Vlastní]

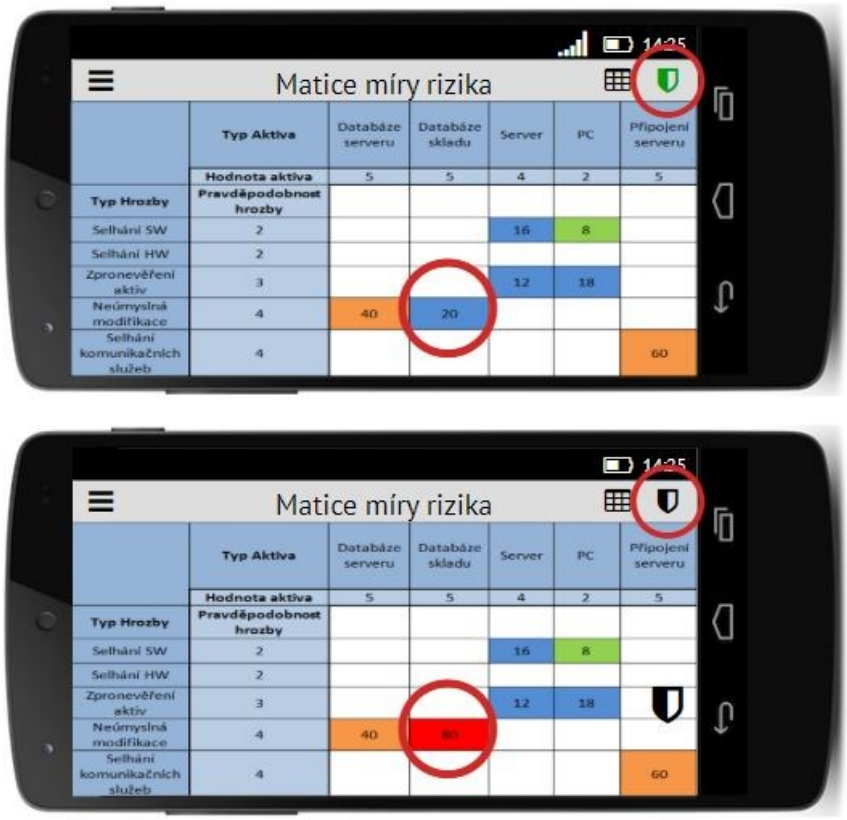
Kliknutím na tlačítko „Potvrdit“ se uživatel dostane zpět na obrazovku přehledu bezpečnostních opatření. Aby vytvořené opatření mohl aplikovat na matici míry rizika, musí vybrat a označit konkrétní pole v tabulce a následně klikne na tlačítko „Aplikovat“ (oba kroky jsou červeně znázorněné) viz obr. č. 30.



Obrázek 30: Obrazovka výběru bezpečnostních opatření [Vlastní]

V posledním kroku se vybrané bezpečnostní opatření dle obr. č. 28 aplikují na matici rizik. Aplikování probíhá automaticky a při zobrazení matice rizik jsou již hodnoty přepočítané. Že jsou opatření aktivní, uživatel zjistí, podle zeleně zbarveného štítu v pravém kraji hlavního panelu. Funkci je možné rovněž deaktivovat kliknutím na tuto ikonku, bezpečnostní opatření přestanou být účinná a do matice rizik se vrátí původní hodnoty. Graficky je tento krok znázorněn na obr. č. 31.

