VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

VYTVOŘENÍ HELP DESKU SW NÁSTROJE PRO ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI

CREATING A HELP DESK SW TOOL FOR CYBER SECURITY MANAGEMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Veronika Brzobohatá

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Petr Sedlák

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Veronika Brzobohatá**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2020/21

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Vytvoření help desku SW nástroje pro řízení kybernetické bezpečnosti

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem mé diplomové práce je vytvoření help desku SW nástroje pro řízení kybernetické bezpečnosti, který by měl být pro uživatele snadný k používání, intuitivní a jednoduchý.

Základní literární prameny:

BRUTON N. How to manage the IT Helpdesk. Great Britain: The Bruton Consultancy, 2002. ISBN 0750649011.

CZEGEL B. Running Effective Help Desk, 2nd Ed. New York: Wiley, 1998. ISBN 978-0471248163.

HALSEY M. The IT Support Handbook. Sheffield: Apress Media LLC, Welmoed Spahr, 2019. ISBN 978-1-4842-5132-1.

JORDÁN V. a V. ONDRÁK. Infrastruktura komunikačních systémů II: Kritické aplikace. Brno: Akademické nakladatelství CERM, 2015. ISBN 978-80-214-5240-4.

SMEJKAL V. a K. RAIS. Řízení rizik ve firmách a jiných organizacích. 4. vyd. Praha: Grada, 2013. ISBN 978-80-247-4644-9.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

Mgr. Veronika Novotná, Ph.D. ředitel	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Diplomová práce je zaměřena na tvorbu návrhu helpdesku pro software ESKO. Tento ESKO software vyvinula firma ISIT Slovakia s.r.o. Helpdesk bude znázorněn pomocí několika softwarů. Některé se používají pro tvorbu diagramů a znázornění workflow, další pak pro grafické úpravy. Helpdesk bude vytvořen na základě aktuálních potřeb firmy a následně jí bude dodán jako výsledný produkt.
Hlavním cílem je rozšířit funkcionalitu webu a doplnění tohoto webu o navrhnutý helpdesk. Bonusem bude knihovna dotazů, která bude fungovat na principu SQL databáze.

Klíčová slova

helpdesk, Lucidchart, JIRA, Canva, kybernetická bezpečnost, GDPR, kybernetický zákon, SQL databáze

Abstract

The diploma thesis is focused on the creation of a helpdesk design for ESKO software. This ESKO software was developed by ISIT Slovakia s.r.o. The helpdesk will be represented by several software. Some are used to create diagrams and represent workflows, others for graphic editing. The helpdesk will be created based on the current needs of the company and then delivered to it as the final product. The main goal is to extend the functionality of an existing website and add to this website and the proposed helpdesk. The bonus will be a query library, which should work on the principle of an SQL database.

Key words

helpdesk, Lucidchart, JIRA, Canva, cyber security, GDPR, cyber law, SQL database

Bibliografická citace

BRZOBOHATÁ, Veronika. *Vytvoření helpdesku SW nástroje pro řízení kybernetické bezpečnosti* [online]. Brno, 2021 [cit. 2021-05-12]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/133634. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 12. května 2021

……

Bc. Veronika Brzobohatá

Poděkování

Chtěla bych poděkovat především panu Ing. Petru Sedlákovi za pomoc při psaní práce, ochotu a odborné rady. Dále poděkování patří mé rodině a přátelům, kteří mě při psaní práce podporovali.

OBSAH

ÚVOD

V dnešní době existuje mnoho různých firem, které se specializují na vývoj softwarů, které nám lidem mají usnadnit práci. Tyto softwary však mohou být pro obyčejného laika složité a těžko se v nich vyzná. Takový člověk se rozhodne hledat pomoc u firmy, která daný software vyvíjí a většinou se obrací přímo na firemní podporu. Ta může mít několik podob a většina z nich se v dnešní době vyskytuje online na webovém rozhraní. Problémy s orientací na webu se netýkají jen starších lidí, naopak spousta lidí z mladší generace si není jistá, který program si můžou stáhnout a který nikoliv. Když už se takový program podaří stáhnout, může nastat orientační problém v samotném programu. Zároveň existuje spousta zákonů a vyhlášek, jak se vůbec na internetu chovat, jak se chovat v případě používání softwarů a podobně. Další problém je, že tyto zákony a vyhlášky jsou poměrně často novelizovány a člověk snadno ztratí přehled.

Pro orientaci na webovém rozhraní, popřípadě i na orientaci v samotném programu jsou vytvořeny takzvané helpdesky. Tyto helpdesky jsou pomůckou pro uživatele. Pomáhají při zodpovídání dotazů a přímo znázorňují jednoduché kroky, kterých chceme v programu dosáhnout.

Proto jsem se rozhodla psát svoji diplomovou práci o tvorbě helpdesku pro software, který vyvíjí slovenská firma, jejíž jméno je ISIT Slovakia s.r.o. Tato firma se specializuje na vývoj softwaru ESKO. Mimo jiné se zmíním o firmách, které mají výhradní práva na prodej softwaru ESKO. Blíže popsána bude firma SEVITECH CZ s.r.o., která se specializuje na prodej tohoto softwaru v České republice.

Cílem mé diplomové práce je návrh jednoduchého helpdesku, který by pak firma mohla reálně využít na svých webových stránkách a v samotném programu. V práci se chci zaměřit na jednotlivé zákony zabezpečující jeho správné a bezpečné fungování. K tvorbě helpdesku použiji grafické nástroje ke znázornění, jak by helpdesk mohl vypadat. Dalším cílem je zjednodušit firmě práci a tím ji i zefektivnit. Konkrétně bude přínosem to, že zaměstnanci nebudou muset odpovídat na spoustu dotazů pomocí telefonní linky a nebudou tak zbytečně a dlouho vytěžování kvůli jednomu dotazu. Budou tak mít více času na další pracovní úkony. Představím jednoduchý návrh na zlepšení fungování helpdesku a rovněž představím i ticketovací systém, který zaměstnancům umožní lépe naplánovat svoji práci, bude také

efektivnější komunikace v týmu a vedení firmy bude mít lepší přehled, na čem aktuálně zaměstnanci pracují.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem mé diplomové práce je vytvoření helpdesku, který by měl být pro uživatele, snadný k používání. Měl by být intuitivní a jednoduchý. Současně budu řešit i design webových stránek, jelikož uživatelé jsou v dnešní době navyklí používat pěkný design.

Helpdesk jsem se rozhodla rozdělit na dvě části, na webovou část a pak na část, která bude reprezentovat Knihovnu dotazů. Tato knihovna bude dostupná na webu i v rámci programu samotného.

K vytvoření webového helpdesku použiji několik grafických softwarů, které mi pomůžou s grafickým návrhem. Na samotný designový návrh webových stránek a Knihovny dotazů použiji software Canva, který se používá k tvorbě designových návrhů. Pro znázornění funkčnosti helpdesku využiji software Lucidchart. Je to software, kterým znázorním workflow, která bude následně používána při řešení dotazů od zákazníků. Workflow bude znázorněna pomocí ERP diagramu, který software Lucidchart umožňuje vytvořit. Vše budu navrhovat způsobem, který bude splňovat platné zákony a vyhlášky o kybernetickém prostředí.

V první části práce se zaměřím na teorii, kde popíšu všechny potřebné postupy, které budu k práci potřebovat a které se budou mé práce týkat. Uvedu zde jednotlivé zákony a vyhlášky, které jsou potřebné pro chápání fungování softwarů a tím pádem i pro tvorbu. Tyto předpisy vydané specializovanými úřady uvedu v teoretické části s popisem.

Ve druhé části se pokusím všechny teoretické postupy aplikovat v praxi. V této části popíšu společnost ISIT Slovakia s.r.o. a následně i firmu SEVITECH CZ. Zaměřím se na analýzu současného stavu ve společnosti. Objasním v práci celý vytvořený program a hlavní moduly a jejich funkčnost. Kromě samotného programu popíšu i firemní webové stránky. Nejdůležitější z celé kapitoly pak bude zaměření se na současnou formu poskytování podpory a pomoci zákazníkům ve formě helpdesku. Znázorním a vylíčím helpdesk v programu i helpdesk na webových stránkách firmy ISIT Slovakia s.r.o.

Ve třetí části se pak budu moct věnovat návrhům na zlepšení současného stavu helpdesku ve firmě. Vytvořím zcela nový návrh, který bude podložen teoretickými základy a grafickým zobrazením. Znázorním funkcionalitu nového helpdesku a kalkulaci nákladů spojených s tvorbou. K odhadnutí doby strávené na tvorbě nového helpdesku použiji časovou analýzu a síťový graf PERT. Využiji software Lucidchart pro tvorbu diagramů a workflow a dále

pak software Canva pro tvorbu grafického znázornění helpdesku. Nový návrh se bude opírat o aktuální požadavky uplatněné firmou ISIT Slovakia s.r.o.

1 TEORETICKÁ VÝCHODISKA PRÁCE

Teoretická část je rozdělena na dvě další části. První část je věnována obecné terminologii v rámci informační bezpečnosti. Druhá část popisuje instituce zodpovědné za informační bezpečnost, související zákony a vyhlášky a na závěr charakteristiku helpdesku.

1.1 Názvosloví

Na začátek je nejdůležitější vysvětlit pojmy, které se v diplomové práci budou často opakovat a je proto důležité se v nich orientovat.

Informační bezpečnost

Informační technologie zpracovávají velké množství informací s velkou hodnotou. Informační bezpečnost má za úkol ochraňovat všechny tyto informace, ať už ve fyzické nebo virtuální podobě, po celou dobu existence těchto informací. Když se informace neochraňují, může dojít k jejich ztrátě a zneužití. Ochrana informací se týká organizace (fyzická, personální, komunikační, ... bezpečnost) a je to ochrana před poškozením, zničením, ztrátou nebo zcizením dat z pohledu integrity (neoprávněné úpravy nebo zničení), dostupnosti (zajištění přístupu a ochrana před neoprávněným přístupem) a důvěrnosti (ochrana před neoprávněným čtením dat) (10).

Kybernetická bezpečnost

Kybernetická bezpečnost se narozdíl od informační bezpečnosti týká celého kybernetického prostoru. Je to souhrn právních, organizačních, technických a vzdělávacích prostředků zajišťujících ochranu kybernetického prostoru. Kybernetický prostor představuje digitální prostředí, kde vznikají informace, které se dále vyměňují a zpracovávají. Tyto informace jsou tvořeny informačními systémy, službami a elektronickou komunikací (12).

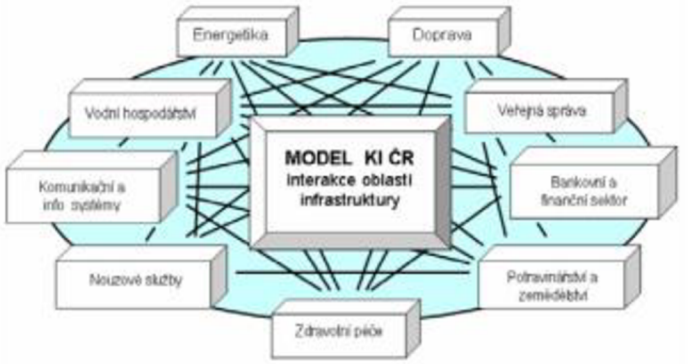
Důležitý pojem pro správné pochopení mé diplomové práce je i kybernetický (bezpečnostní incident). Tento pojem představuje narušení bezpečnosti informací v informačním systému, bezpečnosti služeb nebo integrity, v důsledku toho, že se stala nějaká kybernetická

bezpečnostní událost. Událost je tedy stav, kdy může dojít k narušení bezpečnosti informací a incident pak představuje narušení bezpečnosti informací (12).

Kritická infrastruktura a kritická informační infrastruktura

Kritická infrastruktura představuje vše, co denně používáme. Jedná se například o elektřinu, vodu, plyn a její dennodenní používání (11).

Kritická informační infrastruktura představuje infrastrukturu, jejíž případné narušení, by mělo vliv na bezpečnost státu (11).



Obrázek 1: Schéma interakcí oblastí kritické infrastruktury v ČR definovaných podle stavu v roce 2007
Zdroj: (27)

Významný informační systém

Tímto názvem se označuje systém, který je spravovaný orgánem veřejné moci, ale není součástí kritické infrastruktury. Narušení bezpečnosti informací souvisejících s tímto systémem může ohrozit či omezit výkon působnosti těchto orgánů (12).

Významná síť pak zajišťuje přímé spojení do veřejných komunikačních sítí nebo ke kritické informační infrastruktuře (12).

Rozdíl mezi CIO a CISO

CIO neboli Chief Information Officer, což je vlastně IT ředitel, který se stará o informační technologie v dané společnosti. Má být jakýmsi spojovacím mostem mezi počítačovými odborníky a vedením firmy (15).

CISO neboli Chief Information Security Officer, je to manažer informační bezpečnosti a je za ni zodpovědný. Jeho úkolem je tedy řízení informační bezpečnosti, její průběžné zlepšování, slaďování cílů bezpečnosti s cíli celé organizace (16).

1.2 NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost je hlavním správním orgánem pro kybernetickou bezpečnost. Orgán se zabývá i problematikou ochrany utajovaných informací v oblasti komunikačních a informačních systémů a rovněž kryptografickou ochranou (17).

Dále má tento úřad na starosti veřejně regulované služby, které se týkají družicového systému Galileo. Ten vznikl 1. srpna roku 2017 na základě zákona 205/2017 Sb., kterým se měnil předešlý zákon o kybernetické bezpečnosti a o změně souvisejících zákonů.

Ředitelem NÚKIB je od 20. března 2020 Karel Řehka. Ten se musí pravidelně účastnit jednání Bezpečnostní rady státu a je tak též členem Výboru pro kybernetickou bezpečnost. Tento výbor je pracovním orgánem Bezpečnostní rady státu pro koordinování plánování opatření k podpoření a zajištění bezpečnosti v České republice (17).

1.3 NCKB – Národní centrum kybernetické bezpečnosti

Výkonnou sekcí Národního úřadu pro kybernetickou a informační bezpečnost je Národní centrum kybernetické bezpečnosti (17).

NCKB zajišťuje zejména prevenci před kybernetickými hrozbami proti prvkům kritické infomační infrastruktury, významným informačním systémům, informačním systémům základní služby a některým vybraným informačním systémům veřejné správy. Dále se podílí na řešení kybernetických bezpečnostních incidentů u subjektů výše zmíněných poskytovatelů základních služeb, orgánů veřejné správy a u zvolených subjektů kritické infrastruktury (17).

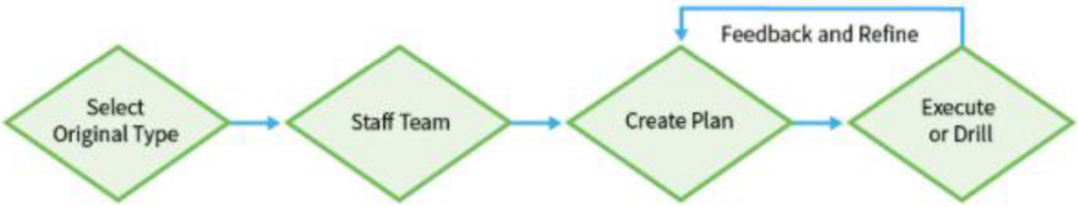
Rovněž nabízí vzdělávání v oblasti problematiky kybernetické bezpečnosti. Spolupracuje s národními i mezinárodními organizacemi za účelem poskytování a zajišťování bezpečnosti kybernetického prostoru. Podílí se i na vývoji a výzkumu v oblasti kybernetické bezpečnosti. Součástí práce NCKB je vyhodnocování rizik, která se mohou v oblasti kybernetické

bezpečnosti vyskytnout a podílí se na vytváření preventivních opatření a následně jejich přijímání (17).

Pod NCKB spadá i vládní CERT a týmy typu CSIRT, které hrají hlavní roli při ochraně kritické informační infrastruktury a významných informačních systémů dle zákona o kybernetické bezpečnosti (17).

CERT můžeme rozdělit na národní a vládní. Národní CERT je vlastně nevládní sdružení odborníků provozované soukromou osobou s určením pro vládní organizace. Cílem CERT sdružení je zajišťovat bezpečnostní opatření, detekovat možné kybernetické bezpečnostní události a hlásit bezpečnostní incidenty. Vládní CERT je pak součástí Národního bezpečnostního úřadu, ale je provozován NCKB. Je určen pro státní instituce. Vydává varování a doporučení před kybernetickými hrozbami a pomáhá vytvářet reaktivní i preventivní opatření (12).

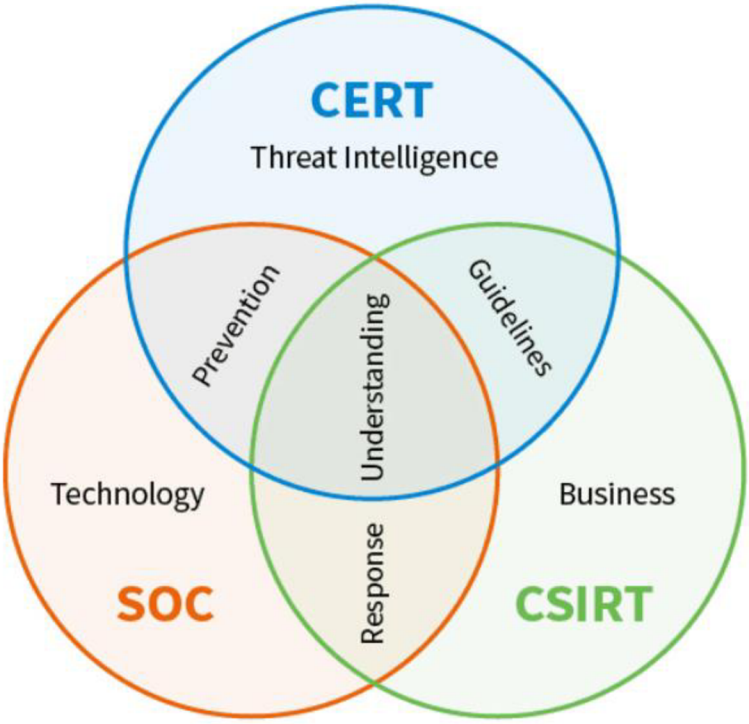
CSIRT neboli Cyber Security Incident Response Team má za úkol chránit kyberprostor a reagovat na incidenty. Má za úkol koordinovat činnosti během řešení incidentů a vytváří preventivní opatření, aby k incidentům nedocházelo. Na obrázku níže je vidět jednotlivé kroky, jak CSIRT tým pracuje (12).



Obrázek 2: Znázornění práce CSIRT týmu
Zdroj: (19)

Úkolem všech těchto týmů je být jakýmsi prvotním zdrojem, co se týká bezpečnosti informací a pomoci pro orgány státu, organizace i jednotlivé občany. Další důležitou rolí je i podílení se na zvyšování vzdělanosti v oblasti bezpečnosti na internetu. Orgány i osoby, které podléhají zákonu o kybernetické bezpečnosti, musí plnit určené povinnosti vůči CERT týmu (17).

Níže je zmíněno Security Operations Center neboli SOC, které zajišťuje komplexní centralizaci řízení bezpečnostních událostí a incidentů s jediným cílem, a to minimalizovat reakční doby na incident a škod, které z incidentu mohou plynout (18).



Obrázek 3: Znázornění činnosti CERT, CSIRT, SOC
Zdroj: (19)

1.4 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů – neboli zákon o kybernetické bezpečnosti vstoupil v platnost 29. 8. 2014 s účinností od 1. 1. 2015. Tento zákon upravuje práva a povinnosti osob v oblasti kybernetické bezpečnosti. Hlavními cíli zákona je stanovit základní úroveň bezpečnostních opatření, zlepšení detekce bezpečnostních incidentů a zavést jejich hlášení a upravit činnost dohledových pracovišť (1). V roce 2017 proběhly dvě novely tohoto zákona. Aktuální znění zákona je účinné od 1. 2. 2020 (1).

1.5 NIS

Směrnice NIS (z angl. Network and Information Security Incidents) neboli směrnice Evropského parlamentu a Rady z roku 2014. Je to směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Evropské unii. Cílem směrnice je harmonizovat právní úpravu států v EU v oblasti bezpečnosti sítí a informačních systémů.

Zavádí jednotný standard úrovně kybernetické bezpečnosti, aby tak mohlo dojít ke zlepšení funkce vnitřního trhu (1).

Do národní legislativy přináší nové typy povinných subjektů, jedná se o:

- Provozovatele základních služeb – PZS
- Provozovatele digitálních služeb – PDS

Provozovatele základní služby lze specifikovat jako soukromý nebo veřejný subjekt z nějakého odvětví, ve kterém poskytuje službu, která je důležitá z hlediska zachování kritických společenských nebo ekonomických činností. Poskytování této služby je závislé na informačních a komunikačních technologiích a možný kybernetický bezpečnostní incident by mohl způsobit narušení poskytování dané služby (17).

V roce 2018 nabyla účinnosti vyhláška, která určuje provozovatele základní služby podle daných kritérií. Tuto vyhlášku zpracoval Národní úřad pro kybernetickou a informační bezpečnost ve spolupráci s odbornou veřejností. Vyhláška je označena č.437/2017 Sb., o kritériích pro určení provozovatele základní služby. Tato vyhláška upravuje dopadová a odvětvová kritéria pro určení provozovatele základní služby. Vymezuje významnost dopadu narušení této základní služby na zabezpečení ekonomických či společenských činností podle § 22a odst. 1 zákona o kybernetické bezpečnosti (17).

Provozovatele digitální služby lze specifikovat jako infomační společnosti, které provozují:

- Online tržiště – umožňuje spotřebiteli nebo prodávajícímu uzavírat smlouvy prostřednictvím internetové stránky online tržiště
- Internetového vyhledávače – umožňuje vyhledávat na všech internetových stránkách na základě dotazu, klíčového slova, a podobně
- Clound computing – umožňuje přístup k úložišti či výpočetním zdrojům, které je možné dále sdílet (12).

1.6 Vyhláška o kybernetické bezpečnosti

Nová vyhláška o kybernetické bezpečnosti je zveřejněna pod označením *"Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech,*

reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)" ve Sbírce zákonů (17).

Vyhláška zpracovává Směrnici NIS a upravuje pro informační systémy kritické informační infrastruktury, významné informační systémy, komunikační systémy kritické infrastruktury, informační systémy základní služby anebo informační systémy nebo sítě elektronických komunikací následující opatření:

- Obsah a rozsah bezpečnostních opatření
- Obsah a strukturu bezpečností dokumentace
- Náležitosti, způsob hlášení kybernetického bezpečnostního incidentu
- Náležitosti oznámení o provedení reaktivního opatření a výsledku tohoto opatření
- Typy a kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů
- Vzor oznámení kontaktních údajů a formu onoho oznámení
- Způsob likvidace dat, jakožto i provozních údajů, informací a všech jeho kopií (17).

1.7 GDPR

GDPR představuje obecné nařízení o ochraně osobních údajů (z angl. General Data Protection Regulation). Je to nový právní rámec v Evropské unii proti neoprávněnému zacházení s daty občanů. Nařízení bylo přijato v roce 2016, ale je platné až od 28. 5. 2018 pro celou Evropské unii (2).

GDPR platí celosvětově pro jakýkoliv subjekt, který zpracovává osobní údaje občanů Evropské unie. Nařízení se tedy týká firem, institucí i jednotlivců, kteří jakkoliv zacházejí s osobními údaji (například zaměstnanců, zákazníků, klientů, dodavatelů, a tak podobně). Osobní údaj se dá definovat jako jakákoliv informace o člověku obecně – tedy jméno, adresa, datum narození, a tak dále (2).

Byly zavedeny pokuty za nedodržování těchto pravidel a byla zavedena nová kontrolní funkce DPO – Data Protection Officer, což je vlastně pověřenec pro ochranu osobních údajů. Úkolem DPO je sledování souladu zpracování osobních údajů s povinnostmi, které vyplývají z nařízení. Dále pak provádění auditů, školení pracovníků a řízení agendy ochrany dat (2).

Firma by měla shromažďovat pouze nezbytná data. Po zpracování by měla být data smazána. Za ochranu těchto dat je zodpovědný celý dodavatelský řetězec (2).

Jeden z největších dopadů zavedení GDPR je posílení práv občanů. Mezi tato práva se řadí například právo na přístup, opravu, výmaz, právo být zapomenut, právo na omezení zpracování, přenositelnost údajů a právo vznést námitku (2).

1.7.1 GDPR v praxi

Obrázek 4: GDPR analýza
Zdroj: (12)

Prvním bodem je provedení analýzy současného stavu. Tato analýza by měla obsahovat datový audit evidence osobních údajů, návrh a doporučení pro dosažení souladu s nařízením GDPR, plán realizace a implementace nápravných opatření, školení zaměstnanců v rámci odpovědnosti při nakládání s osobními údaji a zavedení směrnic a pravidel (12).

Dále by se mělo provést zabezpečení těchto dat. Jedná se o bezpečnostní audit, vytvoření havarijního plánu při porušení ochrany osobních údajů, pravidelné testování funkčnosti bezpečnostních opatření a v neposlední řadě hlášení incidentů dozorovým organům (12).

DPO neboli pověřenec pro ochranu osobních údajů, poskytne poradenství správcům, posoudí vliv na ochranu osobních údajů a podobně (12).

Celkové řízení procesu tedy určitě není jednorázová akce, ale jedná se o několik kroků, které vedou k úspěšnému a dlouhodobému plnění povinností vyplývajících z příslušných nařízení (datový audit, analýza rizik, plán implementace, školení zaměstnanců, a tak dále) (12).

1.8 Analýza rizik

Analýza rizik se dá popsat jako proces definování hrozeb, jejich pravděpodobnosti uskutečnění, dopadu na aktiva a v konečném důsledku stanovení rizik, a to, jak jim předcházet (3).

Analýza rizik zahrnuje tyto činnosti:

- Identifikace aktiv – vymezení aktiv, jejich popis a vlastníky aktiv
- Stanovení hodnoty aktiv – určení hodnoty jednotlivých aktiv
- Identifikace hrozeb a zranitelnosti – obecně akce, které mohou negativně ovlivnit aktiva
- Stanovení závažnosti hrozeb a míry zranitelnosti – pravděpodobnost výskytu hrozby a určení míry zranitelnosti (3)

Analýza rizik jako taková obsahuje velké množství pojmů, které budou vysvětleny níže.

Identifikace rizik

V této první části analýzy je důležité identifikovat rizika a následně vyhodnotit tato rizika. Tato část analýzy rizik se skládá ze tří částí:

- Posouzení dopadů naplnění hrozeb
- Stanovení úrovně rizik
- Rozhodnutí, zda jsou rizika akceptovatelná nebo neakceptovatelná (3).

Hodnocení rizik představuje zvažování nad poškozením aktiv, která mohou být způsobena tím, že se naplní hrozba a je nutné brát ohled na potencionální důsledky. Dále je pak důležité přemýšlet nad pravděpodobností výskytu rizik (3).

1.8.1 Aktivum

Aktivum představuje něco, co má pro subjekt nějakou hodnotu. Aktiva můžeme dělit na hmotná (peníze, majetek, …) a nehmotná (software, informace, …). Základní charakteristikou aktiv je hodnota aktiva (může se jednat o pořizovací cenu, důležitost pro vlastníka, a podobně) a jeho zranitelnost (3).

Z hlediska kybernetické bezpečnosti rozlišujeme dva typy aktiv, a to primární a podpůrná neboli sekundární. Jakási definice se dá najít v normě ČSN ISO/IEC 270005, příloha B, kde je uvedeno, že primární aktiva jsou informace, obchodní procesy a činnosti. Když jsou tyto prvky narušeny, tak organizace nemůže plnit svoje poslání. Podpůrná (sekundární) aktiva jsou hardware a software, sítě, organizace, pracovníci a podobně. Na těchto podpůrných aktivech jsou primární aktiva závislá (20).

1.8.2 Hrozba

Hrozba představuje sílu, událost, aktivitu nebo osobu, která má nechtěný vliv na aktiva a může na nich způsobit nějakou škodu. Škoda, která je způsobena na daném aktivu, se označuje jako dopad hrozby. Základní charakteristikou hrozby je její úroveň, která se hodnotí dle těchto faktorů: nebezpečnost, přístup a motivace. Nebezpečnost je schopnost hrozby způsobit škodu na aktivu. Přístupem rozumíme možnost hrozby působení na aktivum. Motivací je pak zájem o naplnění určité hrozby. Při aktuálním hodnocení hrozeb je důležité přihlížet k vnitřním zkušenostem z incidentů a dřívějším hodnocením hrozeb. Při tomto postupu se musí počítat s tím, že hrozby se můžou měnit, a to zejména v sociálně-ekonomických oblastech (3).

1.8.3 Zranitelnost

Zranitelnost se dá nazvat jako slabina analyzovaného aktiva, které může hrozba využít pro negativní ovlivnění daného aktiva. Zranitelnost, která nemá odpovídající hrozbu nemusí nutně znamenat to, že by se muselo přijímat nějaké opatření, ale měla by být určitě monitorována. Zranitelnost vzniká tam, kde se spojuje hrozba s aktivem. Naprosto základní charakteristika zranitelnosti je úroveň zranitelnosti. Úroveň zranitelnosti se dá zhodnotit na

základě citlivosti, což je v podstatě náchylnost aktiva být poškozeno hrozbou, a na základě kritičnosti, která odpovídá míře důležitosti aktiva pro subjekt (3).

1.8.4 Opatření

Opatření je proces, který byl speciálně navržen pro zmírnění působení dané hrozby, snížení zranitelnosti nebo dopadu hrozby. Předpokladem pro opatření je předejití vzniku škody nebo zmírnění následků této škody (3).

Z pohledu analýzy rizik je opatření definováno efektivitou a náklady. Efektivita určuje, jak opatření zmírní účinek dané hrozby. Tato efektivita se používá ve fázi zvládání rizik jako jeden ze základních parametrů při hodnocení použití daného opatření. Opatření má za úkol snížit úroveň hrozby, zranitelnosti, následků působení hrozby a podobně. Mezi náklady na opatření se řadí náklady na pořízení, zavedení a provozování opatření (3).

1.8.5 Riziko

Obecně pro riziko neexistuje uznávaná definice a je proto definováno různě. Je možné se setkat například s těmito definicemi:

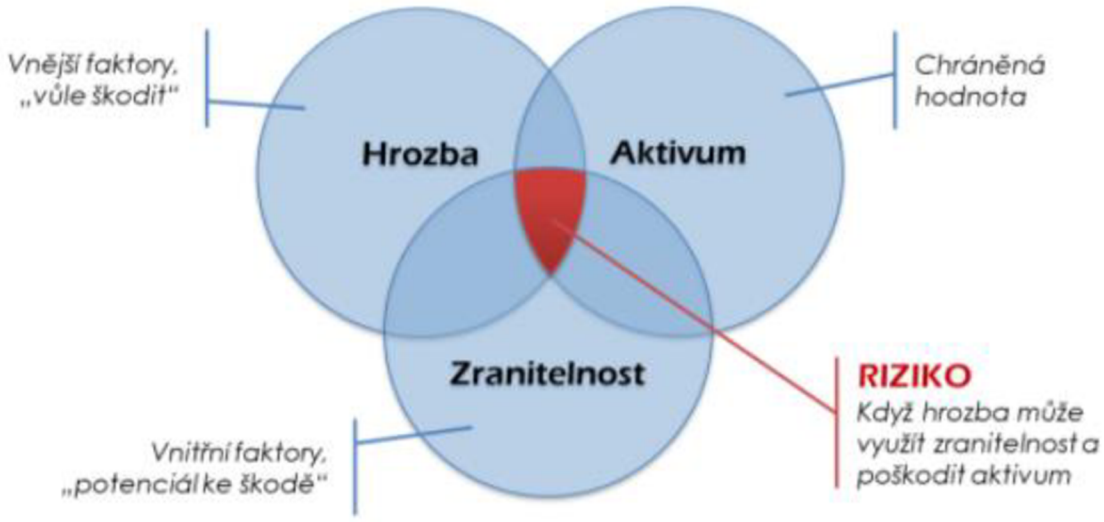
- Pravděpodobnost či možnost vzniku ztráty a obecně nezdaru
- Variabilita možných výsledků nebo nejistota dosažení daný výsledků
- Odchýlení skutečných výsledků od očekávaných (3).

S rizikem jsou tedy nejvíce spjaty dva pojmy. Prvním je pojem neurčitého výsledku. Aby riziko mohlo být nazýváno rizikem, musí existovat alespoň dvě různé variant řešení. Výsledek je tedy nejistý. Druhý pojem spjatým s rizikem je, že alespoň jeden z možných výsledků je nežádoucí. Může se jednat o ztrátu, například majetkovou, peněžní, a podobně (3).

Riziko je tedy vnímáno jako nebezpečí vzniku nějaké ztráty. Rizika obecně chceme snižovat a předcházet jim. Na základě tohoto předpokladu je prvním krokem k úspěchu provést analýzu rizik (3).

Riziko vzniká působením hrozby a aktiva. Hrozba, která nemá vliv na žádné aktivum v analýze rizik, nemusí být v analýze uváděno. Hodnotíme úroveň rizika. Tato úroveň je

vytvořena na základě hodnoty aktiva, zranitelností aktiva a úrovní hrozby působící na aktivum (3).



Obrázek 5: Analýza rizik
Zdroj: (28)

Červená oblast znázorněná na obrázku výše představuje riziko. Toto riziko by mělo být co nejmenší, to znamená, že průnik všech tří bublin by měl být co nejmenší (4).

1.8.6 Minimalizace rizik kritické infrastruktury

Než bude popsána minimalizace rizik v kritické infrastruktuře, je nutné uvést, co ona kritické infrastruktura je. Tento pojem představuje prvek nebo proces (nebo jejich množinu), u kterých by narušení nebo ztráta funkce mělo fatální dopad na nějakou množinu uživatelů (rodina, firma, spolek, a tak dále). Kritická infrastruktura byla více popsána výše v této kapitole (4).

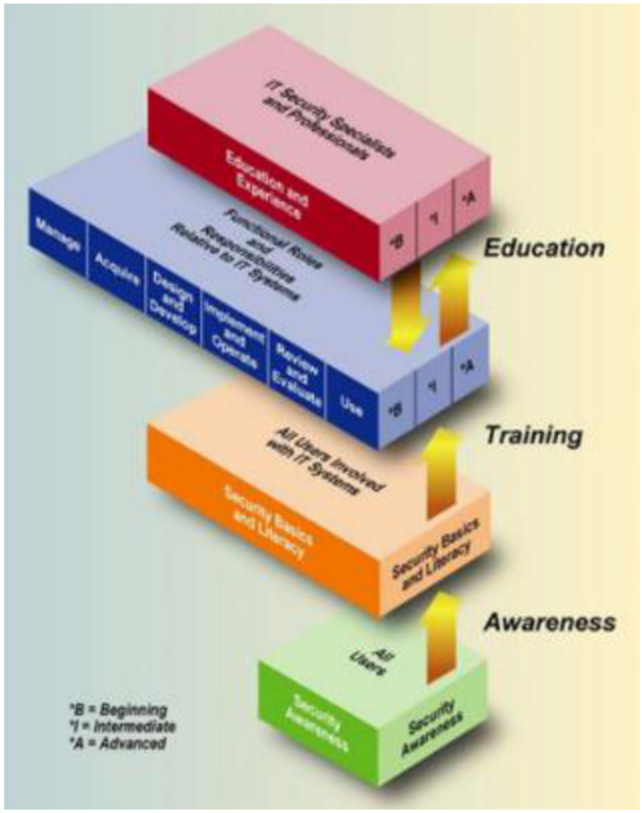
Při řešení minimalizace rizik jsou důležité dva body. Prvním je bezpečnost, do které se zařazují procesy, o které se stará obor bezpečnosti informačních a komunikačních technologií. Jedná se o bezpečnost dat, komunikační infrastruktury, kabeláže a aktivních prvků a tak podobně. Druhým bodem je spolehlivost. K tomu se řadí správný systémový a technický návrh, správný výběr materiálů, dlouhá MTFB (mean time between failures) neboli střední mezi poruchová doba, řízení systému a metody tohoto řízení (4).

1.9 SAE

Následně bude uveden pojem SAE neboli Security Awareness Education. Jednotlivá písmenka ve zkratce znamenají určitý pojem, který dopomáhá vzdělání uživatelů v rámci informační bezpečnosti. Awareness neboli podvědomí znamená schopnost uživatele rozpoznat a zamezit chování, které by mohlo mít vliv na informační bezpečnost. Training neboli výcvik nebo školení znamená akci, která je poskytována uživateli za účelem získání nových vědomostí, schopností a kompetencí. Education neboli vzdělání znamená, že se uživatel musí neustále vzdělávat, aby mohl odolávat bezpečnostním hrozbám. Čtvrtý pojem není přímo v názvu metodiky, ale je pro budování bezpečnostního povědomí velmi důležitý, a to je profesní rozvoj. Ten značí to, že člověk by se měl neustále učit a zdokonalovat (21).

SAE kontinuum je tvořeno vícerozměrným modelem. Tento model má čtyři patra. Do každého patra spadají jiní uživatelé. Například povědomí by měli mít všichni uživatelé, výcvik pak všichni uživatelé, kteří mají, co dočinění s IT systémy. Vzdělání je pak rozděleno na jednotlivé skupiny uživatelů, a to na začátečníky, středně pokročilé a pokročilé. Do stejných skupin se pak dělí i poslední stupeň v SAE kontinuu, a to profesní rozvoj. Profesní rozvoj je určen především pro specialisty v rámci informační bezpečnosti (21).

Celé SAE kontinuum je znázorněno na obrázku níže.



Obrázek 6: SAE kontinuum
Zdroj: (21)

SAE plán se skládá z několika kroků, které jsou potřeba naplánovat. Je jich celkem 11:

- Role a odpovědnosti v programu SAE
- Stanovení cílů pro každou fázi programu
- Rozdělení uživatelů pomocí analýzy
- Školící materiály dle skupin uživatelů
- Cíl pro každou skupinu
- Témata, která jsou potřebná probrat
- Metody nasazení pro každou část programu
- Dokumentace, zpětná vazba
- Vyhodnocení výuky a aktualizace školících materiálů
- Četnost školení
- Celková kalkulace (12).

Následně se musí plán implementovat. Tato implementace má tři stupně:

- Navržení programu, včetně strategie

- Vytvoření programu dle návrhu
- Implementace programu ve firmě (12).

V rámci SAE managmentu existují tři modely, dle kterých lze řídit bezpečnostní školení. Jedná se o centralizovaný systém, v tomto systému je veškerá odpovědnost na odpovědné osobě, což je většinou CIO nebo CISO. Dále pak částečně decentralizovaný model, kde jsou politiky a strategie školení na odpovědné osobě, ale implementace je distribuována mezi více lidí. Poslední model je plně decentralizovaný. V tomto modelu je na odpovědné osobě pouze tvorba politiky a všechny ostatní procesy jsou delegovány na jiné osoby (12).

1.10 Helpdesk

V této kapitole bude popsáno několik forem podpory, se kterou se uživatel může setkat. Helpdesk může být poskytován různými způsoby, a to jak telefonní linkou ve formě call center, emailem, aplikacemi nebo webem. Většinou se však uživatel může setkat s jakousi kombinací těchto prvků (5).

Podle dalšího zdroje se dají problémy helpdesku řešit pomocí položení tří otázek.

Helpdesk se dá pomyslně rozdělit na externí helpdesk a interní helpdesk. Rozdíl mezi nimi bude popsán níže (5).

Interní helpdesk

Zaměstnanci tohoto typu helpdesku se starají o uživatele ve stejné organizaci, ve které sami pracují (5).

Interní helpdesky se liší i napříč firmami. V menší firmě (cca 50-100 počítačů) funguje většinou takový helpdesk na domluvě. Zaměstnanec, který má nějaký problém zavolá IT podporu, která se většinou neskládá z mnoha jedinců (6).

Než bude popsáno, jak interní helpdesk funguje ve větší firmě, bude vysvětlena metodika ITIL.

Metodika ITIL

Metodika ITIL se dá charakterizovat jako soubor praxí prověřených konceptů a postupů, které firmě umožňují lepší plánování a využívání informačních technologií, a to jak ze strany

zákazníků, tak i ze strany dodavatelů IT služeb. Důležitými procesy v rámci ITIL metodiky jsou například:

- Risk management
- Firemní analýza
- Projektový management
- IT asset management (22).

Výše popsaná metodika se využívá při tvorbě helpdesků ve větších firmách (6).

Nevýhodou helpdesků ve větších firmách je že tyto interní helpdesky se nacházejí zpravidla v jiné zemi, a proto tato podpora zaměstnanců pokulhává na základě geografické polohy a nemožnosti komunikace z očí do očí a popřípadě i kvůli jazykové bariéře (6).

Existují základní praktiky pro to, jak mít úspěšný helpdesk. Ten může být založen například na ticketech.

ITSM – IT Service Management

To je souhrn nejlepších praxí a modelů procesů řízení služeb v IT oblasti. Představuje řízení komunikačních a informačních technologií, jejich provoz a rozvoj. Zahrnuje perspektivu zákazníka i poskytovatele IT služeb (23).

Ticketovací systém

Funguje tak, že pro každý incident nebo požadavek musí existovat ticket, pak se žádný úkol nemůže zapomenout ani ztratit (6).

Dále pak musí existovat nějaké úrovně podpory. Úroveň podpory stoupá na základě složitosti problému. Tyto úrovně jsou zpravidla tři. Na první úrovni člověk zanalyzuje problém a posoudí, zdali na něj stačí nebo je potřeba posunout ho na úroveň dva. Na úrovni dva jsou pracovníci obeznámeni s více technickými záležitostmi a jednají spíše o tak zvaných serverových záležitostech. Úroveň tři je potřebná ve chvíli, kdy jde o komplikovanou záležitost, na kterou nedostačuje odbornost pracovníků – často se tak volá k pomoci externí firma, která pomáhá tento problém řešit (6).

Kromě úrovně podpory je důležitá prioritizace úkolů. Každý ticket by měl být ohodnocen prioritou jeho plnění. Určitě by měl být stanovený čas na řešení problému (6).

Priorita a stanovený čas by měli být nastaveny na základě SLA (6). SLA znamená Service Level Agreement, a je to dohoda o úrovni poskytovaných služeb. Definuje rozsah, úroveň a kvalitu dané služby (6).

Je důležité sledovat, o jaký typ problému se jedná, zdali o požadavek na opravu, na nákup, a tak dále (6).
Úplně konečný stav je uzavření ticketu. Ticket musí být uzavřen s určitým výsledkem – tento výsledek volí manažer (6).

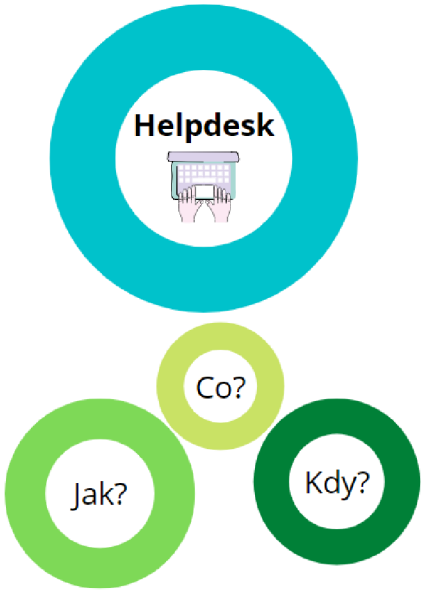
Externí helpdesk

Je určen pro zákazníky, kteří nejsou zaměstnáni v dané organizaci, ze které potřebují poskytnout radu nebo pomoc.