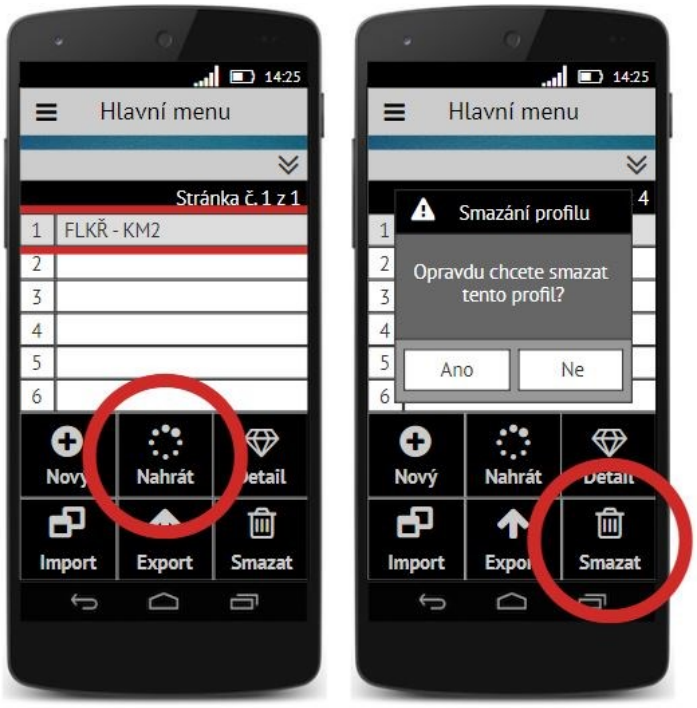
Tímto krokem je vytvoření profilu dokončené. Uživatel nyní otevře hlavní panel, vrátí se na obrazovku „Profil“ a stiskne tlačítko „Uložit“.



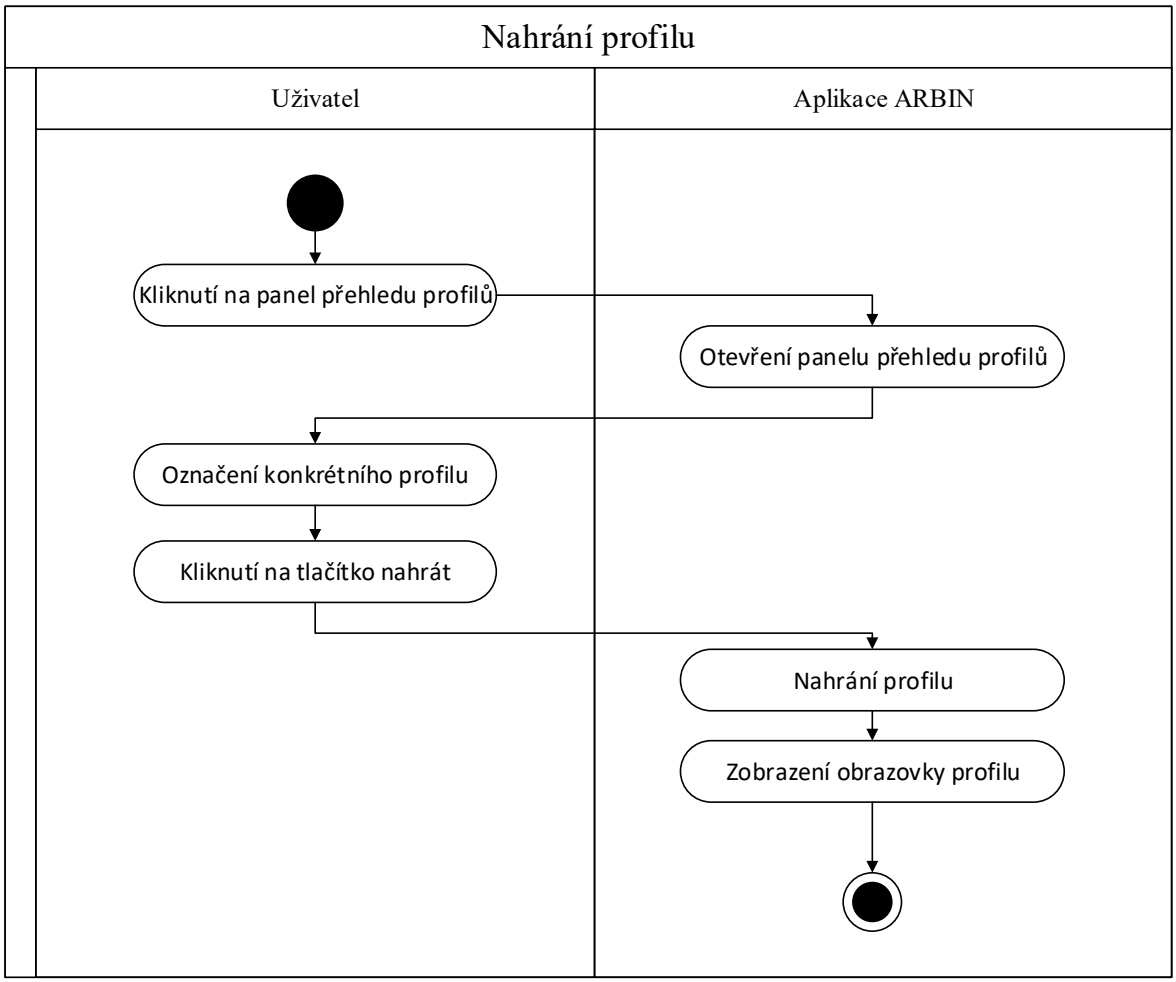
Obrázek 31: Obrazovka aplikování bezpečnostních opatření na matici rizik [Vlastní]

7.5 Nahrání profilu

V případě, že uživatel musel tvorbu profilu přerušit, potřebuje aktualizovat analýzu nebo z jakéhokoliv jiného důvodu potřebuje upravit profil, je možné využít na hlavní obrazovce ve spodním menu aktivitu „Nahrát“. Jako první krok musí uživatel otevřít panel přehledu profilů a následně označit daný profil, který se podbarví šedou barvou (červeně zvýrazněno). Kliknutím na tlačítko „Nahrát“ přejde uživatel na fragment „Profil“ a může pokračovat v tvorbě analýzy dle kapitoly č. 7.3. Graficky je tento krok znázorněn na obr. č. 32. Schéma nahrání profilu lze vidět na obr. č. 33.



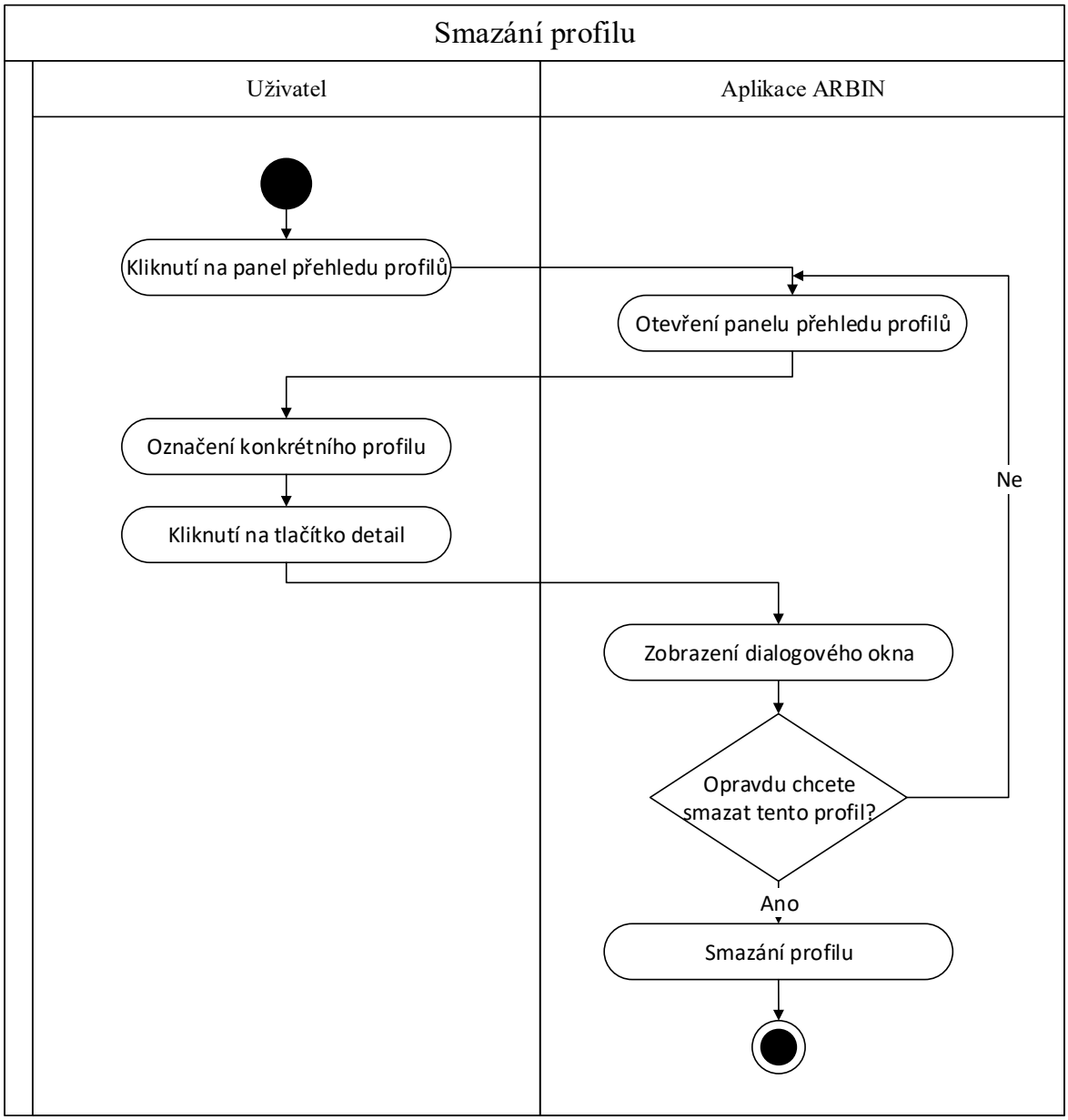
Obrázek 32: Obrazovka nahrání a smazání profilu [Vlastní]