Mezi doporučení pro tvorbu kvalitního externího helpdesku patří tyto prvky:

- Přístup přes webové rozhraní – snadný přístup pro uživatele
- Nastavení uživatelských rolí – přihlašování pod různými rolemi – admin, zaměstnanec umožňuje nastavení odlišných práv a možností používání portálu
- Možnost konfigurace a eskalace
- Zaznamenání informací o stavu požadavku – zaznamenání každého problému (například ve formě výše uvedeného ticketu)
- Jednoduché a intuitivní rozhraní – pro méně zkušené uživatele
- Zabezpečený provoz – ochrana proti zneužití nebo napadnutí (autentizace)
- Možnost zasílání notifikací – upozornění na změny, a podobně
- Dokumentace požadavků – vyhledávací pole, možnost export, tisku, a podobně (7).

Jak bylo napsáno v úvodu kapitoly o helpdesku, podle dalších zdrojů se dá helpdesk rozdělit do různých rolí, které jsou v něm potřeba zastávat. Může se jedná o první, druhou nebo třeba třetí řadu technické podpory. Online poskytování podpory nebo třeba v rámci firmy může být prezenčně dostupný systémový administrátor. Všechny IT podpory, které pracují jako helpdesk, se ale z pohledu zaměstnance helpdesku týkají tří důležitých otázek: Co? Kdy? Jak?. Na tyto otázky se každý zaměstnanec helpdesku snaží najít odpověď (9).



Obrázek 7: Schéma otázek týkající se vedení helpdesku
Zdroj: Vlastní zpracování

Otázka „Co“ se snaží zjistit, co se změnilo, nebo se stalo předtím, než se problém projevil. Při poskytnutí podpory je nutné především snažit se zjistit, co se stalo nebo co se změnilo. Bez položení této otázky nelze zákazníkovi pomoct. Po zodpovězení otázky „Co“ se zúží počet možných scénářů, které se mohly stát (9).

Otázka „Kdy“ zjišťuje, kdy se daný problém projevil. Opět velmi důležitá otázka. Pro zaměstnance helpdesku je složité trasovat problém, který se odehrává už několik týdnů. Pro zjištění dlouho trvajícího problému se dá použít například Event Viewer (9).

Otázka „Jak“ zjišťuje, jak se daný problém začal projevovat. Tato třetí otázka se bere jako nejdůležitější ze všech tří uvedených. Autor v knize uvádí příklad, a to vypnutí počítače. Zákazník přijde na podporu a řekne, že svůj počítač vypnul, avšak počítač mohl vypnout pomocí tlačítka v menu Start, mohl dlouze podržet vypínací tlačítko nebo použil úplně jiný postup. Kvůli těmto případům je důležité pokládat otázku „Jak“ (9).

Autor v knize uvádí několik dalších rad pro řízení dobrého helpdesku. První radou je, že by zaměstnanec neměl mít předsudky a domněnky. Tato rada se týká jak lidí, tak i hardwaru, softwaru nebo aplikací. Dalším problémem, který se může objevit, je jazyková bariéra. Spousta firem má více poboček a helpdesk mají zavedený jen v rámci jedné země, kde se řeší všechny problémy všech dalších poboček ve světě. Z tohoto důvodu může být někdy těžší se spolu domluvit, protože lidé z některých zemí nemusí umět tak dobře daným

jazykem. Dalším faktorem je tak zvaný lidský faktor. S lidmi, kteří se nevyznají v technologiích a obecně počítačích, může dojít k diskomunikaci a ke špatnému pochopení se navzájem. Autor tedy popsal sedm jednoduchých kroků, jak s lidmi o problému mluvit:

- Zákazník nemusí být technicky založený a nemusí mít ani počítačovou gramotnost
- Adaptovat se na jejich styl komunikace a neshazovat se zbytečnými otázkami (například jestli drží správně počítačovou myš)
- Pokládat zákazníkovi pouze otázky, na které se dá odpověď krátce – nejlépe ano/ne
- Postupovat dle seznamu nejčastějších problémů a poruch a postupně je vylučovat
- Nemluvit příliš rychle a pamatovat na to, že zákazníkovi chceme vysvětlit problém pouze jednou
- Zaměstnanec zákazníkovi poradí určité postupy a měl by nechat zákazníka tyto postupy zopakovat, aby bylo jasné, že jim zákazník rozumí a nedošlo tak zbytečně k chybám
- Nedávat zákazníkovi příliš moc instrukcí v jeden moment (9).

Těchto sedm jednoduchých kroků zamezí zmatení a diagnóza problému proběhne rychleji a efektivněji (9).

1.11 Použité programy

V této kapitole budou popsány programy, které byly použity pro tvorbu diplomové práce.

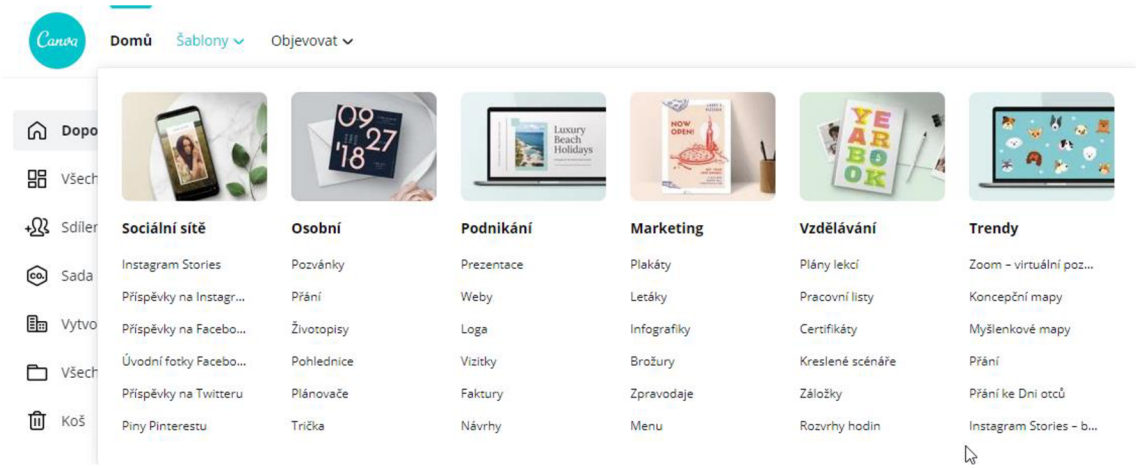
1.11.1 Canva

Canva je online dostupný software, který se používá přímo ve webovém rozhraní.

Zabývá se designem a návrhy. Canva je dostupná zdarma, ale v nabídce je i Canva Pro, jejíž používání je zpoplatněno (14).

Výhodou Canvy je to, že její použití pro studentské účely je zdarma. Dalším stupněm je pak Pro licence, která je pro profesionální designéry a dále pak Enterprise licence, která je určena pro firmy a společnosti. Placená verze je obohacená tím, že se dá pracovat na návrzích

společně s lidmi v týmu. Takzvaná Free verze ale obsahuje více než 250 000 šablon a 5 GB prostoru k uložení svých návrhů a dat (14).

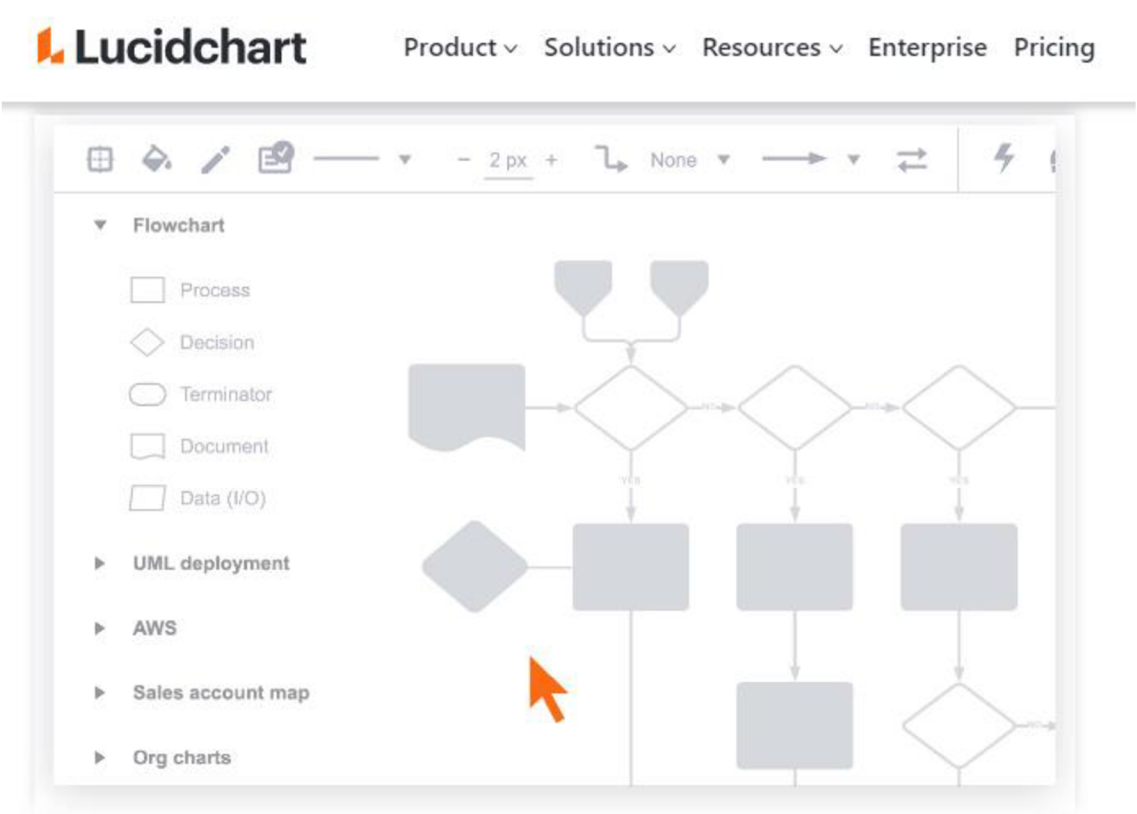


Obrázek 8: Náhled uživatelského rozhraní softwaru Canva
Zdroj: (14)

Při tvoření návrhů je k dispozici výběr z několika možný designových prototypů. Na výběr jsou zde loga, plakáty, fotokoláže, prezentace a podobně. Je možné sem nahrávat vlastní obrázky, které se dají upravovat. Anebo vytvářet návrhy nové z již nahraných vzorů, obrázků, animací a podobně. Obrázky se dají i popisovat textem, kterému jde měnit font, barva a velikost. Možné je použití filtrů a jiných upravovacích nástrojů (14).

1.11.2 Lucidchart

Lucidchart je jednoduchý online nástroj pro vytváření diagramů. Jelikož je to cloudová aplikace, umožňuje práci všem operačním systémům – podporuje Windows, Mac i Linux. Má na výběr z celkem 500 šablon pro vytvoření nového návrhu. Uživatelům usnadňuje práci možnost importu dat z Excelu, Zapieru, Salesforcu či LinkedInu. Je zde možnost spolupráce v týmu, to znamená, že každý člen týmu má přístup k danému návrhu a může ho dotvořovat anebo na něj pouze nahlédnout. Lucidchart dává uživatelům tu výhodu, že uživatel, který nepotřebuje editovat návrhy má pouze free licenci, díky které vidí návrhy jiných uživatelů. Uživatelé, kteří tvoří návrhy musí mít editorskou licenci, jejíž užívání je zpoplatněno (13).



Obrázek 9: Náhled uživatelského prostředí Lucidchart
Zdroj: (13)

Na obrázku výše je vidět, jak vypadá menu pro tvorbu vývojového diagramu. Podobný vývojový diagram bude použitý i v diplomové práci pro znázornění workflow jednotlivých procesů (13).

2 ANALÝZA SOUČASNÉHO STAVU

V praktické části se zaměřím na popis společnosti ISIT Slovakia s.r.o. a následně i na krátký popis společnosti SEVITECH CZ s.r.o.

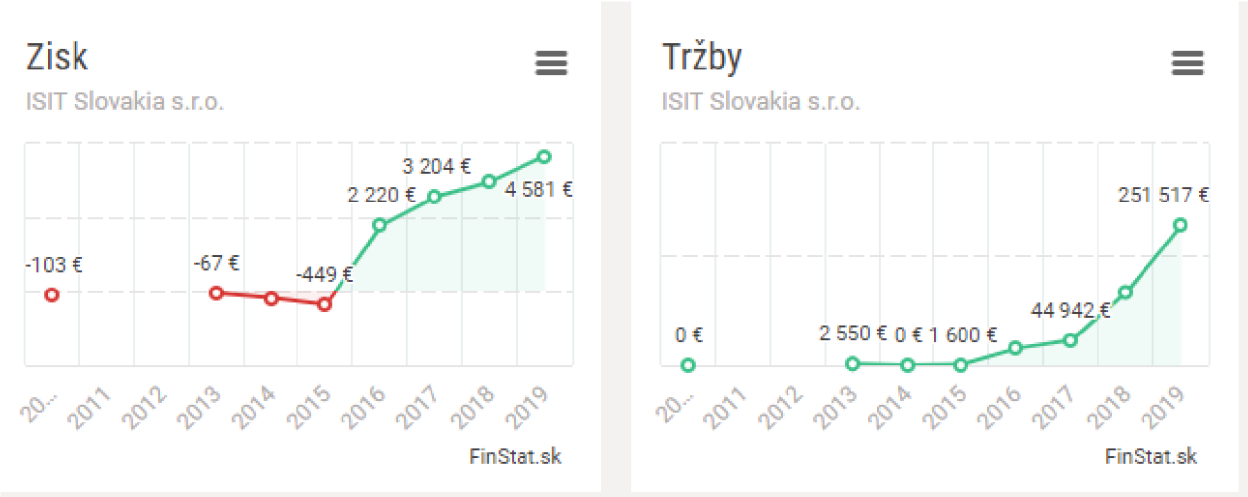
Popíšu, čím se firma ISIT Slovakia zabývá a jaký vyvíjí softwarový produkt. Tento software níže popíšu detailněji, jak vizuálně, tak funkčně. V poslední části kapitoly se zaměřím na současnou podobu firemního helpdesku.

Firmu SEVITECH CZ s.r.o. popíšu stručněji, protože se jedná pouze o výhradního prodejce softwaru v České republice.

2.1 Popis společnosti ISIT Slovakia s.r.o.

Společnost byla založena 3. 6. 2009 v Bratislavě. Základní kapitál byl složen ve výši 6 000 eur. Podle účetní závěrky se firma řadí mezi „Ostatné služby týkajúce sa informačných technológií a počítačov“. Podle dat poskytnutých z finančního statistického úřadu vykazuje společnost trvalou ziskovost i rostoucí míru tržeb.

ISIT Slovakia s.r.o. se zabývá komplexními službami v oblasti informační bezpečnosti a ochrany osobních údajů – GDPR. Poskytuje poradenské a auditorské služby týkající se GDPR podle aktuálně platných zákonů. Její práce se zaměřuje i na školení oprávněných osob. Je totiž důležité udržování a budování bezpečnostního povědomí v organizacích, zpracovávání bezpečnostní dokumentace a taktéž navrhování bezpečnostních opatření a implementaci podmínek dle Nařízení Evropského parlamentu a RADY EU 2016/679 o ochraně fyzických osob při zpracovávání osobních údajů a o volném pohybu těchto údajů v přechodném období (8).



Obrázek 10: Grafové znázornění zisku a tržeb firmy ISIT Slovakia s.r.o.
Zdroj: (24)

Na základě těchto nařízení firma začala vyvíjet nový software, který se nazývá ESKO software CZ. Software představuje řešení pro řízení systémové ochrany údajů a informační bezpečnosti. Základní požadavky informační bezpečnosti jsou dostupnost, důvěrnost a integrita citlivých dat. Prostřednictvím softwaru ESKO firma pomáhá tyto tři aspekty splňovat (8).

Distributor pro prodej softwaru v České republice je firma ISIT SOFTWARE CZ s.r.o. Tato firma byla založena 27. 8. 2020 v Brně. Základní kapitál složila ve výši 200 000 Kč. Tato firma je dceřinou společností již výše zmíněné slovenské firmy (25).

Výhradními prodejci softwaru jsou firmy SEVITECH CZ s.r.o. a DITEC.

Společnost Sevitech se specializuje na dodávání IT služeb se zaměřením na podnikové a manažerské systémy, webové aplikace, outsourcing služeb, konzultační a analytické služby a dále například řízení komplexních projektů. Firma pod daným názvem společnosti funguje od roku 2018 (26).

2.2 O softwaru

Na začátek je nutné zdůraznit, že software je stále ve stádiu vývoje. Některé části a moduly ještě nejsou dodělané, a proto se diplomová práce bude převážně zabývat dokončenými částmi. Konkrétně se stále pracuje na vývoji Kybernetické bezpečnosti organizace (dále KBO) a modul GDPR je už zcela hotový.

Software je dostupný ve slovenském, českém a anglickém jazyce. Je vytvořen na základě informační a kybernetické bezpečnosti na základě praktických zkušeností v právním rámci české a slovenské legislativy při řízení procesů kybernetické bezpečnosti, ochrany osobních údajů a podobně.

Výhody používání software jsou následující:

- Řízení procesů kybernetické bezpečnosti a ochrany osobních údajů/GDPR
- Auditorský nástroj
- SW obsahuje vzorová data pro správné provedení příkazů
- Licence se updatuje o všechny změny, aby nebyla opomenuta žádná změna v zákonech
- Vlastník SW může využít poradenství (8).

2.2.1 Licenční podmínky a specifikace licencí

Rozlišují se dva typy licence. Licenci klient a licenci admin (8).

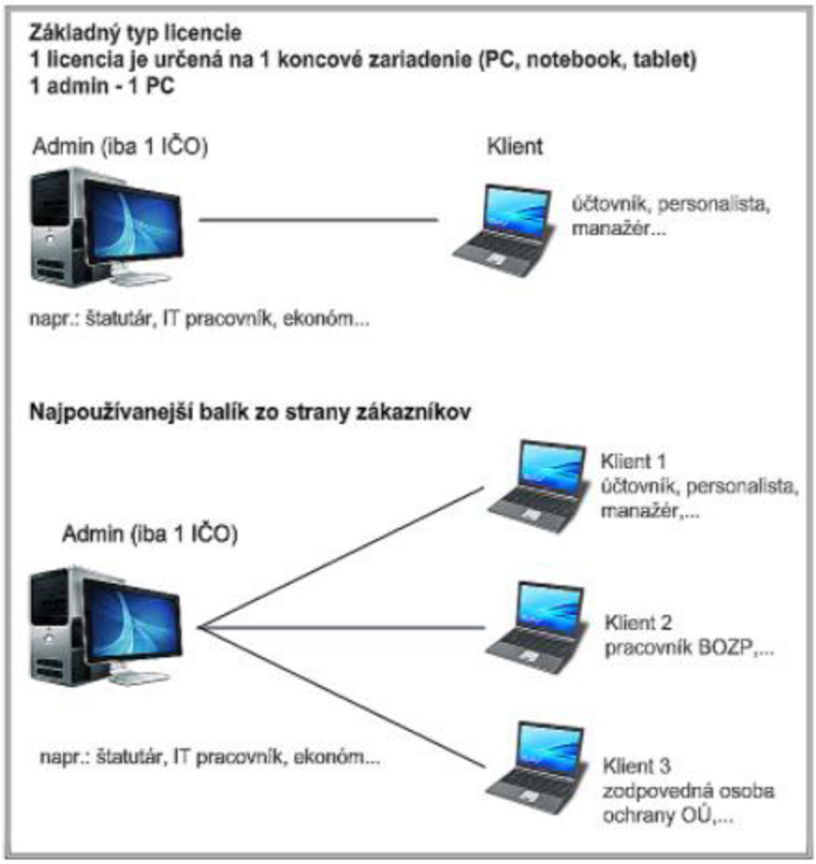
- Základní licence – určená pro jeden počítač
- Admin licence – určená pro instalaci produktu na server (server může být i počítač, který je vyhrazený pro práci s hlavní aplikací a slouží zároveň jako úložiště dat)
- Klientská licence – určená pro instalaci na počítači klienta, umožňuje spouštět SW ve variantě, kdy se uživatel připojuje na centrální databázi s omezenými právy
- Demo verze – je to bezplatná licence, která se smí používat na libovolném počtu počítačů současně, firma neodpovídá za vady ani za škodu (8).

Součástí každé placené licence je licenční klíč (8).

Software je vhodný pro všechny typy podniků. Od malých až po velké (8).

Pro malou firmu je vhodná jedna licence s jedním adminem. Licenčně je pokrytá pro jedno IČO a je uplatnitelná pro jeden počítač. Pokud je potřeba zakoupit další licence, můžou se volit ty na klientské bázi. Stejný typ je vhodný i pro střední anebo velký podnik (8).

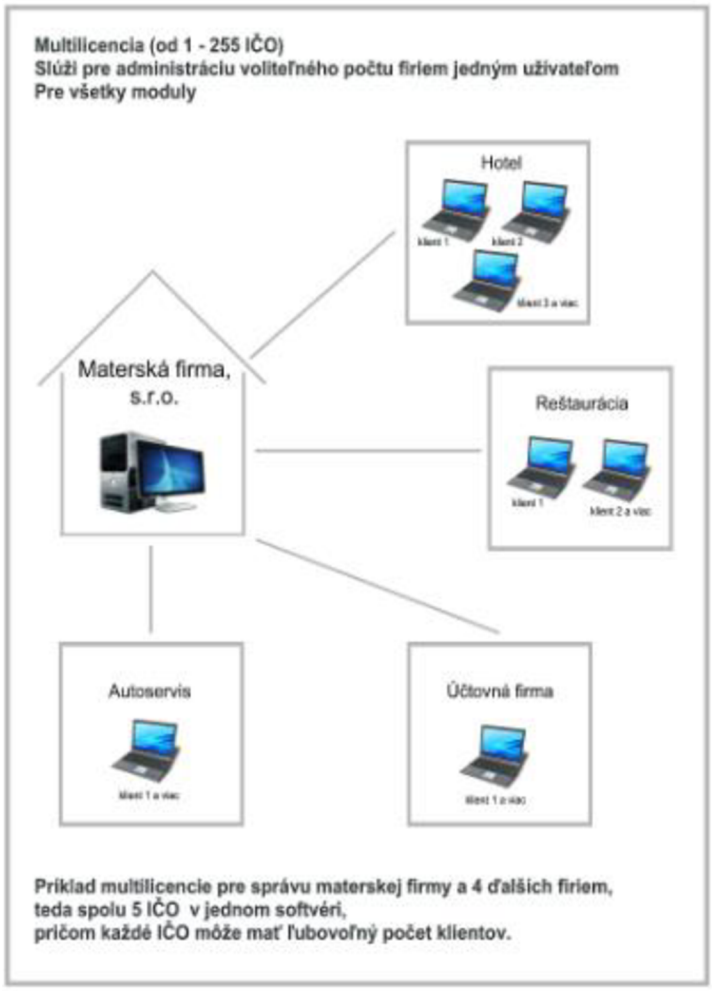
Níže na obrázku je schéma, na kterém je znázorněno, jak může být použita admin licence s klient licencí.



Obrázek 11: Použití admin a klient licence
Zdroj: (8)

Pokud je potřeba licence pro více firem, avšak pod stejným IČO, je vhodné zvolit jiný typ licence a to multilicenci. Ta funguje pro jednu až několik firem. Každá samostatná firma si však musí pořídit alespoň jednu klientskou licenci, aby mohla klientská licence komunikovat s multilicencí. V rámci zakoupení roční licence je v ceně podpora na 12 měsíců zdarma. V případě vypršení jednoho roku užívání je možné provést takzvaný renewal maintance (což je vlastně obnovení platnosti licence na další období), kdy se dá uplatnit sleva na produkt ve výši 10 % (8).

Níže je vidět schéma znázorňující možné použití multilicence.



Obrázek 12: Použití multilicence
Zdroj: (8)

2.2.2 Systémové požadavky SW

SW pracuje na principu klienta a databáze SQL. Databáze je umístěná na lokálním počítači, serveru s operačním systémem Windows anebo na cloudu v data centrech. Všechny části systému spolu s databázovým serverem jsou součástí instalačního souboru. Součástí každé licence je instalační manuál a uživatelská příručka (8).

Níže jsou uvedeny systémové požadavky, aby bylo program možné spustit a díle s ním pracovat:

- Windows 7 SP1 a vyšší
- 2 GB RAM
- NET Framework 4.5

- Databázový server SQL nebo předplatné Windows Azure (balíček obsahuje Microsoft SQL server)
- 10 GB volného místa na systémovém disku
- Rozlišení monitoru 1920x1080 (8).

Systém je možný propojit s již existujícími softwary, například s účetním softwarem SAP (8).

2.2.3 Hlavní moduly programu

V následující části práce popíšu jednotlivé moduly, které jsou v programu dostupné. Dále krátce popíšu jednotlivé záložky, které se dají v jednotlivých modulech najít.

Modul eGDPR

Modul je organizačním a technickým opatřením v informačním systému, který řídí evidenci informačních systémů – agend. Řídí management bezpečnostních incidentů a generuje odpovědi zodpovědným osobám. Nabízí i vzorkovou bezpečnostní dokumentaci, záznamy o likvidaci osobních údajů, kamerový monitorovací systém, test proporcionality a interní automatizovaný audit (8).

Tento modul je již plně funkční.

Modul GDPR s vazbami posouzení DPIA

Jedná se o plnohodnotný modul, který obsahuje test proporcionality a vazby posouzení vlivu DPIA podle vyhlášky Úřadu na ochranu osobních údajů č. 158/2018 – evidence podpůrných aktiv, klasifikace jich a vlastníků, identifikace hrozeb, rizik, zranitelnosti a dopadů. Analýzy a vazby s generováním dokumentu Posouzení vlivu pro jednotlivé zpracovatelské činnosti v konkrétních účelech zpracování (8).

Je zde možné provádět evidenci informačních systémů i agend, k dispozici je vzorová bezpečnostní dokumentace, evidence souhlasů či nesouhlasů subjektů údajů, test proporcionality a možnost provedení interního automatizovaného auditu. Management bezpečnostních incidentů, záznamy o likvidaci osobních údajů (8).

Tento modul je rovněž plně funkční.

Obrázek 13: Modul GDPR a jeho funkce
Zdroj: (8)

Modul kybernetická bezpečnost organizace (KBO)

Na začátek je důležité zmínit, že tento modul je stále ve fázi vývoje a probíhají finální úpravy, aby se mohl začít dodávat firmám, které o něj mají zájem.

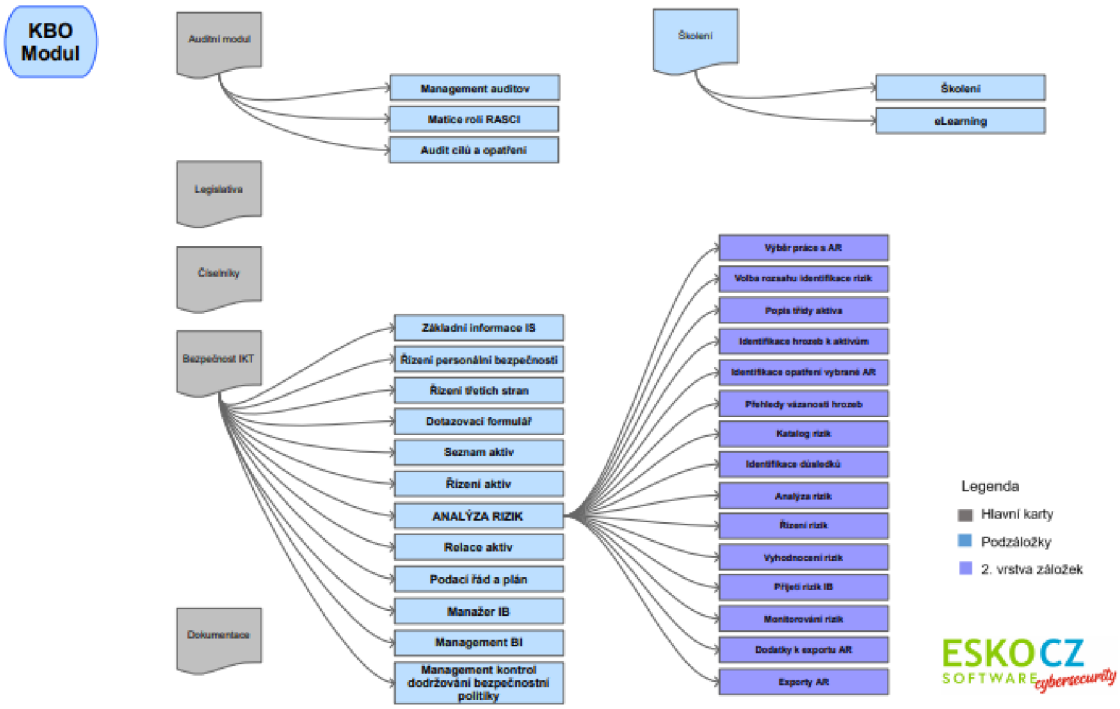
Modul pracuje v souladu se zákonem o kybernetické bezpečnosti. Přehledně se zde vedou dokumenty související s procesy a prvky kybernetické bezpečnosti. Nachází se zde management informačních rizik – evidence a ohodnocování aktiv, vlastníci aktiv, zranitelnost aktiv, hrozby spojené se zranitelností aktiv, evidence a ohodnocování rizik a jejich dopadů, dále pak přijatá ochranná opatření (8).

Software nabízí rozmanitý seznam tříd aktiv, která se dají vnímat jako podpůrná aktiva dle normy ISO/IEC27005 (8).

Na následujícím obrázku je vidět z jakých částí se KBO modul skládá. A že je funkčně propojen i s modulem GDPR a například i s e-learningovými programy.

Obrázek 14: Modul KBO a jeho funkce
Zdroj: (8)

Dále jsem vybrala obrázek, na kterém je dobře znázorněn obsah jednotlivých záložek v programu.



Obrázek 15: Modul KBO a jednotlivé záložky programu
Zdroj: (8)

Šedou barvou jsou znázorněny hlavní karty. To je Auditní modul, Legislativa, Číselníky, Bezpečnost IKT a Dokumentace. Světle modrou barvou jsou znázorněny podzáložky a fialovou pak druhá řada podzáložek.

Všechny záložky budou popsány níže, ale jejich celková funkčnost bude popsána až v kapitole, která se zabývá funkčností programu – kapitola 2.2.5.

První záložkou je Auditní modul, která byla vytvořena speciálně pro auditory. Nachází se zde evidenční část všech realizovaných auditů, matice rolí RASCI a audit cílů a opatření.

Dále jsou v programu dvě záložky – Legislativa a Číselníky, které nejsou ve schématu plně znázorněny, a proto si je více popíšeme v kapitole 2.2.5.

Z obrázku je patrné, že nejrozsáhlejší je část Bezpečnost IKT. Je zde celkem 12 podzáložek. Jsou to záložky: Základní informace IS, Řízení personální bezpečnosti, Řízení třetích stran, Dotazovací formulář, Seznam aktiv, Řízení aktiv, Analýza rizik, Relace aktiv, Podací řád a plán, Manažer IB, Management BI a Management kontrol dodržování bezpečnostní politiky. Na obrázku je opět vidět, která z podzáložek má největší obsah – je to podzáložka

Analýza rizik. Je zde dalších 15 podzáložek. Je to například: Popis třídy aktiva, Katalog rizik a Vyhodnocení rizik.

2.2.4 Doplňkové moduly

Program má k dispozici dva doplňkové moduly. Jeden z nich se týká kategorizace prací z hlediska zdravotního rizika. Druhý je určen na komplexní správu zaměstnaneckých benefitů, které chce zaměstnavatel evidovat a vyhodnocovat v časových intervalech. Jedná se například o tyto benefity: stravenky, služební auto, mobilní telefon, a tak dále (8).

2.2.5 Program – funkcionalita a vzhled

Obrázek 16: Úvodní obrazovka programu
Zdroj: Vlastní zpracování

Obrázek výše znázorňuje úvodní obrazovku po otevření programu. Na úvodní obrazovce je název softwaru, jazyk aplikace, ikonka klíče, otazníku a pak dvě hlavní tlačítka na spuštění modulů.

Jazyk aplikace lze měnit mezi českým jazykem a slovenským jazykem. Další jazyky zatím nejsou dostupné, ale plánuje se i anglická verze.

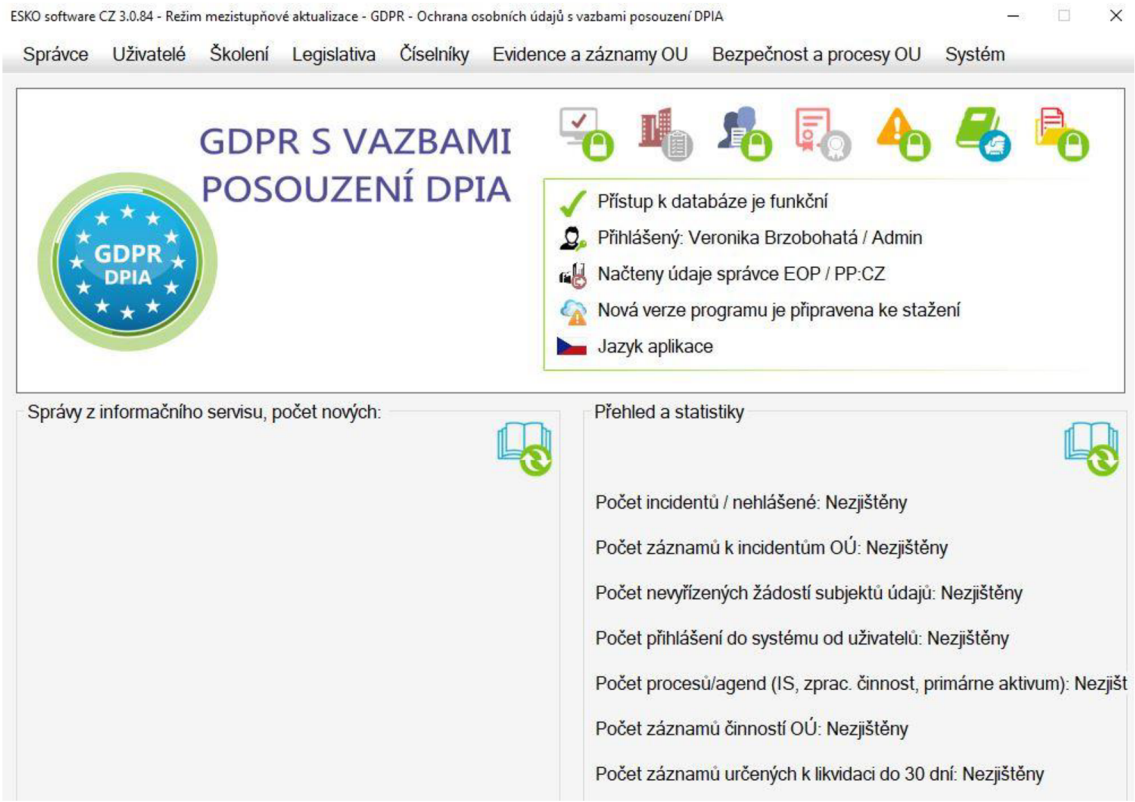
Malá ikonka klíče slouží k aktivacím v rámci programu. Dají se zde aktivovat extra moduly dostupné v rámci programu. Jsou zde vidět i informace o platnosti licence, licenční kód a pod kterou firmu licence spadá.

Druhá malá ikonka otazníku znázorňuje nápovědu a pomoc v rámci softwaru. Funkcionalita v rámci tohoto tlačítka bude blíže popsána v kapitole 2.4 Současná forma helpdesku v programu.

Následují dvě velká tlačítka. Tato tlačítka spouští konkrétní modul, který chce uživatel v danou chvíli používat. Po kliknutí na některý z modulů se objeví přihlašovací okno. Po zadání přihlašovacích údajů (jména a hesla) může uživatel začít s daným modulem pracovat.

GDPR

Po kliknutí na tlačítko GDPR S VAZBAMI A POSOUZENÍ DPIA se objeví nové okno s funkcionalitami spjatými s daným modulem. Toto okno je vidět na obrázku níže.



Obrázek 17: GDPR tlačítko
Zdroj: Vlastní zpracování

V rámci okna je v levé části obrazovky vidět, ve kterém modulu se zákazník právě nachází. V pravé polovině okna jsou vidět základní údaje o tom, kdo je přihlášený, zda je dostupný přístup k databázi a popřípadě, jestli existuje nová verze programu (obrázek mráčku s oranžovým vykřičníkem). Nad těmito základními informacemi se nachází sedm nejpoužívanějších ikon v rámci programu. Tyto ikony lze různě měnit podle potřeby. V horní liště se nachází několik záložek, které jsou pro tento modul stěžejní z hlediska funkčnosti, vyplňování údajů a na jejich základě pak probíhá vyhodnocování. Záložek je zde celkem osm. Níže je podrobnější popis všech uvedených záložek.

V rámci záložky Správce má zákazník možnost upravovat informace týkající se organizace, která software využívá. Je možnost používat software pro více firem a pomocí tohoto pole přepínat mezi jednotlivými firmami.

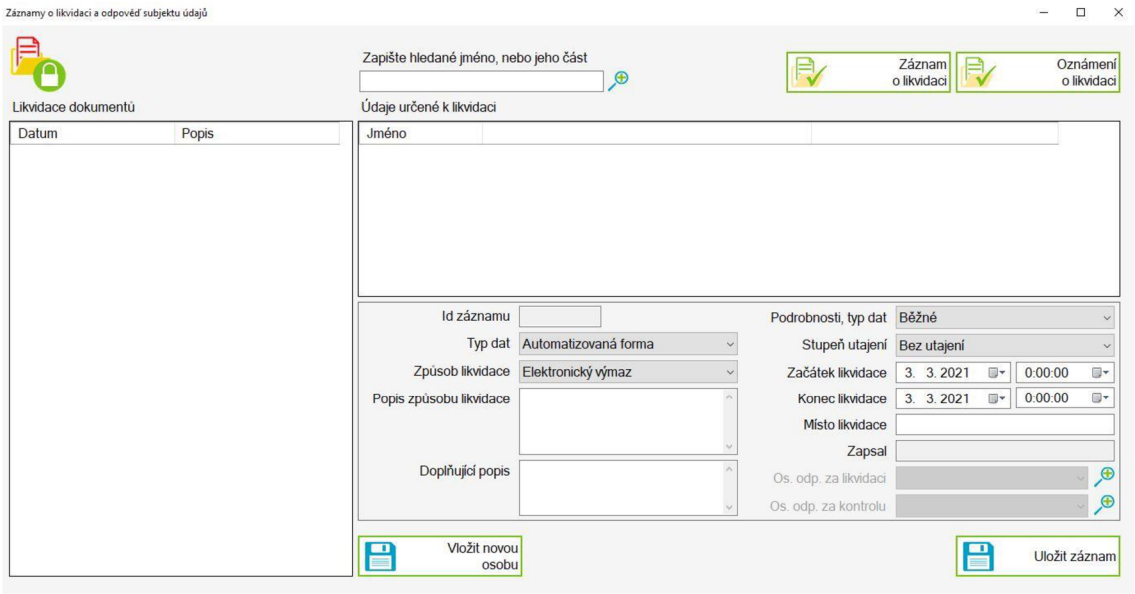
V záložce Uživatelé je možnost přidání či odebrání nebo úprava uživatelů, kteří používají daný software. Na úvodní obrazovce GDPR modulu je v pravé části vidět, kdo je zrovna přihlášený v programu.

V záložce Školení jsou dostupné Vzory školení pro oprávněné osoby – to jsou například Povinnosti v oblasti ochrany osobních údajů 2020. A dále pak možnost účastnit se nějakého e-learningu. Je zde obecný popis školení, dále pak objednávkový systém a přihlášení do e-learningu.

V záložce Legislativa jsou dostupné tři legislativy. Jedna se týká legislativy v rámci Slovenské republiky, další pak v rámci České republiky a konečně třetí v rámci mezinárodně platných standardů.

Záložka Číselníky představuje v podstatě seznam jednotlivých segmentů.

Záložka Evidence a záznamy OU, jak už název vypovídá, obsahuje evidenci a záznamy spojenými s ochranou osobních údajů. Níže na obrázku je zobrazen ovládací panel, kterým je možné odstraňovat záznamy, které již firma nepotřebuje uchovávat. V této záložce pak bude seznam již nepotřebných a zlikvidovaných údajů.



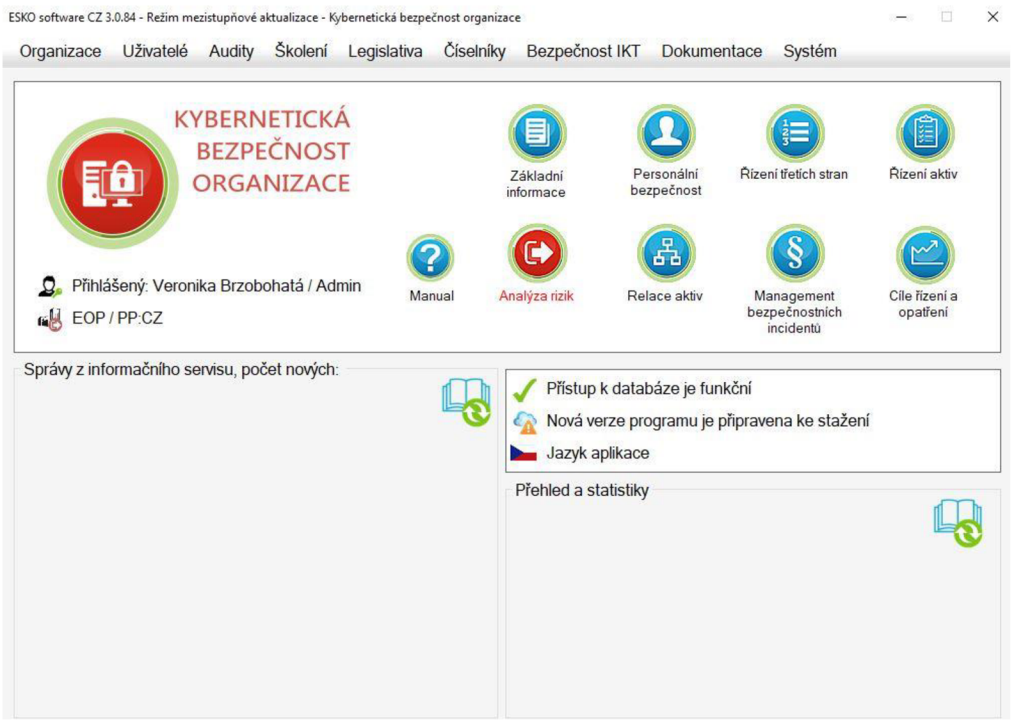
Obrázek 18: Záznamy o likvidaci záznamů
Zdroj: Vlastní zpracování

Záložka Bezpečnost a procesy OU, jak už název vypovídá, znázorňuje jednotlivé procesy, které se týkají osobních údajů, ve firmě a hodnotí se jejich bezpečnost.

Poslední záložkou je záložka Systém. V této záložce si uživatel nastavuje aplikaci a přístup do databáze, dále pak odpovědné osoby, externí přístupy a podobně. V rámci záložky se dají importovat údaje z programů Excel nebo mzdových a personálních systémů. Je zde přístupné tlačítko Pomoc, které, jak bylo zmíněno výše, bude blíže popsané v kapitole 2.4. Je zde i možnost zálohy a obnovy databáze, zjištění, zda existuje nová verze programu a aktivace programu, která je dostupná z úvodní obrazovky po zapnutí programu a je znázorněná tlačítkem s klíčem.