Obrázek 33: Schéma nahrání profilu [Vlastní]

7.6 Smazání profilu

Dle stejného funkčního principu se postupuje i v případě, že uživatel chce daný profil nadobro smazat. Využije k tomu aktivitu spodního menu „Smazat“. Po stisknutí tohoto tlačítka se uživateli zobrazí dialogové okno, které od uživatele vyžaduje odezvu. Předmětem tohoto okna je ověření záměru smazat daný profil. Po stisknutí tlačítka „Ano“ dochází k úplnému smazání profilu. Tento krok je graficky znázorněny na obr. č. 32. Schéma nahrání smazání lze vidět na obr. č. 34.

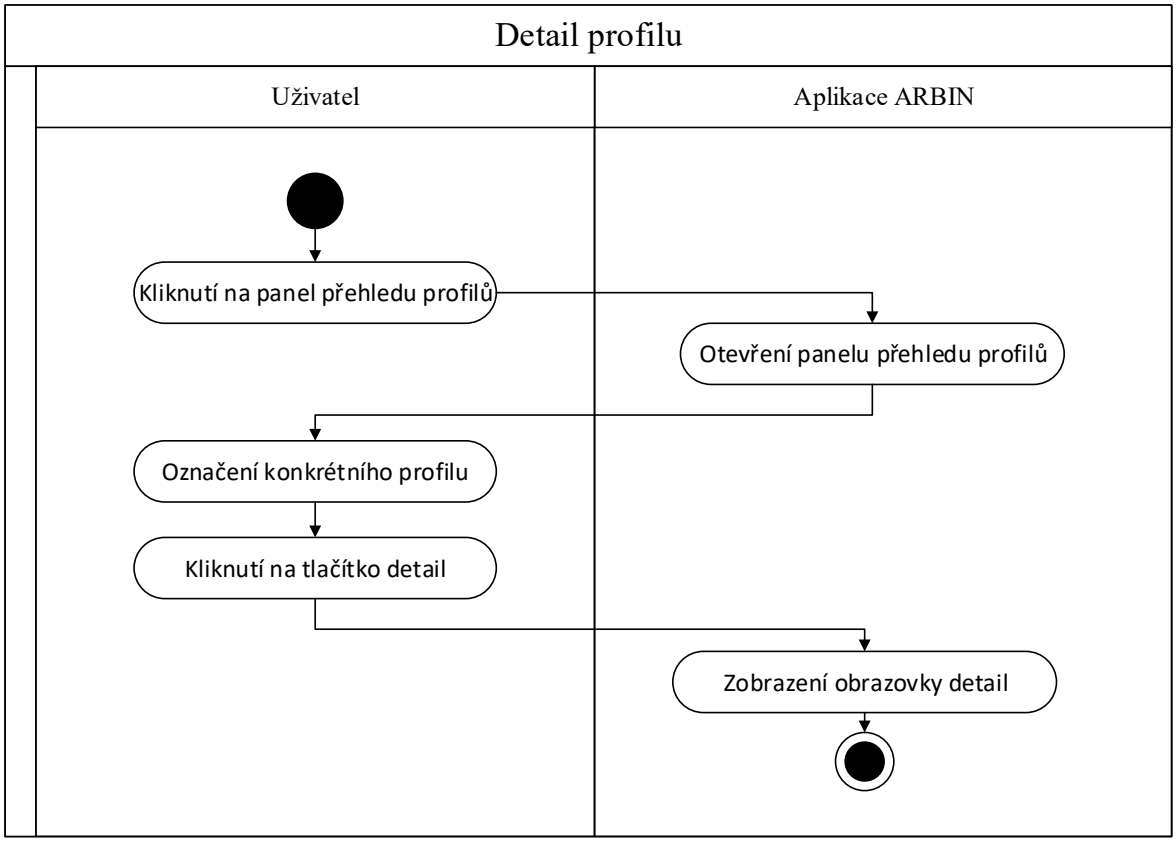


Obrázek 34: Schéma smazání profilu [Vlastní]

7.7 Detail

Při vybrání konkrétního profilu a stisknutí tlačítka „Detail“ nacházejícího ve spodním menu se uživateli zobrazí fragment se čtyřmi needitovatelnými položkami, které obsahují základní informace o profilu. Tato možnost hlavně navazuje na funkci „Import“, kdy uživatel může rychle nahlédnout na importovaný profil. Jedná se o položky „Název“, „Zpracovatel“, „Datum zpracování“ a „Charakteristika“ viz obr č. 35. Schéma otevření detailu profilu lze vidět na obr. č. 36.

Obrázek 35 Obrazovka detail [Vlastní]



Obrázek 36 Schéma zobrazení detailu profilu [Vlastní]

ZÁVĚR

V diplomové práci jsem se zabýval problematikou návrhu datového modelu mobilní aplikace pro analýzu rizik v oblasti bezpečnosti informací. Práce je členěna do dvou částí a to na teoretickou a praktickou část.

Teoretická část je členěna do čtyř kapitol. První kapitola je zaměřena na datové modelování a využívání principu tří architektur. Dále jsou zde popsány jednotlivé fáze vývoje datového modelu, tedy úroveň konceptuální, logická a fyzická. Ve druhé kapitole je obecně shrnuta problematika bezpečnosti informací. Obsahuje výčet pojmů, důležitých pro pochopení celkového kontextu, úvod do informační bezpečnosti a jeho