KBO

Z úvodního okna je dostupné druhé velké tlačítko a po kliknutí na toto tlačítko se zobrazí modul KYBERNETICKÁ BEZPEČNOST ORGANIZACE. Níže na obrázku je vidět nově otevřené okno.



Obrázek 19: KBO tlačítko
Zdroj: Vlastní zpracování

Okno modulu je v podstatě identické jako v případě GDPR modulu. Rozdílem je, že v levé části okna se nachází název modulu a hned pod ním je vidět, kdo je v programu přihlášen. Ostatní základní informace, jako například verze programu, jazyk a přístup k databázi, se nachází v levé části okna pod jednotlivými nejpoužívanějšími ikonami. Tyto ikony lze měnit podle potřeby.

V horní liště se nachází devět záložek. Níže budou záložky popsány podrobněji.

První záložka se jmenuje Organizace. Tato záložka je v podstatě identická se záložkou Správce v modulu GDPR. Zákazník má možnost upravovat informace týkající se organizace, která software využívá. Je možnost používat software pro více firem a pomocí tohoto pole přepínat mezi jednotlivými firmami.

Druhá záložka se týká uživatelů. Opět je tato záložka identická se záložkou Uživatelů v modulu GDPR.

Novinkou tohoto modulu oproti GDPR je záložka Audity. V rámci této záložky je dostupný management auditů, RASCI matice a cíle řízení a opatření. Tento modul je důležitý pro auditory.

V záložce Legislativa jsou dostupné tři legislativy. Jedna se týká legislativy v rámci Slovenské republiky, další pak v rámci České republiky a třetí v rámci mezinárodně platných standardů.

Číselníky představují seznamy jednotlivých prvků v rámci daného modulu. Je zde například číselník hrozeb, kde můžeme najít, jaké všechny hrozby jsou v programu již přednastavené a může se s nimi v dalších částech programu pracovat. Dále například číselník rizik a tak dále.

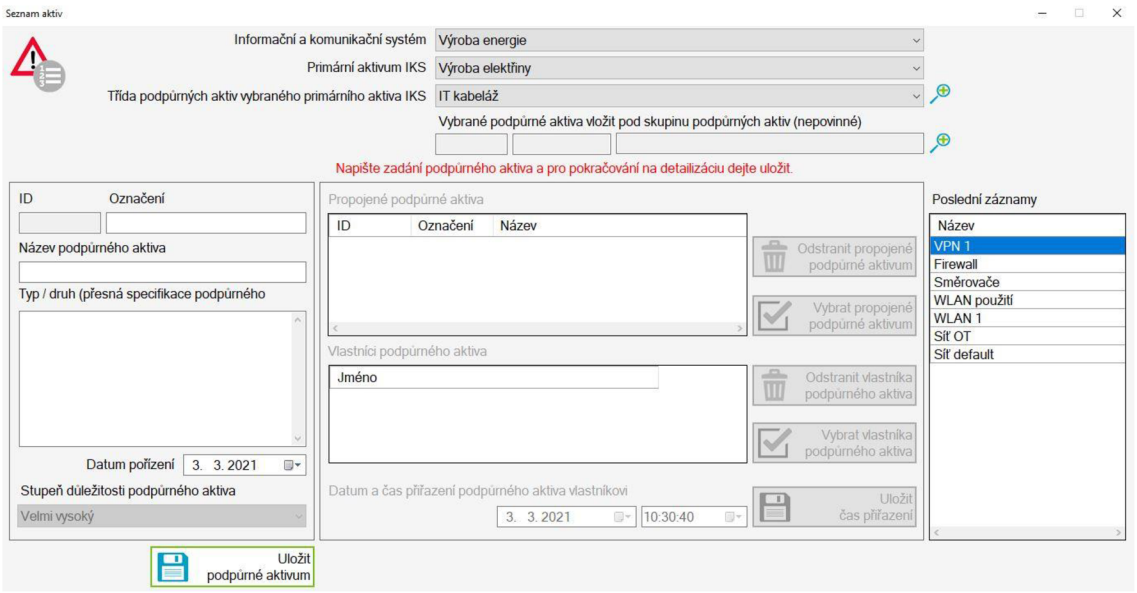
Bezpečnost IKT

Bezpečnost IKT je nejdůležitější záložkou modulu, protože zde se tvoří analýza rizik. Nachází se zde podzáložky jako seznam aktiv, řízení těchto aktiv, relace aktiv a podobně. Jelikož zde probíhá nejvíc úkonů, které musí uživatel provést, rozhodla jsem se vypsat podzáložky detailněji do jednotlivých odstavců.

První věc, která je důležitá pro správnou funkčnost programu je vyplnění podzáložky Základní informace. Zde se přidává nový informační komunikační systém (dále IKS). Po zadání IKS se do programu přidají primární aktiva. Na pravé straně obrazovky jsou další informace, které můžeme doplnit k primárnímu aktivu. Například v záložce Bezpečnostní model je důležité zvolit odpovídající bezpečnostní model a správné nastavení legislativy. Dále pak v záložce Role a uživatelé se vybírají již dříve vytvoření uživatelé v záložce Uživatelé. Těmto uživatelům jsou přiřazována primární aktiva a určují se garanti aktiv.

Po vytvoření IKS a primárních aktiv se uživatel opět vrátí do záložky Bezpečnost IKT a vybírá druhou podzáložku, což je Personální bezpečnost. V této podzáložce se vybírají již vytvoření uživatelé, které pak dále budeme chtít zvolit jako garanty aktiva.

Další podzáložkou je Seznam podpůrných aktiv, kde se přiřazují podpůrná aktiva k primárním aktivům. Na tato podpůrná aktiva opět existuje seznam v číselníku, ze kterého si může uživatel aktiva vybrat. Pokud ovšem není v seznamu dané podpůrné aktivum může si ho uživatel nově vytvořit pomocí formuláře znázorněného níže. Ve formuláři je nejdůležitější správně vyplnit IKS a primární aktivum.



Obrázek 20: Seznam aktiv
Zdroj: Vlastní zpracování

V podzáložce Řízení aktiv se vybírá třída podpůrného aktiva. Hvězdičkou jsou zde označena systémem přednastavená aktiva, pod která se nedají přiřazovat podpůrná aktiva. Toto nastavení lze ale změnit. Třídy slouží k řízení funkcí nástroje, z nichž nejdůležitější je skrývání nebo zobrazování třídy aktiv v dalším běhu nástroje a po naplnění příslušnými aktivy. Tato funkce byla zavedena z důvodu toho, aby se zobrazovala jen ta aktiva a související hrozby, zranitelnosti a opatření, které jsou do nástroje vloženy. Záměrem je nezatěžovat pracovníky informacemi z nezavedených technologií neboli nezavedených podpůrných aktiv.

Relace aktiv představuje namapování nových aktiv, hrozeb, opatření a zranitelností.

V podzáložce Analýza rizik se pak vytvoří nová nebo se otevře existující analýza. V případě, že by chtěl uživatel analýzu vyexportovat, klikne na tlačítko export analýzy a software mu dá vybrat, kterou část analýzy chce vyexportovat. V pravé části obrazovky se zase objeví několik záložek. Například v záložce Identifikace zavedených opatření se nachází zaklikávací pole, které se zaškrtne v případě, že opatření bylo zavedeno. Opatření se uloží i s údajem, kdo opatření zavedl.

Dokumentace byla popsána výše a detailnější popis funkčnosti již není potřebný.

Poslední záložkou je záložka Systém, která je identická se záložkou Systém v modulu GDPR. Nebude již proto znovu popisována.

KBO a GDPR – společná funkcionalita

Každá licence obsahující hlavní moduly – tedy GDPR a KBO. Tyto dva hlavní moduly mají společnou některou funkcionalitu, která bude popsána v této kapitole.

Je to například forma licencování a personalizace uživatelských práv. Stejnou funkcionalitu má i management bezpečnostních incidentů z pohledu řízení bezpečnostních incidentů s celkovým hlášením pro manažera informační bezpečnosti. Pouze z pohledu řízení bezpečnostních incidentů je vyvinuto individuální řešení pro každý modul, a to z důvodu odlišné legislativy.

Důležitý je i monitoring přístupů, který se nachází v části Systém a zaznamenává přístupy jednotlivých uživatelů k citlivým datům. Monitoring je vytvářen pomocí časových razítek, identifikací uživatele, konkrétní událostí a detailem oné události.

Funkce importu údajů je rovněž u obou modulů stejná. Zákazník má možnost importovat data z externích databází, z personálních a mzdových programů či z externích systémů pomocí MS Office Excel.

Data je možné zálohovat, a to vytvářet zálohy ke konkrétnímu datu, zálohovat databáze a vybírat data ze záloh.

Důležitá je i funkce pro pomoc. Je to forma helpdesku, kterou lze najít přímo v programu. Jsou zde umístěny manuály k aplikaci, zákaznická podpora ve formě telefonických a emailových kontaktů a technická podpora doplněná o možnost využití programu TeamViewer. Je zde přímo odkaz na stažení programu TeamViewer. Dále se zde nacházejí opravné balíčky pro tiskové sestavy a databáze MS Access.

2.3 Současná forma helpdesku

2.3.1 Současná forma helpdesku na webu

Helpdesk na webové stránce můžeme najít jako čtvrtou záložku v menu. Tato záložka je nazvaná jako Podpora.

Obrázek 21: Náhled záložek na webové stránce
Zdroj: (8)

Tato záložka je rozdělena do několika sekcí:

- FAQ – nejčastější dotazy
- Zákaznická podpora
- Technická podpora
- Video návody
- Systémové požadavky

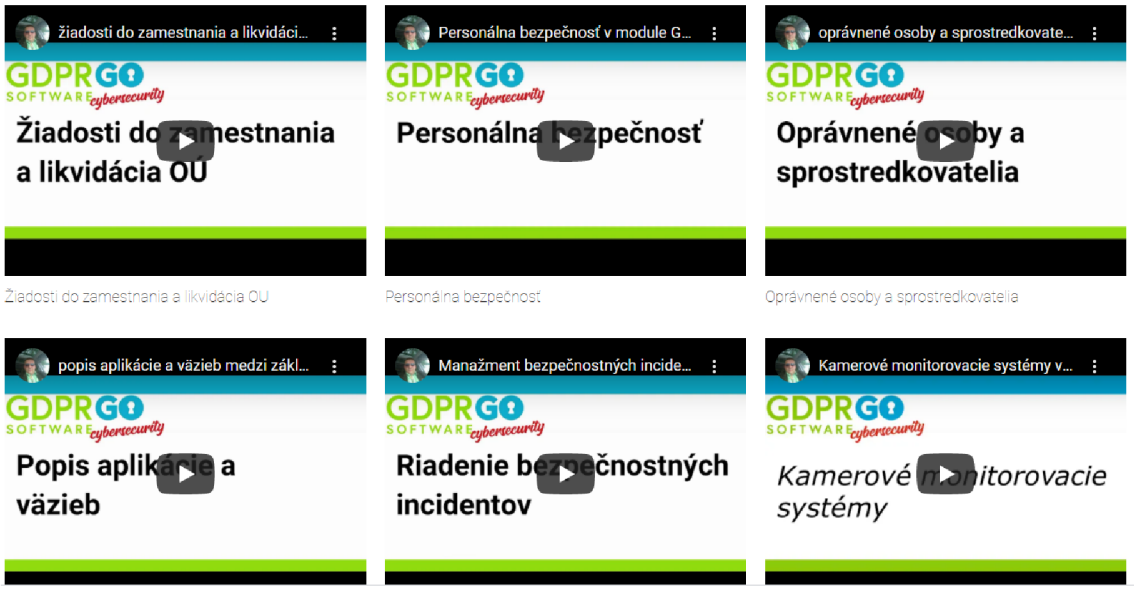
Nyní jednotlivé záložky popíšu detailněji.

Záložky FAQ zobrazuje nejčastější dotazy od zákazníků, které se týkají vyplňování polí v programu, s jakými poli je nejlepší začínat při vyplňování údajů a podobně. Dotazy se ale netýkají pouze naplnění programu, ale třeba i aktualizací v rámci programu, problémů s přístupem do databáze a tak dále.

Zákaznická podpora – z mého pohledu velmi důležitá záložka. Je zde nabídnuta zákazníkům telefonní linka, na kterou se zákazník může dovolat 8 hodin denně. Rovněž se zde nachází emailová adresa, na kterou zákazník může zaslat svůj dotaz. Další možností je spojení přes TeamViewer a přímo zákazníkovi ukazovat na jeho vlastním počítači jednotlivé postupy. Tato forma podpory se týká pomoci s obsluhou programu, informací o objednávkách a fakturaci a podobně.

Technická podpora se trochu liší od zákaznické podpory, a to v tom, že řeší problémy s instalacemi, databázemi a jinými technickými záležitostmi. Opět se na stránkách uvádí telefonní číslo a emailová adresa.

Video návody zveřejněné na webových stránkách jsou velmi pěkně zpracované. Každé video je natočeno na konkrétní problematiku, se kterou se může uživatel v programu setkat. Náhled na jednotlivá videa je zobrazen na obrázku níže.

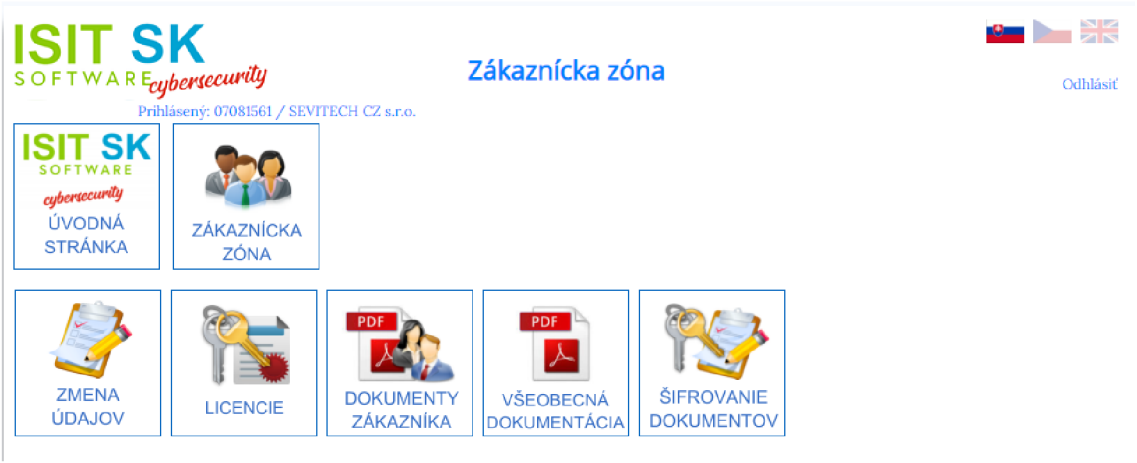


Obrázek 22: Náhled na webovou stránku s video návody
Zdroj: (8)

Systémové požadavky pro správnou funkčnost programu jsou dostupné i v záložce Technická podpora. Jedná se o hardwarové prvky, kterými musí zařízení disponovat, aby se dal program nainstalovat a dále používat.

Dále je na stránkách k dispozici záložka Vzdělávanie, kde se zákazník může podívat na aktuálně dostupná školení a e-learningové kurzy.

Za další součást helpdesku považuju i uživatelské rozhraní, které se nachází v páté záložce pod názvem Zákaznická zóna. Zde se může uživatel přihlásit a nahlédnout do svého účtu. Účet jako takový a ani jeho tvorba není však v záložce popsána. Níže je popis zákaznické zóny.



Obrázek 23: Náhled na menu Zákaznické zóny
Zdroj: (8)

V zákaznické zóně je celkem pět polí, které zákazníka zajímají. Prvním je Změna údajů, kde uživatel může nastavit své kontaktní údaje, fakturační údaje, a hlavně heslo pro aktivaci licencí. Dalším políčkem je správa licencí. V této části zákaznické zóny uživatel vidí svoje aktivní licence a do kdy jsou platné. Dále se zde nachází dvě políčka, která se týkají dokumentace. V prvním poli je dokumentace zákazníka. V této části jsou dokumenty, které může uživatel potřebovat při práci s programem. Jsou zde PDF soubory s jednoduchými návody. Ve všeobecné dokumentaci zákazník najde normy, vyhlášky a zákony, které jsou potřebné pro orientaci v jeho oblasti podnikání. Je zde dokumentace pro firmu, obec-město, školu a tak dále. Poslední záložkou je šifrování dokumentů, kde firma radí, jak zašifrovat svoje výstupy přímo v MS Office Word. Na závěr k zákaznické zóně bych chtěla zmínit odhlašovací tlačítko v pravé horní části stránky a rovněž možnost přepínat jazyk do slovenštiny, češtiny a angličtiny.
Helpdesk celkově je dle mého názoru vytvořen poměrně přehledně, všude jsou uvedeny kontakty, kam se může uživatel obrátit v případě dotazu. Jako problém vidím to, že člověk nenajde informace na jednom místě, ale jsou tak nějak všude na webových stránkách. Proto bych chtěla ucelit a zkompletovat informace do jednoho pole nazvaného Helpdesk.

2.3.2 Současná forma helpdesku v programu

V této kapitole bude popsána forma helpdesku, která funguje nyní v rámci nainstalované aplikace.

Jak bylo popsáno v kapitole 2.2.5 Program – funkcionalita a vzhled, existuje v úvodním okně tlačítko s otazníčkem, které zákazníka nasměruje k nápovědě a pomoci přímo v nainstalovaném programu. Tato nápověda je znázorněna na obrázku níže.

Obrázek 24: Pomoc k programu
Zdroj: Vlastní zpracování

Na obrázku výše je vidět celkem sedm možností pomoci, ze kterých si může zákazník vybrat.

Jsou zde dva PDF soubory s manuálem a popisem jednotlivých funkcí programu. Další PDF informuje o novinkách, které se můžou vyskytnou v novějších verzích programu.

Je zde zmíněná zákaznická a technická podpora, kterou může zákazník najít i na webových stránkách. Uveden je zde email a telefonní číslo.

Asi nejlepší a nejvyužívanější je zde možnost použití programu TeamViewer. Díky tomuto programu se může technik z firmy připojit na zákazníkův počítač a názorně mu vše ukázat

v programu anebo udělat i přímo nějaký zásah v programu za něj. Jediná nevýhoda pro méně technicky zdatné jedince je ta, že TeamViewer je program navíc a uživatel si ho musí sám stáhnout a nainstalovat, aby byla tato možnost pomoci proveditelná.

Poslední dvě tlačítka se zaměřují na instalace. První tlačítko se týká tiskových sestav a možnosti zobrazení chyby při načítání seznamu. V tomto případě je zde možnost stáhnout si opravný balíček tiskových sestav. V případě druhého tlačítka se jedná o instalaci MS Access databáze. Tuto databázi je nutné doinstalovat v případě vytvoření nového správce nebo organizace, přičemž se k danému správci či organizaci nevytvoří nové číselníky.

3 NÁVRH ŘEŠENÍ

Nedílnou součástí diplomové práce je návrh vlastního řešení. Na základě zhodnocení současného stavu společnosti, jakožto i jejího helpdesku, jsem se rozhodla vytvořit novou formu helpdesku. Tento nový návrh bude mít modernější nádech a bude vyřešen i lépe technicky. Na základě mého řešení by měl jít problém vyřídit přehledněji a v kratším čase, než tomu bylo doteď.

3.1 Důvod tvorby helpdesku

Z mého pohledu je současný helpdesk společnosti velice nemoderní a zastaralý. Odpovědi na otázky se poměrně špatně hledají, jelikož nekvalifikovaný uživatel, popřípadě úplný laik, se nemusí dobře orientovat v menu. Může zde například narazit na problém, že neví, co spadá pod zákaznickou podporu a co spadá pod technickou podporu.

Další problém vidím v tom, že když zákazník potřebuje zavolat a poradit s postupem, tak uvedená telefonní čísla jsou dostupná pouze od 8:00 do 16:00 hodin, a to může být pro některé zákazníky nevyhovující. Je zde sice uvedena emailová adresa, ale v případě napsání dotazu se může stát, že zpráva bude přehlédnuta nebo zapadne do spamu. Toto řešení je tedy z mého pohledu neúplné, nespolehlivé a poměrně zastaralé.

Dalším úskalím současného helpdesku je to, že informace jsou rozházené po celé webové stránce. Z mého pohledu je lepší všechny informace sjednotit a sepsat je na jedno místo.

Nevýhodou současného helpdesku je, že je dostupný v rámci nainstalovaného programu a pokud dojde k poruše nebo výpadku programu, nemá uživatel k helpdesku přístup.

Kvůli těmto zásadním nedostatkům jsem se rozhodla vytvořit nový, velice jednoduchý a intuitivní online helpdesk. Bude mít modernější vzhled a bude mít přesně popsaná tlačítka, aby se uživatel v helpdesku orientoval na první pohled. Moderní vzhled je dle mého názoru důležitou součástí dnešních helpdesků, protože uživatel se pěkným helpdeskem „proklikává“ snadněji. Dalším bonusem bude pro uživatele nově vytvořená Knihovna dotazů, kde budou uloženy všechny dříve položené otázky od uživatelů programu.

3.2 Nový návrh

Na vytvoření celkového návrhu jsem použila dva softwary. Jedním z nich byla Canva a druhým pak Lucidchart. Oba tyto softwary byly detailně popsány v teoretické části. V této kapitole je pouze uveden krátký popis pro připomenutí.

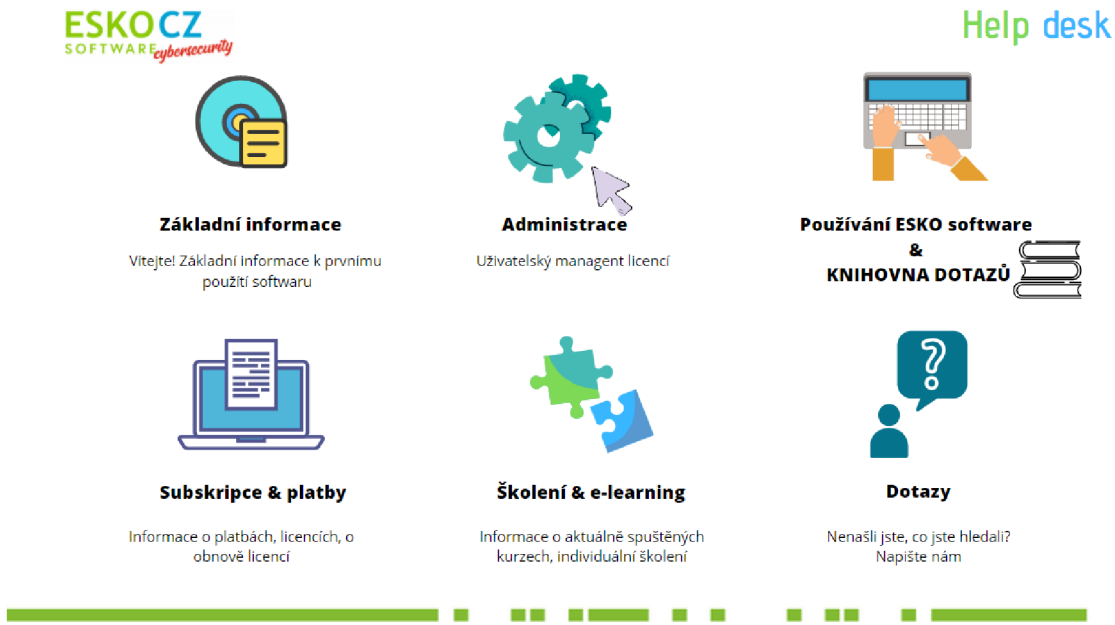
Návrh jsem rozdělila do dvou částí. První částí je helpdesk vytvořený pomocí webového rozhraní, ve kterém budou všechny informace, které se týkají softwaru. Helpdesk na webovém rozhraní je znázorněn jednoduše, a to pomocí několika dlaždicových tlačítek. Druhým návrhem je pak Knihovna dotazů přístupná z webu a vytvořená pomocí SQL databáze. Do této knihovny se uživatel dostane pouze po přihlášení do Zákaznické zóny.

3.2.1 Návrh helpdesku a knihovny dotazů

Canva je software, který se používá přímo na webovém rozhraní. Obecně se zabývá designem. Je možné zde nahrávat vlastní obrázky, které je možné upravovat anebo vytvářet obrázky nové z již uložených obrázků. Možné je použití filtrů a jiných upravovacích nástrojů. Obrázky se dají i popisovat textem.

Ve své práci použiji Canvu na návrh helpdesku – převážně z hlediska designu. Navrhnu, jak by mohla vypadat webová stránka, která bude zastupovat stránku helpdesku. Jednotlivé obrázky na stránce budou představovat tlačítka, která uživatele přesměrují na webovou stránku zaměřující se na dané téma. Toto téma bude znázorněno názvem tlačítka a velmi krátkým popisem pod tlačítkem, aby uživatel věděl, co po rozkliknutí na webové stránce nalezne za informace.

Na obrázku níže je vidět návrh nového helpdesku. Tento helpdesk bude přístupný z hlavního menu panelu na webových stránkách společnosti.



Obrázek 25: Náhled na menu helpdesku
Zdroj: Vlastní zpracování

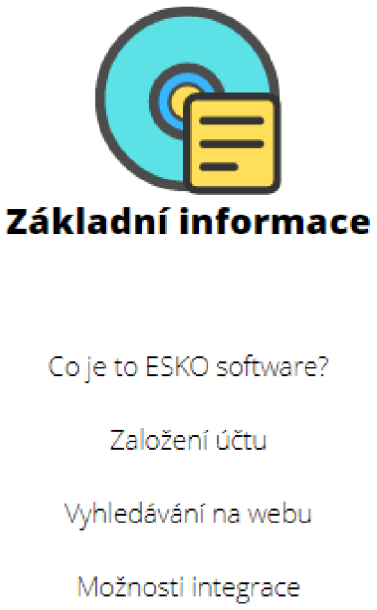
V novém návrhu helpdesku je vidět šest klikacích polí. Každé pole má svůj název a krátký popisek. To by mělo usnadnit uživateli orientaci v helpdesku na první pohled. Jedná se o těchto šest tlačítek:

- Základní informace
- Administrace
- Používání ESKO software & KNIHOVNA DOTAZŮ
- Subskripce a platby
- Školení a e-learning
- Dotazy

V rámci helpdesku bude zaveden i nový ticketovací systém. Ten bude primárně použit v políčku Dotazy, ale využije se i v políčku Školení a e-learning. Ticketovací systém bude blíže popsán v kapitole 3.2.7 Dotazy. Druhá část návrhu helpdesku se týká Knihovny dotazů, ta bude popsána v kapitole 3.2.4 Používání ESKO software & KNIHOVNA DOTAZŮ.

Nejprve popíšu jednotlivá tlačítka, a co v nich uživatel najde, a v rámci tlačítka Dotazy popíšu nový ticketovací systém.

3.2.2 Základní informace



Obrázek 26: Tlačítko Základní informace
Zdroj: Vlastní zpracování

Po kliknutí na tlačítko Základní informace se uživateli objeví další menu, kde se rozvětvují další možné dotazy.

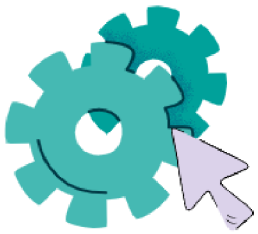
V prvním řádku v menu Základní informace je popsání, co to obecně ESKO software je, na co se používá a proč by ho zákazník mohl potřebovat. Na základě těchto informací se může zákazník rozhodnout, zda by si chtěl založit účet.

Po kliknutí na Založení účtu uvidí zákazník informace, které souvisí se zakládáním nového účtu. Obsahem budou i výhody, proč je dobré založit si účet na stránkách. Mezi tyto výhody patří například: informace o platbách na jednom místě, management zakoupených licencí, přístup do Knihovny dotazů a tak dále.

V záložce Vyhledávání na webu bude jednoduše vysvětlen princip vyhledávání v rámci webového portálu.

V Možnosti integrace zákazník uvidí možnosti propojení ESKO programu s jinými programy. Jedná se například o integraci se systémem SAP.

3.2.3 Administrace



Administrace

Popsání uživatelského rozhraní

Přidání/odebrání licencí

Přidání/odebrání správců účtu

Možnost reportů, exportů informací

Obrázek 27: Tlačítko administrace
Zdroj: Vlastní zpracování

Po kliknutí na tlačítko Administrace se zákazníkovi zobrazí uživatelské rozhraní, které je nyní dostupné v záložce Zákaznická zóna.

Budou zde popsány všechny záložky, které uživatelské rozhraní nabízí, jako je například: správa licencí, správa faktur a plateb v rámci softwaru.

Bude zde zobrazeno, jak administrátor může přidávat další členy týmu pro správu licencí, budou popsána jednotlivá práva, která zaměstnanec může v tomto rozhraní mít.

Na závěr budou vysvětleny možnosti reportů, kterých je program schopný v rámci správy licencí. Všechny informace dostupné v uživatelském rozhraní budou možné vyexportovat do MS Excel.

3.2.4 Používání ESKO software & KNIHOVNA DOTAZŮ

Obrázek 28: Tlačítko Používání ESKO software
Zdroj: Vlastní zpracování

Po kliknutí na tlačítko Používání ESKO software & KNIHOVNA DOTAZŮ bude uživatel přesměrován do menu, kde si může zvolit, co přesně mu není na používání jasné. Budou zde na výběr video návody, vzorové ukázky dokumentace, podle kterých lze vytvořit vlastní dokumentaci, a v poslední možnosti bude dostupná Knihovna dotazů.

Video návody bych ráda ponechala ve stavu, ve kterém již byly vytvořeny, ale navrhla bych nový design stránky, tak aby odpovídal celkovému designu helpdesku.

Do tohoto menu bude zahrnuta i zmiňovaná Knihovna dotazů, která bude fungovat jako databáze všech dříve položených dotazů. Vždy když se zákazník zeptá na nějaký dotaz pomocí formuláře v sekci Dotazy, a dotaz by mohl být zajímavý i pro ostatní uživatele softwaru, bude zveřejněn do Knihovny dotazů. Do Knihovny dotazů bude mít přístup pouze přihlášený zákazník, což by mělo být motivací pro založení účtu. Knihovna se bude nacházet na webu a bude propojená s SQL databází, kde se budou jednotlivé dotazy uchovávat.

Níže uvidíte příklad toho, jak by knihovna mohla vypadat.

Obrázek 29: Knihovna dotazů
Zdroj: Vlastní zpracování

Webové rozhraní bude obsahovat vyhledávací pole (vpravo nahoře), do kterého zákazník zadá klíčové slovo nebo slova. V našem případě jsem pro uvedení příkladu zvolila klíčové slovo „aktualizace“. Podle tohoto klíčového slova se zobrazí související dotazy, které již napsal někdo dříve. Pro příklad jsou zde tři dotazy:

- Jak stáhnu aktualizaci softwaru?
- Je potřeba program aktualizovat?
- Aktualizovala se mi verze operačního systému Windows a program teď nefunguje.

Tento seznam dotazů obsahujících klíčové slovo „aktualizace“ je znázorněn na levé straně obrázku. Po kliknutí myší na otázku, která odpovídá dotazu zákazníka, se objeví náhled otázky v pravé části stránky. V mém uvedeném příkladu zákazníka zajímala odpověď na první otázku: „Jak stáhnu aktualizaci softwaru?“. V této fázi po kliknutí na dotaz zákazník neztratí vyhledávání dotazů a stále bude vidět seznam dalších dotazů.

Náhled otevřené otázky bude zobrazen v pravé části obrazovky, jak je znázorněno na obrázku. Náhled bude obsahovat přesné znění položeného dotazu, datum, kdy byl dotaz vytvořen, kdo na dotaz odpovídal (to je důležité pro interní procesy ve firmě – aby zaměstnanci na helpdesku měli větší přehled), zda dotaz spadá k modulu GDPR nebo KBO

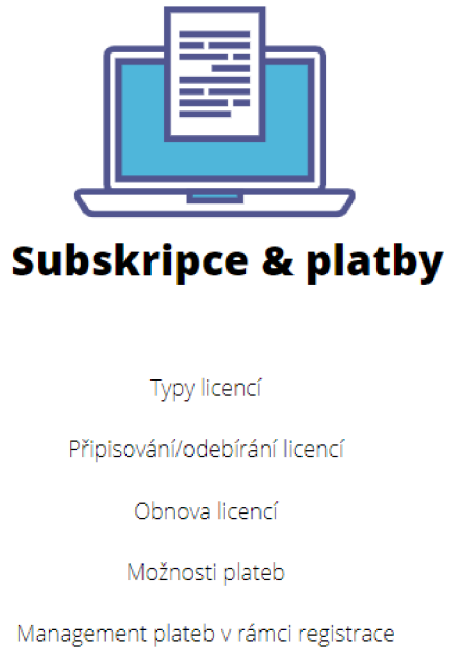
a konečně odpověď na dotaz. V případě, že by opravdu nebylo uživateli něco jasné je zde i možnost přidat komentář a popřípadě se v rámci této otázky na něco doptat.

Pokud zákazník nenajde odpověď na své zadané klíčové slovo, je dole na levé straně stránky možnost vytvořit nový dotaz. Tento nový dotaz bude vytvořen pomocí formuláře v sekci Dotazy, kam bude zákazník přesměrován.

Zaměstnanec helpdesku uvidí rozhraní maličko jinak. Bude zde ještě skryté pole, do kterého zaměstnanec vyplní na základě, kterého ticketu se dotaz zpracovával, aby byl později dohledatelný.

Tato Knihovna dotazů nebude přístupná přímo v programu, a to z toho důvodu, že kdyby se něco stalo s programem a nebyl v daný okamžik funkční, zákazník by neměl možnost si sám pomoci, protože by se ke Knihovně dotazů nedostal. Z toho důvodu je lepší mít knihovnu online s přístupem na webové stránce. V programu bude pouze uveden odkaz na webovou stránku, kde se Knihovna dotazů nachází.

3.2.5 Subskripce a platby



Obrázek 30: Tlačítko Subskripce & platby
Zdroj: Vlastní zpracování

Po kliknutí na tlačítko Subskripce a platby bude uživatel přesměrován do menu, ve kterém bude vysvětleno, jaké existují typy licencí v rámci softwaru a jak funguje jejich obnovování a připisování.

Budou zde vystaveny platební údaje a možnosti provedení plateb jako například: platební kartou online, převodem a podobně.

Popsán bude i management plateb, pokud by si uživatel založil účet. Bude znázorněna jednoduchost používání účtu a přesměrování do sekce Základní informace – Založení účtu.

3.2.6 Školení a e-learning

Obrázek 31: Tlačítko Školení & e-learning
Zdroj: Vlastní zpracování

Po kliknutí na toto tlačítko bude uživatel přesměrován do menu, kde bude popsán průběh školení a jednotlivých e-learningových kurzů. Bude možné otevřít rozvrh školení i dostupných e-learningových kurzů. A přímo v této sekci bude možnost i zapsání se do kurzu.

V menu je i Možnost individuálního školení. Po zvolení této možnosti se na stránce zobrazí formulář, ve kterém bude nutné vyplnit jméno, příjmení, emailovou adresu, platební metodu, počet účastníků a datum a hodinu požadovaného školení. Na základě tohoto formuláře bude ve firemním systému vytvořen ticket, který si bude moci převzít daný školitel ve firmě.

3.2.7 Dotazy

Po kliknutí na tlačítko Dotazy bude zákazník přesměrován na stránku, kde bude možné vyplnit formulář se specifickým dotazem.

Formulář bude obsahovat následující pole: jméno, příjmení, emailová adresa, typ problému, předmět, textové pole a možnost přidání souboru. Typ problému bude ve formě scrollbaru, kde bude na výběr pět hlavních problémů, se kterými se může zákazník setkat.

Bude to například:

- problém s instalací,
- problém s licencí,
- problém s ovládáním programu,
- problém s platbou
- problém s uživatelským účtem.

Ve výběru bude i možnost „Jiný problém“.

Do textového pole bude mít zákazník možnost co nejlépe popsat svůj problém a do místa přidání souboru bude moci poskytnout podpoře i snímek obrazovky zachycující daný problém.

Sekce dotazů a vyplňování formuláře bude propojena s SQL databází, kde se nachází všechny již dříve položené dotazy. Všechny nové dotazy budou v databázi porovnávány s předešlými dotazy, aby se zamezilo duplicitě. Pro lepší vysvětlení této problematiky jsem vytvořila vývojový diagram, který najdete v podkapitole 3.3.2 Workflow.

Na stránce bude i odkaz na Knihovnu dotazů, kde si bude moc uživatel se zákaznickým účtem najít předešlé dotazy.

3.3 Ticketování

Na základě vyplněného formuláře v sekci Dotazy nebo v sekci Školení a e-learning se budou tvořit tickety, jak už bylo řečeno výše.

Tyto formuláře budou automaticky převáděny na tickety v interním helpdesku. A po vyřešení ticketu a jeho zavření bude odpověď automaticky odeslána dotazovanému.

Systém ticketování by si mohla i jednoduše vytvořit firma sama, avšak stálo by to dodatečné náklady v podobě pracovní síly, údržby systému a podobně. Proto jsem se rozhodla udělat průzkum trhu a najít firmu, která poskytuje software, který by byl pro tyto potřeby nejlepší.

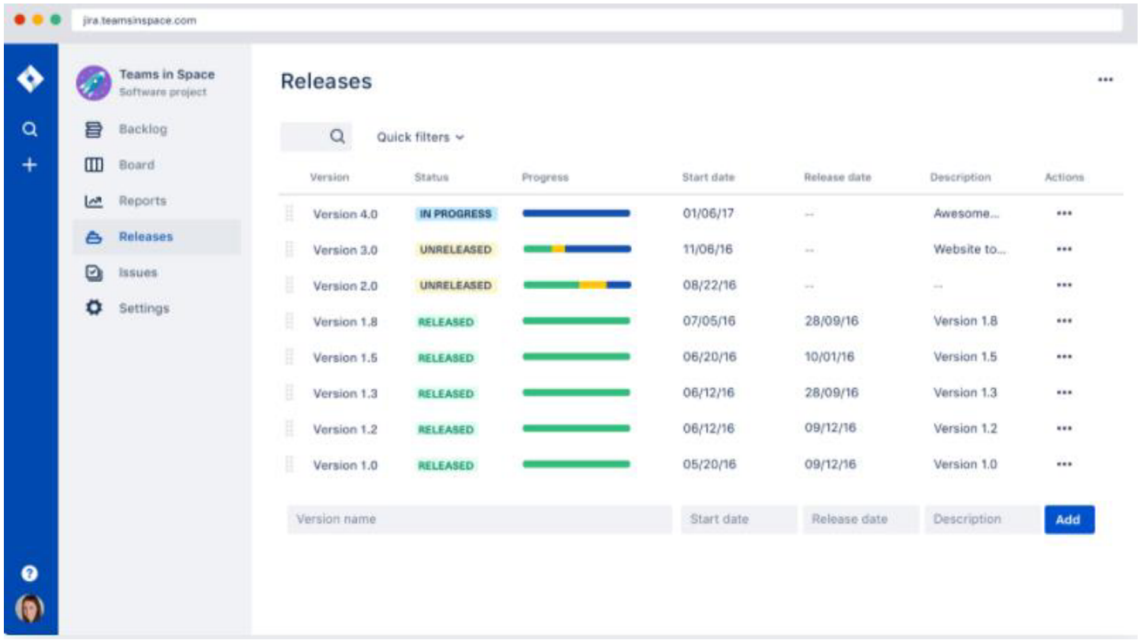
Po průzkumu trhu jsem se tedy rozhodla zvolit externí software. Jmenuje se JIRA Software a ten je vyvíjen firmou Atlassian. JIRA nabízí spoustu softwarů na ticketovacím principu, které se liší velikostí týmů nebo přesnou funkcí, kterou má software zastávat. V mém případě jsem hledala software, který by firmě umožňoval funkci helpdesku, a tedy hlavně spolupráci mezi zaměstnanci. Mou vizí bylo, aby zaměstnanci mohli navzájem vidět, o který úkol se kdo stará, který úkol ještě není obsazen a který úkol už je vyřešen. Zároveň aby spolu mohli zaměstnanci v daném softwaru komunikovat. Všechny tyto možnosti nabízí software JIRA – IT Service Management.

3.3.1 JIRA a IT Service Management

Software IT Service management funguje na ITSM řešení. ITSM řešení bylo již popsáno výše v teorii, proto ho již nebudu popisovat znovu.

Součástí tohoto řešení je i to, že celé funguje společně s JIRA platformou. Tento software je koncipován tak, že pomáhá lépe plánovat úkoly – dají se zde tvořit nové úkoly a dále se potom zpracovávají tak, že se může danému úkolu přiřadit určitá priorita. Součástí plánování úkolů je i komunikace mezi jednotlivými zaměstnanci v podobě komentářů. Úkolům je přiřazeno i datum, kdy by měly být splněny. Konečnou fází jsou reporty, které lze ze systému posléze stahovat.

Níže na obrázku je vidět, jak prostředí vypadá a na první pohled je patrné, jak JIRA funguje.



Obrázek 32: Náhled na uživatelské rozhraní softwaru JIRA
Zdroj: (29)

Přímo v systému JIRA lze navrhnout jakákoliv potřebná workflow v týmu, a to pro jakýkoliv proces. Každý proces se ale může trochu lišit. Jednotlivé procesy popíšu v další podkapitole.

Rovněž pro každý úkol nebo proces je vhodné zvolit jinou zkratku pro odlišení úkolů. Například problém s licencí se bude značit jako LIC, problém s instalací se bude značit jako IT. Tabulka s jednotlivými zkratkami je zobrazena níže v textu – Tabulka 3.

JIRA software je zdarma pro deset uživatelů. To by v mém případě mělo pro začátek postačovat.

V případě rozšíření používání bych volila licenci Standard, která je pro 1-100 uživatelů. Stojí sedm dolarů na měsíc pro jednoho uživatele, tedy 84 USD ročně. Cenu jsem přepočítala na české koruny dle aktuálně platného kurzu 1USD ≐ 21,42 Kč (30). Po přepočítání na české koruny mi vyšla částka 1 800 Kč za jednoho uživatele. Toto řešení jsou poměrně levné, protože funguje na cloudu. Pro lepší znázornění jsem níže vytvořila tabulku.

Tabulka 1: Přehled nacenění JIRA software licencí

JIRA software licence	Počet uživatelů	Cena
Free	Max 10	0
Standard	1–100	7 USD/uživatel

Zdroj: Vlastní zpracování

Software IT Service Management pomáhá řídit a urychlovat práci mezi podporou, vývojáři a dalšími členy týmu. Existují tu funkce jako on-call, alert management a major incident management s workflow, která znázorňuje pořadí úkolů mezi členy týmu. Existuje zde také licence zdarma, která je ale jen do tří uživatelů. V případě, že by firma potřebovala na helpdesk více než tři lidi, je zde licence Standard, která stojí 20 USD měsíčně pro jednoho uživatele. Celkem by tedy tato licence vyšla na 240 USD ročně za jednoho člověka, tedy asi 5 280 Kč. Převod měn jsem provedla dle aktuálně platného kurzu 1USD ≐ 21,42 Kč (30).

Tabulka 2: Rozepsání cen JIRA software licencí dle počtu pracovníků ve firmě

JIRA IT service management licence	Počet uživatelů	Cena měsíčně v USD	Cena ročně v USD	Cena ročně v CZK
Free	Max 3	0 USD	0 USD	0 CZK
Standard	1	20 USD	240 USD	5 141 CK
	10	200 USD	2 400 USD	51 408 CZK

Zdroj: Vlastní zpracování

Na základě velikosti firmy ISIT Slovakia, si myslím, že by naprosto stačila Free verze v obou výše zmíněných případech. Firma po implementaci nebude potřebovat více než tři zaměstnance helpdesku.