systému řízení. Rovněž jsou v této kapitole vyjmenovány a charakterizovány nejpoužívanější metodiky. Třetí kapitola se věnuje problematice analýzy rizik bezpečnosti informačního systému a způsobu jejího provedení. V poslední kapitole teoretické části práce se nachází použité metody a cíle práce.

Praktická část práce je složena ze tří kapitol. V pořadí pátá kapitola charakterizuje aplikaci jako takovou. Předmětem šesté kapitoly je návrh konceptuálního datového modelu, včetně popisu jeho datových konstruktů. Sedmá kapitola obsahuje návrh uživatelského rozhraní, jehož součástí jsou i schémata funkčnosti jednotlivých kroků. Mezi tyto kroky patří přihlášení do aplikace, dále podkapitola věnovaná funkcionalitě úvodní obrazovky, vytváření nového profilu, návrh bezpečnostních opatření a jejich následné aplikování, nahrávání již vytvořeného profilu, smazání profilu a v poslední řadě náhledová funkce detail.

Lze konstatovat, že cíl práce byl splněn. V průběhu zpracování diplomové práce byly identifikovány možné dodatečné funkcionality, které by zvýšily využitelnost aplikace v praxi.

Základní kostru aplikace, která je v práci navrhnuta, lze v budoucnu doplnit o další nadstandartní funkce, jako je například v případě několikanásobného nesprávného zadání přihlašovacích údajů neumožnění vstupu na určitou časovou dobu, či zablokování účtu. Dále lze do procesu hodnocení aktiv zahrnout možnost, díky které si uživatel může sám vybrat hodnotící kritéria dle svých preferencí a logiky věci. Součástí implementace této funkce by muselo být rovněž upravení výpočtového aparátu. Funkcionalita aplikace počítá s procesy import a export, které by v budoucnu mohly být rovněž předmětem případného rozšíření. Cílem práce byl návrh datového modelu mobilní aplikace, tudíž byla vynechána fyzická (implementační) úroveň datového modelování.