Po delší době používání si ale myslím, že tři uživatelé jsou málo, a proto jsem vypočítala i cenu pro deset uživatelů. Pro deset uživatelů kvůli tomu, že do JIRY budou mít přístup i ostatní zaměstnanci. Cena vyšla na 2 400 USD ročně.

Na základě provedení této analýzy si myslím, že firmě naprosto postačí základní verze JIRA software a pouze v případě rozšiřování firmy bych uvažovala o přikoupení doplňku IT Service Management pro deset uživatelů.

Důležitou součástí ticketů je přiřazení stupně priority řešení a rozhodně musí být viditelné datum vytvoření ticketu. Na základě priority a data vytvoření ticketu bude stanovené nové datum, do kdy musí být ticket vyřešen, aby to bylo vyhovující pro zákazníka a zároveň proveditelné pro zaměstnance. Priorita by se značila čísly od tří do jedné s tím, že P3 je nejnižší možná priorita a P1 je nejvyšší možná priorita.

Jak jsem již výše napsala, může se jednat například o tyto situace, které bude potřeba řešit:

- problém s instalací,
- problém s licencí,
- problém s ovládáním programu,
- problém s platbou,
- problém s uživatelským účtem.

Na základě těchto situací je níže uvedena tabulka 3, ve které je každému problému přiřazena zkratka – tuto zkratku budu dále nazývat projekt.

Dále bude jen k uvedení příkladu uvedena priorita projektu, datum vytvoření a datum možného ukončení.

Tabulka 3: Možné uživatelské problémy a jejich rozdělení do zkratek

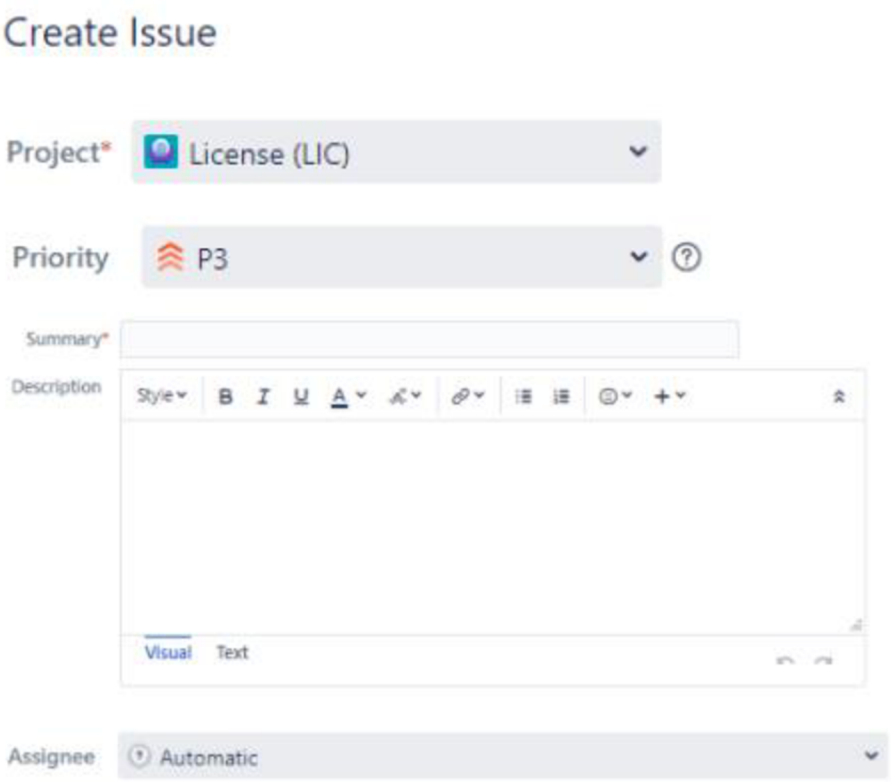
Situace	Zkratka	Priorita	Datum vytvoření ticketu	Datum, kdy by měl být ticket dokončen
Problém s instalací	INS	P2	1.1.2021	6.1.2021
Problém s licencí	LIC	P1	1.1.2021	4.1.2021
Problém s ovládáním programu	PRO	P3	1.1.2021	8.1.2021
Problém s platbou	PAY	P1	1.1.2021	4.1.2021
Problém s uživatelským účtem	ACC	P2	1.1.2021	6.1.2021
Jiný problém	OTH	P2	1.1.2021	6.1.2021

Zdroj: Vlastní zpracování

V tabulce jsem odhadla dobu dokončení ticketů dle nastavených priorit.

Prioritní úkoly – P1 by měly být dokončeny nejdříve, a to v průběhu tří dní. Středně prioritní úkoly v průběhu pěti dní a nejméně prioritní úkoly do jednoho týdne. Priority jsou čistě orientační, jak pro zaměstnance a jejich manažera, tak i pro zákazníka.

Pro lepší znázornění jsem vytvořila návrh, jak bude ticket při tvorbě vypadat. Do ticketu se vlastně převedou informace z formuláře, který vytvořil zákazník.



Obrázek 33: Vytvoření ticketu
Zdroj: (29)

V první řadě bude uveden projekt, kterým je ticket charakterizován. Následně bude uvedena priorita a krátký nadpis s následným bližším popisem problému. Na konci je ještě políčko Assignee, které znázorňuje, do které fronty ticket spadne. Frontou označuji tickety daného projektu, které spadají pod nějakého zaměstnance. Tento zaměstnanec bude mít seznam například LIC projektů. A tomuto seznamu se říká fronta.

3.3.2 Workflow

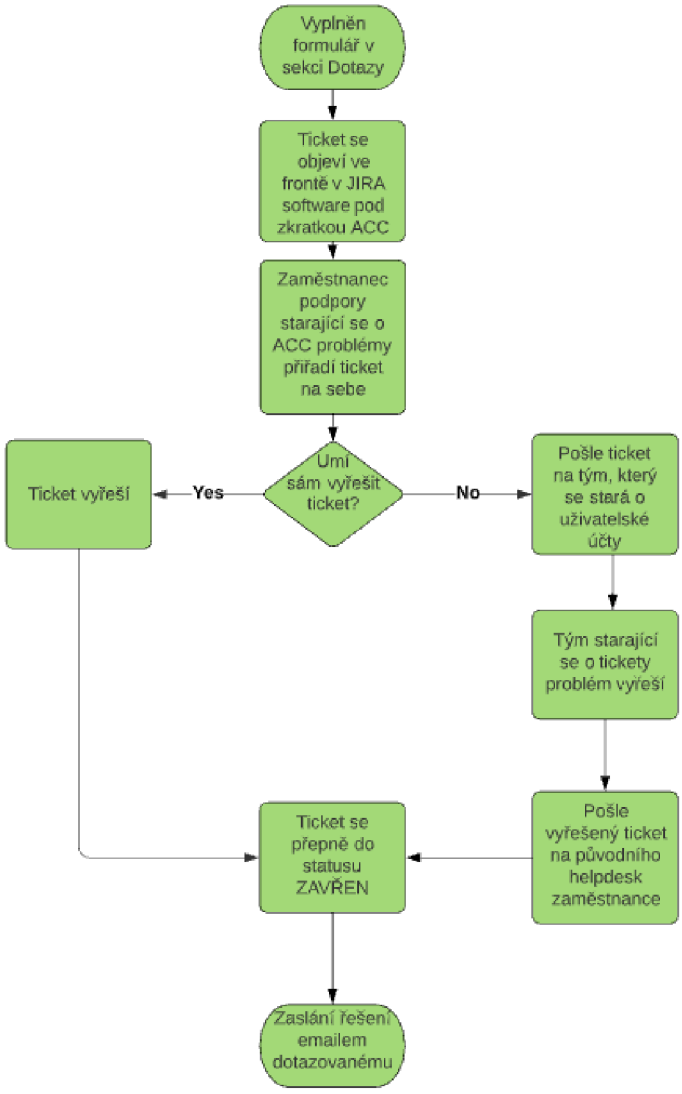
V rámci ticketů je velice důležitá workflow. Ta se bude lišit v jednotlivých projektech s jednotlivými úkoly.

Všechny workflow grafy jsou vytvořené pomocí softwaru Lucidchart, který byl popsán v rámci teoretické části práce.

Na základě požadavků z webového formuláře v sekci Dotazy bude vytvořen ticket. Co vše tento formulář obsahuje, je popsáno v kapitole 3.2.7 Dotazy.

Ticket bude mít hlavičku, která se bude skládat z nadpisu – obecně něco jako předmět emailu a dále typu problému. Tyto dvě informace budou nejdůležitější pro sestavení workflow. Typ problému bude na webové stránce zobrazen pomocí scrollbaru, kde si zákazník vybere, do jakého typu problému jeho požadavek spadá. V kapitole Dotazy jsem sepsala pět základních typů problémů, se kterými se může uživatel setkat. Jedná se o: problém s instalací, problém s licencí, problém s ovládáním programu, problém s platbou a problém s uživatelským účtem. Pokud si nevybere ani jednu z těchto pěti možností, bude zde na výběr možnost „Jiný problém“.

Nyní znázorním workflow dvou problémů. Prvním je „Problém s uživatelským účtem“ se zkratkou ACC – account.



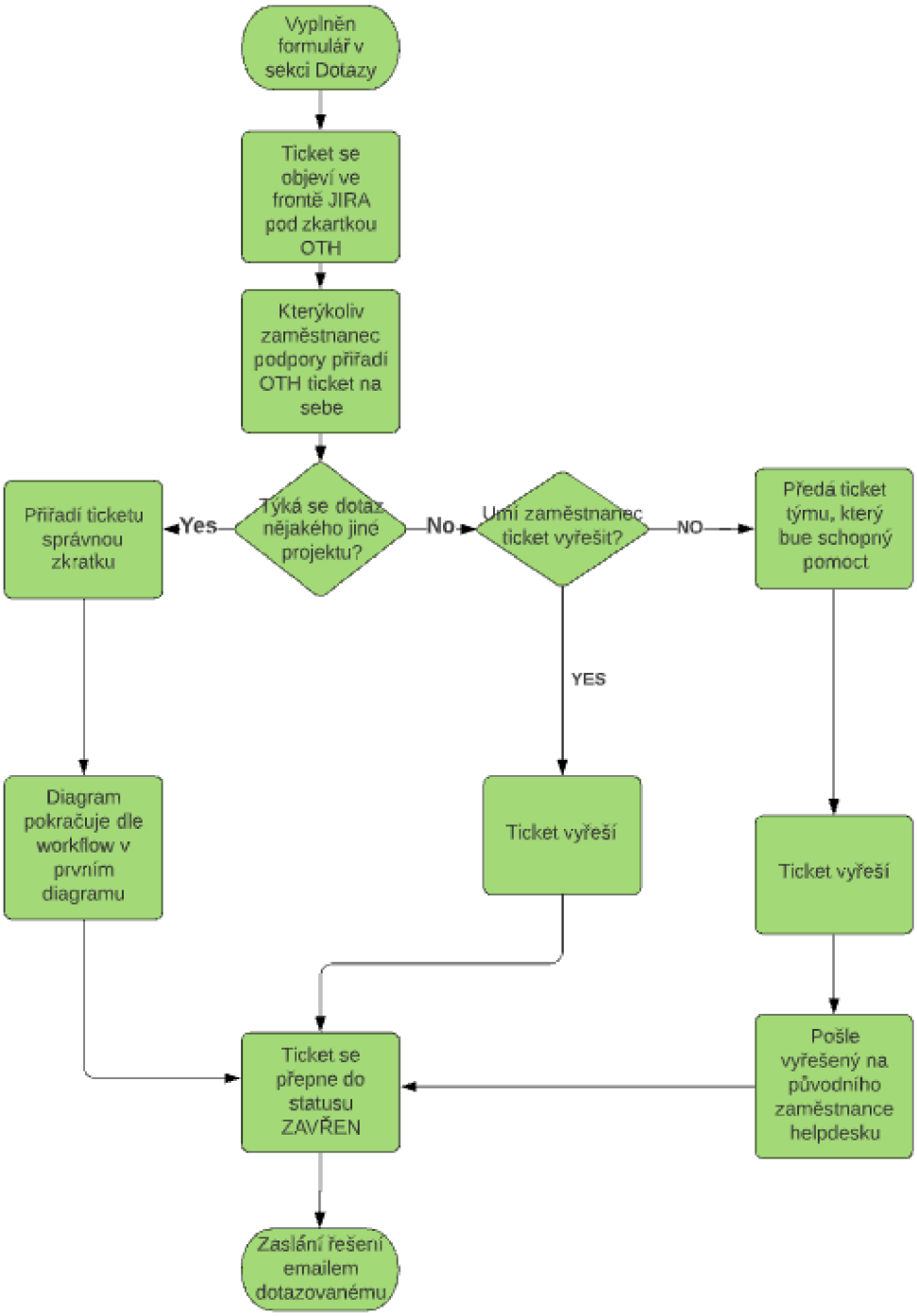
Obrázek 34: Workflow řešení: Problém s uživatelským účtem
Zdroj: Vlastní zpracování

V sekci Dotazy bude vyplněn formulář založení nového dotazu. Na základě vyplnění tohoto formuláře se vytvoří v JIRA softwaru ticket pod novým označením – v tomto případě pod zkratkou ACC. Zaměstnanec, který se bude specializovat na oblast problematiky týkající se uživatelského účtu, si vezme tento ticket na starost. To znamená, že se bude starat o jeho vyřešení. A to znamená, že spadne do fronty řešící problémy s označením ACC.

Dále je ve workflow rozhodující blok, který zajišťuje to, že zaměstnanec podpory nemusí vědět vše o uživatelských účtech. Pokud neví, jak na dotaz správně odpovědět, obrátí se na tým, který přímo vyvíjí uživatelské účty. Tento tým si vezme ticket na starost. Bude tedy ve frontě vývojářské. Vývojáři buď poradí zaměstnanci helpdesku, co dělat dál anebo popřípadě za něj problém vyřeší a pošlou mu vyřešený ticket zpět. Druhá možnost rozhodovacího bloku je taková, že zaměstnanec helpdesku umí problém vyřešit hned sám.

Na závěr se ticketu změní status na zavřený (tím pádem vyřešený) a odpověď se pošle zákazníkovi. Buď formou emailu nebo se mu může zobrazit v historii jeho položených dotazů přímo na jeho zákaznickém účtu.

Druhý příklad workflow, který chci znázornit se týká možnosti „Jiný problém“. Pro tento problém byla vytvořena zkratka OTH – other.



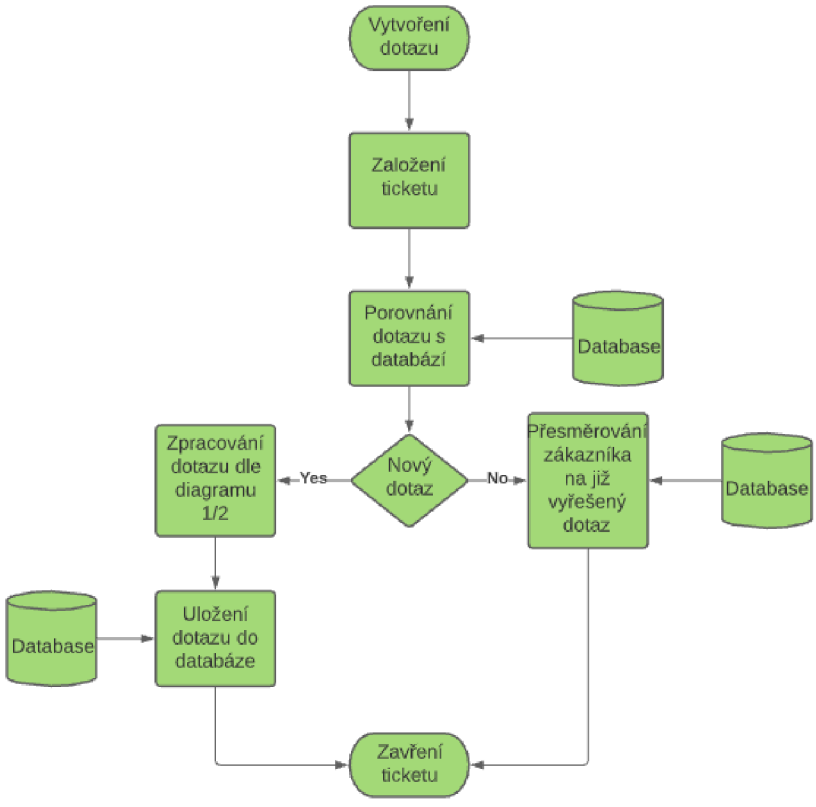
Obrázek 35: Workflow řešení: Jiný problém
Zdroj: Vlastní zpracování

V sekci Dotazy bude vyplněn formulář založení nového dotazu. Na základě vyplnění tohoto formuláře se vytvoří v JIRA softwaru ticket pod novým označením – v tomto případě pod zkratkou OTH. Jiný problém, který je označen zkratkou OTH na sebe může vzít kterýkoliv ze zaměstnanců helpdesku.

Dále je ve workflow rozhodující blok, který zajišťuje to, že zákazník mohl chybně vyplnit formulář a chybně tak zařadit ticket do projektu. Pokud zákazník špatně zařadil ticket opraví tento problém zaměstnanec podpory.

Po přidání ticketu ke správnému projektu se ticket řeší stejným způsobem, který byl popsán u prvního diagramu. V případě, že se opravdu jedná o jiný problém řeší zaměstnanec helpdesku ticket podobným způsobem. Buď ví, jak problém vyřešit nebo se obrátí na tým, který se se danou problematikou zabývá. Workflow končí zavřením ticketu a posláním odpovědi zákazníkovi.

Jak jsem popsala výše – konkrétně v kapitole 3.2.4 Používání ESKO software & KNIHOVNA DOTAZŮ bude firma svým zákazníkům poskytovat jako součást podpory i Knihovnu dotazů. Tato knihovna bude fungovat na principu SQL databáze, kde budou uloženy dotazy. Níže jsem vytvořila vývojový diagram, který znázorňuje workflow pro zamezení duplicit v knihovně.



Obrázek 36: Workflow zamezující duplicit v Knihovně dotazů
Zdroj: Vlastní zpracování

V sekci Dotazy vytvoří zákazník pomocí formuláře nový dotaz. Tento dotaz bude rovnou založen i v systému JIRA pomocí ticketu.

Aby se zamezilo duplicitám v knihovně bude tento dotaz porovnán s databází již existujících dotazů. V případě, že dotaz bude stejný jako některý z databáze, bude ticket automaticky zavřen a zákazník bude přesměrován do knihovny na již existující dotaz. Pokud však bude dotaz nový, bude zpracováván podle výše znázorněných diagramů, ale ve finální fázi se ještě uloží do SQL databáze všech položených dotazů – do knihovny. Po uložení nového dotazu do databáze se ticket zavře.

3.4 Postup při implementaci helpdesku

V této části diplomové práce se zaměřím na postup při implementaci vytvořeného helpdesku. Rovněž se zmíním o rizicích spojených s implementací.

3.4.1 Kroky implementace

Implementace jako taková nebude ve firmě příliš složitá, protože firma nebude potřebovat importovat žádná data do nového helpdesku, a to právě kvůli způsobu, jakým je helpdesk vytvořen. Jelikož je helpdesk z pohledu vnímání zákazníka webová stránka, není potřeba žádná náročnější implementace.

Avšak v případě Knihovny dotazů bude implementace poměrně náročnější, protože je potřeba spojení oné webové aplikace znázorňující helpdesk a SQL databáze. Toto spojení se vytvoří jednoduše, a to pomocí PHP kódu přímo v těle webové stránky, kde se bude nacházet helpdesk.

Následně bude nutná implementace ticketovacího systému JIRA. Nejsložitější na celé implementaci jsou data, která jsou potřebná zmigrovat do nového systému. Jelikož ale firma předtím nepracovala s žádným podobným systémem, nebude potřeba žádná data migrovat. Dále bude potřeba JIRA software nastavit přesně podle potřeb firmy, a to konkrétně nastavit jednotlivé fronty, do kterých se budou tickety třídit, nastavit jednotlivé projekty a týmy, které se budou o tickety starat, prioritizaci ticketů a podobně. Tato část je z pohledu implementace asi nejnáročnější, jak z pohledu provedené práce, tak z časového hlediska. Níže uvedu bodový seznam činností, které se budou muset provést při implementování JIRA softwaru:

- Vytvoření jednotlivých front a projektů (LIC, INS, PRO, …)
- Vytvoření jednotlivých týmů zodpovědných za tickety
- Pozvání daných zaměstnanců do softwaru
- Nastavení prioritizace ticketů
- Nastavení odhadovaného času dokončení ticketu
- Nastavení vpisovacích polí v rámci ticketu
- Propojení JIRA softwaru s webovou stránkou – sekce Dotazy a dotazovací formulář

K celé implementaci je potřeba průběžně vytvářet projektovou dokumentaci. Tuto projektovou dokumentaci bude mít na starost projektový manažer. Zde bude možnost využití Ganttova diagramu, který má výhodu znázornění kapacity lidí, požadavky na kooperace a podobně. Ganttův diagram je možné vytvořit v softwaru Lucidchart. V dokumentaci nesmí chybět záznamy z porad, sledování výkonů zaměstnanců, ukončení projektu, následná fakturace a celkové vyhodnocení.

3.4.2 Rizika implementace

V této kapitole jsou zmíněna nejzásadnější rizika, která by mohla ovlivnit následné fungování helpdesku.

- Nedostupné pracovní síly
- Nevyhovující hardware
- Překročení rozpočtu
- Špatný návrh helpdesku
- Špatně naprogramovaný helpdesk
- Nepřehledný design
- Technické problémy
- Špatná komunikace mezi jednotlivými týmy
- Nedodržení fází implementace
- Odlišný výsledek od očekávání

3.5 Celkové finanční zhodnocení

Nejprve bych chtěla pomocí časové analýzy PERT znázornit, jak dlouho bude asi trvat vytvoření a dokončení celého projektu – čili návrh a implementace nového helpdesku ve firmě.

Do analýzy PERT jsem zvolila zahrnutí následujících činností:

1) Schválení projektu
2) Výběr programátorského a designového týmu
3) Výběr projektového manažera
4) Stanovení cílů a funkcí
5) Návrh vlastností helpdesku
6) Návrh vzhledu helpdesku
7) Schválení návrhu
8) Vizualizace
9) Vznik zkušebních verzí
10) Testování funkčnosti
11) Výběr finální verze
12) Dodatečné testování
13) Tvorba knihovny s dotazy
14) Zabudování knihovny na webový helpdesk
15) Testování funkčnosti knihovny
16) Seznámení manažerů s výsledky
17) Implementace helpdesku
18) Proškolení uživatelů
19) Cenová kalkulace
20) Dokončení projektu

3.5.1 Harmonogram činností – analýza PERT

Údaje o postupnosti činností projektu				Trvání - pracovní dny				Termíny zahájení a ukončení činností				Rezerva
Označení činnosti	Popis činnosti	i	j	a	m	b	t(ij)	ZM	KM	ZP	KP	RC
A	schválení projektu	-	B	1	2	3	2,0	0	2	0	2	0
B	výběr programátorského a designérského týmu	A	C	1	2	3	2,0	2	4	2	4	0
C	výběr projektového manažera	B	D	2	4	6	4,0	4	8	4	8	0
D	stanovení cílů a funkcí	C	E,F	2	3	4	3,0	8	11	8	11	0
E	návrh vlastností helpdesku	D	G	5	7	10	7,2	11	18,2	11,0	18,2	0
F	návrh vzhledu helpdesku	D	G	4	6	11	6,50	11	17,5	11,7	18,2	0,7
G	schválení návrhu	E,F	H,I	1	2	3	2,0	18,2	20,2	18,2	20,2	0
H	vizualizace	G	J	3	5	7	5,0	20,2	25,2	20,2	25,2	0
I	vznik zkušebních verzí	G	J	2	4	6	4,0	20,2	24,2	21,2	25,2	1
J	testování funkčnosti	H,I	K	5	10	15	10,0	25,2	35,2	25,2	35,2	0
K	výběr finální verze	J	L	3	6	9	6,0	35,2	41,2	35,2	41,2	0
L	dodatečné testování	K	M	4	8	12	8,0	41,2	49,2	41,2	49,2	0
M	tvorba knihovny s dotazy	L	N,O	10	15	20	15,0	49,2	64,2	49,2	64,2	0
N	zabudování knihovny na webový helpdesk	M	P	3	6	9	6,0	64,2	70,2	68,2	74,2	4
O	testování funkčnosti knihovny	M	P	5	10	15	10,0	64,2	74,2	64,2	74,2	0
P	seznámení manažerů s výsledky	N,O	Q	1	2	3	2,0	74,2	76,2	74,2	76,2	0
Q	implementace helpdesku	P	R	2	3	4	3,0	76,2	79,2	76,2	79,2	0
R	proškolení uživatelů	Q	S	10	15	20	15,0	79,2	94,2	79,2	94,2	0
S	cenová kalkulace	R	T	2	4	6	4,0	94,2	98,2	94,2	98,2	0
T	dokončení projektu	T	-	1	2	3	2,0	98,2	100,2	98,2	100,2	0

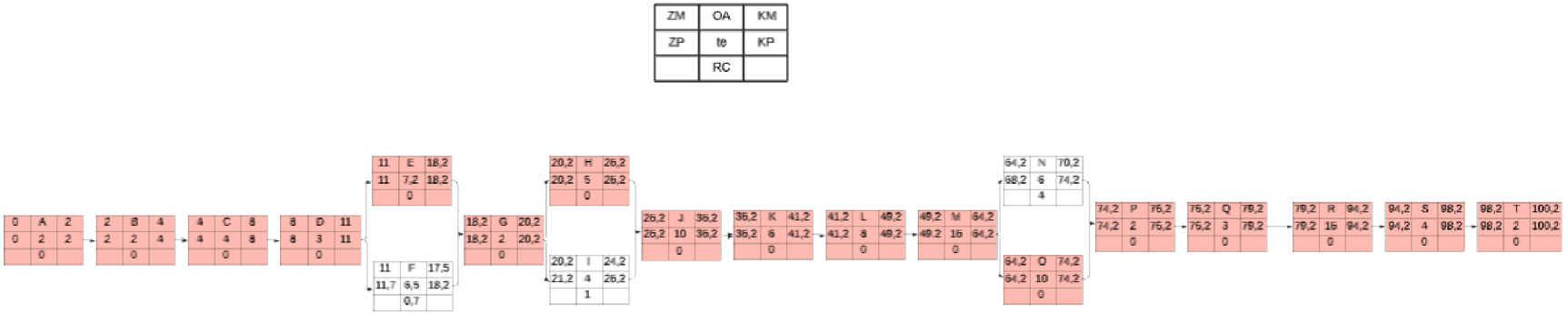
Obrázek 37: Analýza PERT – tabulka
Zdroj: Vlastní zpracování

Pro lepší pochopení tabulky je níže legenda:

ZM – začátek možný, KM – konec možný, ZP – začátek přípustný, KP – konec přípustný, RC – celková rezerva, a – optimistický odhad trvání činnosti, m – realistický odhad trvání činnosti, b – pesimistický odhad trvání činnosti, t – odhad doby trvání činnosti

Z tabulky je patrné, kolik času zabere celkové dokončení projektu (sloupec KM – konec možný, řádek T). Předpokládá se, že všechny zdroje budou plně k dispozici a nedojde k žádnému zpoždění. Projekt by měl trvat asi 101 pracovních dní. S tím, že v celém projektovém týmu bude šest lidí – tři zaměstnanci programátoři, dva zaměstnanci designéři a poslední zaměstnanec s funkcí projektového manažera.

Síťový graf PERT



Obrázek 38: Síťový graf PERT

Zdroj: Vlastní zpracování

Na výše znázorněném síťovém grafu je světle červenou barvou označena tak zvaná kritická cesta, která znázorňuje nejdelší cestu v projektu. Na kritické cestě leží všechny činnosti kromě činností F, I a N.

Z výše provedené časové analýzy by se projektu účastnilo aktivně šest lidí, při osmi hodinové pracovní době v přepočtu 808 pracovních hodin. V přepočtu hodinovou sazbou 250 Kč činí náklady návrhu a celkové implementace 202 000 Kč na jednoho zaměstnance. Pro výpočet celkových nákladů jsem 202 000 Kč vynásobila šesti zaměstnanci a vyšla maximální celková částka 1 212 000 Kč. U této částky je nutno brát v potaz, že ne všichni zaměstnanci se budou podílet na projektu celých 101 pracovních dní, a proto bude reálná částka nižší než vypočtená.

Po spuštění helpdesku se celkové finanční zhodnocení odvíjí i od počtu zaměstnanců pracujících v helpdesku. Nyní má firma jednoho zaměstnance, který se stará o zákaznickou podporu, což je pro splnění pracovních požadavků málo. Rovněž ticketovací systém bude na obsluhu časově náročnější, a proto nestačí jeden zaměstnanec. Proto bych navrhovala, že by ve firemním helpdesku mohli začít pracovat tři až čtyři zaměstnanci. A jelikož práci zastanou velmi dobře i studenti, bylo by postačující mít jednoho zaměstnance na plný úvazek a ostatní na částečný úvazek – ti by se v práci střídali. Postupem času se může počet zaměstnanců zvýšit.

Firma má v plánu, že helpdesk bude dostupný pět dní v týdnu, osm hodin.

Ze začátku bych tedy navrhovala čtyři helpdesk zaměstnance, kteří budou obstarávat telefonní hovory a dotazy psané do formuláře na webových stránkách pomocí ticketovacího systému. Jeden ze zaměstnanců by byl zaměstnaný na plný úvazek a tři další by mohli být například studenti, kteří by měli částečný úvazek. To znamená, že zaměstnanci na částečný úvazek by se střídali. V práci by byli přítomni minimálně dva zaměstnanci současně (jeden zaměstnanec na plný úvazek a jeden na částečný) a maximálně tři zaměstnanci současně (jeden zaměstnanec na plný úvazek a dva na částečný).

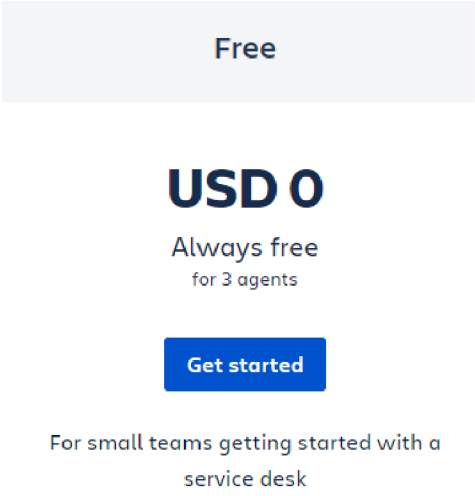
V tabulce 4 jsem uvedla hrubý odhad měsíčních nákladů na mzdy.

Tabulka 4: Výpočet celkových nákladů za mzdy zaměstnanců

Typ úvazku	Počet hodin v práci týdně	Hodinová hrubá sazba (odhadem)	Hrubá mzda/měsíc (odhadem)
Plný	40	250,-	40 000,-
Částečný	0–20	150,-	12 000,- (při 20 h/týdně)
Částečný	0–20	150,-	12 000,- (při 20 h/týdně)
Částečný	0–20	150,-	12 000,- (při 20 h/týdně)
Maximální celkové náklady za mzdy/měsíc			76 000,-/měsíc

Zdroj: Vlastní zpracování

Na základě výše uvedeného maximálního počtu zaměstnanců pracujících současně by bylo možné pořídit Jira Service Management zdarma, protože do tří uživatelů je možné tento software používat bezplatně.



Obrázek 39: Bezplatná licence pro tři uživatele
Zdroj: (29)

V práci by měli zaměstnanci helpdesku přidělené notebooky, a to pro každého zaměstnance jeden na plný i částečný úvazek. Doporučovala bych notebooky do 30 000,- korun českých. Celkem by náklady na hardware činily, v případě čtyř zaměstnanců, 120 000,- korun českých.

Celkové náklady před zahájením provozu helpdesku by činily asi 1 332 000,-. V tomto odhadu je započtena doba strávená zaměstnanci na dokončení projektu a následně pořízení hardwaru pro zaměstnance helpdesku. Tyto dva náklady jsou uvedeny v tabulce níže.

Tabulka 5: Celkové náklady před zahájením provozu helpdesku

Náklad	Částka
Dokončení projektu	1 212 000,-
Pořízení hardwaru	120 000,-

Zdroj: Vlastní zpracování

Po zavedení helpdesku do plného provozu by se náklady sestávaly pouze z mezd zaměstnanců helpdesku. Tyto mzdy a odhadnutá částka jsou uvedeny v tabulce 4. V potaz neberu fixní náklady jako je elektrická energie a pronájem, protože ty firma platí i nyní a v této oblasti se nebude odehrávat žádná změna.

V případě, že by bylo potřeba provozovat helpdesk šest dní v týdnu, musel by se zvýšit počet zaměstnanců. Toto opatření by vyžadovalo více lidských zdrojů, zvýšily by se náklady na mzdy, na hardware, a další náklady spojené s prací na helpdesku. Bylo by třeba navýšit počet uživatelů v programu JIRA, a to jak v základním programu, tak i v IT Service Managementu, což by vytvořilo opět dodatečné náklady.

ZÁVĚR

Cílem diplomové práce bylo navrhnutí nového helpdesku, který bude pro uživatele více intuitivní a informace budou sjednocené. Dalším důležitým bodem vytvořeného helpdesku bylo i splnění požadavku na zařazení Knihovny dotazů.

V první „Teoretické části" jsem postupně vysvětila všechny pojmy, které pak dále používám v diplomové práci. Jednalo se především o pojmy spojené se zákony a vyhláškami, které se týkají kybernetické bezpečnosti. Vysvětlila jsem, co znamená helpdesk a jak na pojem helpdesku správně nahlížet. V závěru teoretické části jsem popsala softwary, pomocí kterých jsem helpdesk navrhovala.

V druhé části „Analýza současného stavu", jsem analyzovala současný stav firmy. Popsala jsem firmu ISIT Slovakia a produkt, který firma vyvíjí. Uvedla jsem, které moduly má firma v rámci programu k dispozici a co lze v jednotlivých modulech vytvořit za dokumentaci. Tato dokumentace bude sloužit pro splnění požadavků v souladu s kybernetickým zákonem a s ním spojených vyhlášek.

Třetí část „Návrh řešení" se věnuje návrhu a popisu nově vytvořeného helpdesku. Jsou zde uvedeny důvody tvorby nového helpdesku, designový návrh a dále popis funkcionality. Nový helpdesk má tu výhodu, že se nachází na webových stránkách, na rozdíl od současného helpdesku, který je vestavěný v softwaru. Výhoda je to především v tom, že pokud dojde k nefunkčnosti programu nebo nastanou problémy s jeho instalací, může se uživatel obrátit na nově vytvořený helpdesk. Tento helpdesk bude díky vystavení na webu stále dostupný. Dalším benefitem je, že vytvořený helpdesk bude přístupný v českém jazyce. Avšak největší kladnou změnou je nově vytvořená Knihovna dotazů. Tato knihovna představuje SQL databázi všech položených dotazů od uživatelů a bude implementována na webové rozhraní. Tuto knihovnu bude moct navštívit každý přihlášený zákazník. Díky tomu, že knihovna bude v online podobě na webových stránkách, bude pro uživatele neustále dostupná. Na konci kapitoly je uveden postup implementace helpdesku a možná implementační rizika. Poslední kapitolou je celkové ekonomické zhodnocení návrhu. Před uvedením helpdesku do provozu by firma vynaložila náklady ve výši asi 1 332 000 Kč. Po zahájení provozu by pak platila měsíční variabilní náklady ve výši asi 76 000 Kč.

SEZNAM POUŽITÝCH ZDROJŮ

(1) Legislativa KB. *Národní úřad pro kybernetikou bezpečnost* [online]. [cit. 2020-12-03]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

(2) GDPR. *GDPR - Obecné nařízení o ochraně osobních údajů prakticky* [online]. Mgr. Eva Škorničková [cit. 2020-12-03]. Dostupné z: https://www.gdpr.cz/gdpr/

(3) SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4. vydání. Praha: Grada, 2013. ISBN 978-80-247-4644-9.

(4) JORDÁN, Vilém a Viktor ONDRÁK. *Infrastruktura komunikačních systémů II: Kritické aplikace*. Brno: AKADEMICKÉ NAKLADATELSTVÍ CERM, s.r.o. Brno, 2015. ISBN 978-80-214-5240-4.

(5) BRUTON, Nigel. *How to manage the IT Helpdesk*. Druhé. Great Britain: The Bruton Consultancy, 2002. ISBN 0750649011.

(6) JAK NA HELPDESK? KOUZLO ÚSPĚCHU TKVÍ V DOBRÉ ORGANIZACI INCIDENTŮ. *Blog Aira* [online]. Copyright Aira Group, 2020 [cit. 2020-12-03]. Dostupné z: https://blog.aira.cz/jak-na-helpdesk-kouzlo-uspechu-tkvi-v-dobre-organizaci-incidentu

(7) Czegel, B.: Running Effective Help Desk, 2nd Edition. Wiley, New York, 1998. ISBN 13: 978-0471248163

(8) GDPR Software [online]. Slovakia: noGrey, 2020 [cit. 2020-12-03]. Dostupné z: www.gdpr-software.eu

(9) HALSEY, Mike. The IT Support Handbook. Sheffield, UK: Apress Media LLC: Welmoed Spahr, 2019. ISBN 978-1-4842-5132-1.

(10) Informační bezpečnost. *Centrum pro veřejnou zprávu* [online]. [cit. 2021-03-08]. Dostupné z: https://www.acsa.cz/verejnasprava/dalsi-sluzby/informacni-bezpecnost/

(11) Jaké povinnosti vyplývají pro orgány veřejné moci ze zákona o kybernetické bezpečnosti? - II. *Právní prostor* [online]. ATLAS CONSULTING spol., 1999–2021, 01.12.2015 [cit. 2021-03-08]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/jake-povinnosti-vyplyvaji-pro-organy-verejne-moci-ze-zakona-o-kyberneticke-bezpecnosti-ii

(12) SEDLÁK, Petr. *Kybernetická bezpečnost obecně* [prezentace]. Brno, 2021 [cit. 2021-03-21]. Dostupné z: https://www.vutbr.cz/

(13) *Lucidchart* [online]. USA: Lucid Software, 2021 [cit. 2021-03-21]. Dostupné z: https://www.lucidchart.com/

(14) *Canva* [online]. Canva, 2021 [cit. 2021-03-21]. Dostupné z: https://www.canva.com/pro/

(15) Kdo je pravý CIO? *Business world* [online]. Praha: IDG Czech Republic, 2018, 1.2.2004 [cit. 2021-03-21]. Dostupné z: https://businessworld.cz/personalni-udalosti/kdo-je-pravy-cio-4009

(16) CISO (Chief Information Security Officer) - Manažer informační bezpečnosti. *Management mania* [online]. Managementmania.com, 2016, 22.09.2015 [cit. 2021-03-21]. Dostupné z: https://managementmania.com/cs/ciso-chief-information-security-officer-manazer-informacni-bezpecnosti#:~:text=CISO%20(Chief%20Information%20Security%20Officer)%2C%20n%C4%9Bkdy%20t%C3%A9%C5%BE%20Information%20Security,za%20informa%C4%8Dn%C3%AD%20bezpe%C4%8Dnost%20v%20organizaci.

(17) *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Praha: NÚKIB [cit. 2021-03-21]. Dostupné z: https://www.nukib.cz/cs/ (https://nukib.cz/cs/kyberneticka-bezpecnost/))

(18) Security Operations Center. *AEC* [online]. Praha: AEC, 2021 [cit. 2021-03-21]. Dostupné z: https://www.aec.cz/cz/produkty-a-sluzby/Stranky/soc.aspx

(19) The Complete Guide to CSIRT Organization: How to Build an Incident Response Team. *Exabeam* [online]. Foster City: Exabeam, 2021, 19.07.2018 [cit. 2021-03-21]. Dostupné z: https://www.exabeam.com/incident-response/csirt/

(20) Jak identifikovat primární a podpůrná aktiva a zachytit závislost mezi nimi. *Clever and Smart* [online]. Miroslav Čermák, 2008 - 2021, 12. 03. 2016 [cit. 2021-03-21]. Dostupné z: https://www.cleverandsmart.cz/jak-identifikovat-primarni-a-podpurna-aktiva-a-zachytit-zavislost-mezi-nimi/)

(21) Security Awareness, Training, and Education - A Learning Continuum. *Pratum* [online]. Des Moines, IA | Cedar Rapids, IA | Dallas, TX | Kansas City, KS: Pratum, 2021, 16.08.2016 [cit. 2021-03-21]. Dostupné z:

https://www.pratum.com/blog/331-security-awareness-training-and-education-learning-continuum

(22) Co je ITIL. *Tayllorcox* [online]. TAYLLORCOX, 2019 [cit. 2021-03-21]. Dostupné z: https://www.tx.cz/itil/metodika

(23) ITSM (IT Service Management). *Management mania* [online]. Praha: ManagementMania.com, 2016, 04.11.2016 [cit. 2021-03-21]. Dostupné z: https://managementmania.com/cs/it-service-management#:~:text=IT%20Service%20Management%20je%20souhrn,z%C3%A1kazn%C3%ADk%C5%AF%20i%20poskytovatele%20IT%20slu%C5%BEeb

(24) ISIT Slovakia s.r.o. *FinStat* [online]. Finstat, 2021 [cit. 2021-03-21]. Dostupné z: https://www.finstat.sk/44783990#

(25) ISIT SOFTWARE CZ s.r.o. *Veřejný rejstřík a Sbírka listin* [online]. České republika: Ministerstvo spravedlnosti, 2015, 27. srpna 2020 [cit. 2021-03-21]. Dostupné z: https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=1094108&typ=PLATNY

(26) *Sevitech CZ* [online]. Praha: SEVITECH CZ, 2020 [cit. 2021-03-21]. Dostupné z: https://www.sevitech.cz/

(27) *The Science for Population Protection* [online]. 2009 [cit. 2021-03-24]. Dostupné z: http://www.population-protection.eu/prilohy/casopis/6/43.pdf

(28) SEDM + JEDNO PRAVIDLO ŘÍZENÍ RIZIK. *Tomáš Bezouška* [online]. WordPres, 2021, 14.6.2020 [cit. 2021-03-24]. Dostupné z: http://bezouska.cz/sedm-a-jedno-pravidlo-rizeni-rizik/

(29) JIRA. *Atlassian* [online]. Atlassian, 2021 [cit. 2021-04-23]. Dostupné z: https://www.atlassian.com/software/jira

(30) *Kurzy měn: Kurzovní lístek ČNB* [online]. Kurzy.cz, spol. s r.o., AliaWeb, spol. s r.o., 2000 - 2021 [cit. 2021-4-27]. Dostupné z: https://www.kurzy.cz/kurzy-men/

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

GDPR	General Data Protection Regulation
KBO	Kybernetická bezpečnost organizace
IKS	informační komunikační systém
IKT	informační a komunikační technologie
ITSM	IT service management
ITIL	information technology infrastructure library
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
NCKB	Národní centrum kybernetické bezpečnosti
CIO	Chief Information Officer
CISO	Chief Information Security Officer
NIS	Network and Information Security Incidents
DPO	Pověřenec pro ochranu osobních údajů
ISO	International Organization for Standardization
SAE	Security Awareness Education
IT	informační technologie
EU	Evropská Unie
s.r.o.	společnost s ručením omezeným
SW	software
DPIA	data protection impact assessment
FAQ	nejčastější dotazy

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH TABULEK