SEZNAM POUŽITÉ LITERATURY

[1] SKŘIVAN, Jaromín. Datové modely a návrhy relačních schémat [online]. Praha, 2008 [cit. 2019-02-08]. Dostupné z: https://sites.ff.cuni.cz/uisk/wp-content/uploads/sites/62/2016/01/Datov%C3%A9-modely-a-n%C3%A1vrhy-rela%C4%8Dn%C3%ADch-sch%C3%A9mat_Sk%C5%99ivan.pdf.

[2] ŘEPA, Václav. VÝVOJOVÉ TRENDY METODIK VÝVOJE INFORMAČNÍCH SYSTÉMŮ - VÝZVA BPR. Dostupné z: http://nb.vse.cz/~repa/veda/EurOpen99%20Paper.pdf.

[3] SOMMERVILLE, Ian a Ludmila KALUŽOVÁ. Softwarové inženýrství. Brno: Computer Press, 2013. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-251-3826-7.

[4] KALUŽA, Jindřich a Ludmila KALUŽOVÁ. Modelování dat v informačních systémech. Praha: Ekopress, 2012. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-86929-81-1.

[5] BRUCKNER, Tomáš. Tvorba informačních systémů: principy, metodiky, architektury. Praha: Grada, 2012. Management v informační společnosti. ISBN 978-80-247-4153-6.

[6] E-R Diagram [online]. [cit. 2019-02-10]. Dostupné z: http://kubenka.org/PEF/1_rocnik/Internetove_technologie/tema_1_opory_a_soubory/cviceni_1_5_ER_diagram.pdf.

[7] Datové modelování - vztahy [online]. [cit. 2019-02-10]. Dostupné z: http://informacni-technologie.studentske.cz/2009/02/kardinalita-vztahu.html.

[8] Úvod do datového modelování [online]. [cit. 2019-02-10]. Dostupné z: https://www.interval.cz/clanky/webml-datove-modelovani/.

[9] Relační modelování [online]. [cit. 2019-02-15]. Dostupné z: (http://michaelkuty.github.io/ssz-ai-hk-3/prog/3.html).

[10] Objektové modelování [online]. [cit. 2019-02-15]. Dostupné z: https://www.fi.muni.cz/~smid/mis-objekt.htm.

[11] Fyzický datový model [online]. [cit. 2019-02-16]. Dostupné z: http://www.vrstevnice.com/akce/grandaction/vskola/7statnice/otazky/otazkaSTM17_vycuc.pdf.

[12] JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín, 2013. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-7454-312-8.

[13] Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu. [online]. 2016, [cit. 2019-02-18]. Dostupné z: www.mvcr.cz/soubor/terminologicky-slovnik-mv-verze-ke-stazeni.aspx.

[14] DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[15] POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

[16] DRASTICH, Martin. Systém managementu bezpečnosti informací. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-4251-9.

[17] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

[18] Information security [online]. [cit. 2019-02-25]. Dostupné z: https://www.cherwell.com/library/blog/what-is-an-information-management-security-system/.

[19] COBIT [online]. [cit. 2019-02-26]. Dostupné z: https://www.researchgate.net/figure/The-COBIT-cube_fig5_224162993.

[22] CRAMM [online]. [cit. 2019-02-26]. Dostupné z: https://www.researchgate.net/figure/The-COBIT-cube_fig5_224162993.

[23] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-19-4.

[24] CIMBÁLNÍKOVÁ, L; BILÍKOVÁ J; TARABA, P. Databáze manažerských metod a technik: co je důležitější v současné společnosti znalostí: rozvoj lidských zdrojů, nebo jejich řízení. ISBN 978-80-7329- 380-2.

[25] Princip tří architektur [online]. [cit. 2019-02-26]. Dostupné z: https://cs.wikipedia.org/wiki/Datov%C3%A9_modelov%C3%A1n%C3%AD#/media/File:P3A.jpg.

[26] WRÓBLEWSKI, Piotr. Algoritmy. Brno: Computer Press, 2015. ISBN 978-80-251-4126-7.

[27] ANDRESS, Jason. The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Second edition. Boston: Elsevier/Syngress, Syngress is a imprint of Elsevier, [2014]. ISBN 978-0-12-800744-0.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

COBIT	Control Objectives for Information and related Technology.
CRAMM	Risk Analysis and Management Method.
HW	Hardware.
ICT	Informační a komunikační technologie.
IS	Informační systém.
ISMS	Information Security Management System.
IT	Informační technologie
ITIL	Information Technology Infrastructure Library.
SW	Software.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK