Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Informační bezpečnostní systémy

Bakalářská práce

2021 Šárka Razimová

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Šárka Razimová**
Osobní číslo:	**E18349**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Téma práce:	**Informační bezpečnostní systémy**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cíl práce: vytvořit podklady pro výuku informačních bezpečnostních systémů.

Osnova:

- rešerše informačních bezpečnostních systémů,
- analýza požadavků trhu práce na odborníky v oblasti informačních bezpečnostních systémů,
- vytvoření podkladů pro výuku informačních bezpečnostních systémů.

Rozsah pracovní zprávy: **Cca 35 stran.**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

Burda, K. *Základy elektronických zabezpečovacích systémů*. Brno: Akademické nakladatelství CERM, 2017. ISBN 978-80-7204-967-7.
Dobda, L. *Ochrana dat v informačních systémech*. Praha: Grada, 1998. ISBN 80-7169-479-7.
Křeček, S. *Příručka zabezpečovací techniky*. 3. aktualiz. vyd. Blatná: Blatenská tiskárna, 2006. ISBN 80-902938-2-4.
Kyncl, J. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.

Vedoucí bakalářské práce: **doc. Ing. Miloslav Hub, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2020**
Termín odevzdání bakalářské práce: **30. dubna 2021**

L.S.

prof. Ing. Jan Stejskal, Ph.D.
děkan

RNDr. Ing. Oldřich Horák, Ph.D.
vedoucí ústavu

V Pardubicích dne 1. září 2020

Prohlašuji:

Práci s názvem Informační bezpečnostní systémy jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 28. 4. 2021

Šárka Razimová v. r.

PODĚKOVÁNÍ

Tímto bych ráda poděkovala svému vedoucímu práce doc. Ing. Miloslavu Hubovi, Ph.D. za jeho vstřícnost, pomoc, odborné a cenné rady, které mi pomohly při tvorbě této bakalářské práce. Také bych chtěla poděkovat své rodině, která mě po celou dobu studií podporovala.

ANOTACE

Tato bakalářská práce se zaměřuje na oblast informačních bezpečnostních systémů. Nejprve je provedena rešerše informačních bezpečnostních systémů a analýza trhu práce. Práce přehledně zobrazuje seznam středních a vysokých škol, na kterých lze příslušné obory studovat, a souhrn profesí, ve kterých lze získané vědomosti uplatnit. Dále je realizován průzkum požadavků zaměstnavatelů na uchazeče, kteří by chtěli najít uplatnění v tomto oboru. Součástí je zhodnocení výuky informačních bezpečnostních systémů na Fakultě ekonomicko-správní Univerzity Pardubice a doplňkové studijní materiály, které byly v rámci práce vytvořeny.

KLÍČOVÁ SLOVA

bezpečnost, bezpečnostní systémy, informační bezpečnostní systémy

TITLE

Information security systems

ANNOTATION

This bachelor thesis focuses on the field of information security systems. First, a search of information security systems and analysis of the labor market is performed. The thesis clearly displays a list of high schools and universities where the relevant fields can be studied and a summary of professions in which the acquired knowledge can be applied. Furthermore, a survey of employers' requirements is carried out to applicants who would like to find employment in this field. It includes an evaluation of the teaching of information security systems at the Faculty of Economics and Administration of the University of Pardubice and additional study materials that were created within the work.

KEYWORDS

security, security systems, information security systems

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

AHD	Analog high definition
AI	Umělá inteligence (z angl. Artificial Intelligence)
CCTV	Kamerový systém (z angl. Closed-circuit television)
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique
CISSP	Certified Information Systems Security Professional
CPP	Certified Protection Professional
ČR	Česká republika
DPPC	Dohledové a poplachové přijímací centrum
EKV	Elektronická kontrola vstupu
EPS	Elektrická požární signalizace
EZS	Elektronická zabezpečovací signalizace
FES	Fakulta ekonomicko-správní
FUIBS	Úvod do informačních bezpečnostních systémů
IBS	Informační bezpečnostní systémy
ICT	Informační a komunikační technologie (z angl. Information and Communication Technologies)
IT	Informační technologie
IS	Informační systém
MDC	Multifunkční dohledové centrum
MZS	Mechanické zábranné systémy
PCO	Pult centralizované ochrany
PSP	Physical Security Professional
PZTS	Poplachový zabezpečovací a tísňový systém
UPa	Univerzita Pardubice
VLAN	Virtual Local Area Network
ZDP	Zařízení dálkového přenosu
WDR	Wide Dynamic Range
IR	Infračervené záření (z angl. Infrared)

ÚVOD

S rychlým rozvojem společnosti dochází i k neustálému rozvoji a modernizaci bezpečnostních technologií, které se stávají pro tuto společnost dostupnější a tím i široce nasazované v nejrůznějších oblastech. V případě organizací se zvyšuje potřeba ochrany důvěrných informací, obchodního tajemství a know-how. Domácnosti se naopak snaží ochránit především majetek a další hodnotná aktiva. To ovšem nejsou jediné případy, kdy se s těmito technologiemi setkáváme. Často je totiž ani nevnímáme, a přesto jsou všude kolem nás – ve školách i zaměstnáních, v obchodech a na úřadech, ale také například v ulicích okolo našeho bydliště.

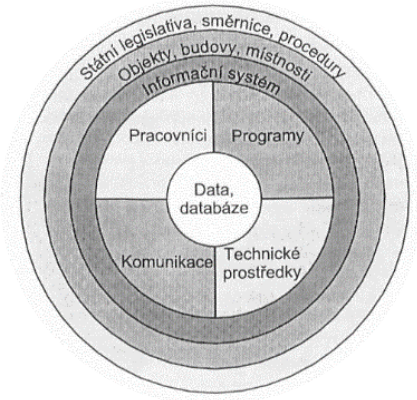
V této bakalářské práci je popsána oblast bezpečnostních systémů včetně pojmu „informační bezpečnostní systémy“. Další část práce analyzuje situaci na trhu práce. Shrnuje střední a vysoké školy v České republice, které se zabývají výukou informačních bezpečnostních systémů, a představuje povolání, ve kterých se v této oblasti lze uplatnit. Součástí práce je rovněž průzkum požadavků zaměstnavatelů na budoucí uchazeče v tomto oboru. Závěrečná část práce je zaměřena na zhodnocení výuky informačních bezpečnostních systémů na Fakultě ekonomicko-správní Univerzity Pardubice a tvorbu studijních materiálů, které budou sloužit jako doplňkové materiály k výuce předmětu Úvod do informačních bezpečnostních systémů (FUIBS/CUIBS) na této škole.

1 INFORMAČNÍ BEZPEČNOSTNÍ SYSTÉMY

1.1 Informační systémy

Informačním systémem (zkráceně IS) můžeme rozumět systém vzájemně propojených procesů a informací, přičemž procesy s těmito informacemi pracují [15]. Procesy zde chápeme jako funkce, jež zpracovávají informace vstupující do systému a přetvářejí je na informace, které ze systému vystupují. Funkce tedy zajišťují sběr, uložení, přenos, zpracování a distribuci informací. Informace jsou definovány jako údaje sloužící zejména k rozhodování nebo řízení v rozsáhlejším systému [15]. Do funkce IS se rovněž promítá komponenta okolí. Tuto komponentu tvoří všechny objekty, které při změně svých vlastností ovlivňují daný systém. Souhrnně lze říct, že bezpečný informační systém je takový systém, který ochraňuje informace během procesu jejich vstupu, uložení, zpracování, přenosu a výstupu proti ztrátě důvěrnosti, dostupnosti a integrity, a to i při jejich likvidaci [6].

Informační systém tvoří 4 základní složky: hardware a software (tvoří část informačních technologií, které informační systém využívá, přičemž informačními technologiemi rozumíme tu techniku, která má za úkol zpracování informací a dat), data a lidé [6]. Jelikož se IS skládá z více částí, tak bezpečnost nejlépe zajistíme aplikováním komplexních ochranných mechanismů. Obecný model informačního systému je na obrázku 1.



Obrázek 1: Obecný model informačního systému a reálného okolí

Zdroj: [6]

1.2 Informační bezpečnostní systémy

Především v souvislosti s ochranou informačních systémů, ale i ochranou hodnotných aktiv firem i domácností se můžeme setkat s pojmy „informační bezpečností systémy“ či „integrované bezpečnostní systémy“. Informační bezpečnostní systémy (zkratka IBS) jsou systémy, ve kterých jsou technické a organizační prvky navrženy tak, aby byly schopny poskytnout dostatečně možnou bezpečnost před známými vnějšími vlivy pro předem danou konkrétní oblast anebo zájem [18]. Zájmem rozumíme zpravidla majetek, ale i jiná hodnotná aktiva, která by mohla být poškozena, zničena či odcizena. IBS v technickém pojetí tvoří soustava mechanických, elektrických, elektronických a jiných součástek, které tvoří pevně zabudované překážky zabraňující vstupu neoprávněných osob do chráněného prostoru [18]. Z fyzického opatření IS se tak stává poměrně rozsáhlá samostatná kategorie systémů, které nějakým způsobem zpracovávají a podávají informace o narušení bezpečnosti, a mohou i nemusí ke své činnosti využívat informační technologie, přičemž primárním úkolem všech těchto systémů je zajistit rychlou a relevantní identifikaci narušení daného objektu či systému a zároveň včas upozornit majitele, případně jinou pověřenou osobu [11]. Každý takový systém by měl být navržen na základě analýzy rizik tak, aby splňoval požadovanou míru bezpečnosti pro předem určený chráněný zájem.

V dnešní době se stává přítomnost IBS v organizacích i na jiných místech již nutností. Dokazuje to i průzkum z roku 2020, vypracovaný společností Perfect Crowd Research pro českou firmu Jablotron, kde odpovědi pochází přímo od pachatelů trestné činnosti – zlodějů. Z průzkumu vyplývají tyto informace [14]:

- do rodinných domů by se pachatelé vloupali raději v noci, zatímco do bytu by se až 75 % zlodějů vloupalo přes den,
- 75 % dotazovaných uvedlo, že využili neopatrnosti obětí jejich činu – pootevřené okno, klíče schované v blízkosti dveří, otevřená ventilace…,
- 2 minuty – jen tak málo času lupičům stačí k překonání zámku u běžných dveří, pokud objekt nedisponuje elektronickým zabezpečením,

- blízkost lidí respondenti nepovažovali za žádnou překážku,
- přítomnost psa by určité procento pachatelů odradila, ale rozhodně není 100% překážkou,
- zloděje neodradí ani to, že do objektu neuvidí – trend neprůhledných skel, zatažené žaluzie či další podobná opatření také nemohou zaručit ochranu objektu,
- pokud by většina pachatelů narazila při vloupání na alarm napojený na pult centrální ochrany, okamžitě by činnosti zanechala a objekt opustila.

Pokud se tedy rozhodneme pro zabezpečení objektu, musíme si v první řadě položit tyto základní otázky: Co chceme chránit (celý objekt, určité zařízení, informace atd.)? Před čím chceme danou věc chránit (vloupání, přírodní vlivy…)? Zda a případně které osoby musí být chráněny? Jakým způsobem ochranu zajistíme? [11]

1.2.1 Dělení z hlediska prostorového zaměření

Informační bezpečností systémy dělíme podle několika různých hledisek. Nejzásadnějším z nich je hledisko prostorového zaměření, které dělíme na ochranu obvodovou, plášťovou, prostorovou, předmětovou a vícestupňovou [18].

Obvodová či perimetrická ochrana signalizuje narušení obvodu chráněného prostoru. Pod obvodem prostoru chápeme takovou hranici, která je vymezena jistou bariérou (zeď, plot, příkop…). [18]

Plášťová ochrana má za úkol signalizovat narušení pláště daného objektu (dveře, okna, podlahy atd.). Objektem zde rozumíme samotný stavební objekt, ať už je to celá budova, či vymezená skupina místností. [18]

Prostorová ochrana upozorňuje na jevy v chráněném prostoru, které představují nebezpečí (např. detekce pohybu). Předpokladem je, že neoprávněná osoba již vnikla do objektu a pohybuje se v prostoru, ve kterém jsou nainstalovány detektory. [17]

Předmětová ochrana chrání cenné předměty (obrazy, umělecké předměty,

trezory…). V případě, že bude chráněný předmět napaden, dojde k signalizaci. Tato ochrana dokáže detekovat použití hrubého mechanického nářadí, hydraulického tlakového nářadí, užití trhavin a další. [17]

Vícestupňová ochrana kombinuje výše uvedené ochrany objektu v jeden ucelený soubor. [17]

1.2.2 Související legislativa a normy

Legislativa popisuje právní základ ochrany, jež je popsána zákony, normami a jinými nařízeními. Slouží především jako podklad při zpracovávání stavebních projektů/návrhů a pro užívání technických prostředků používaných při této ochraně. Dodržování legislativních norem je důležité především pro předejití budoucích trestněprávních důsledků (určení viníků, vzniklé škody a vyčtení náhrady). [17]

V rámci Evropské unie je zabezpečovací technika popisována směrnicemi Evropských společenství. Směrnice Evropských společenství je druh dokumentu, o jehož vydávání se stará Evropská komise. Povinnosti vyplývající ze směrnic, týkajících se technického charakteru, jsou závazné pro výrobce, dovozce a distributory. K podpoře plnění obsahu směrnic jsou vydávány evropské harmonizované normy, které nejsou závazné, ale jejich splnění je doporučeno. Evropské normy jsou vytvářeny organizacemi CEN a CENELEC. V České republice jsou tyto technické směrnice přebírány formou nařízení vlády ČR. Základní legislativní požadavky tvoří zákon č. 22/97 Sb., o technických požadavcích na výrobky. [10] Jednotlivé normy jsou děleny do skupin dle oblastí a způsobu využití [11]:

- EN 50131 Poplachové systémy – Elektrické zabezpečovací systémy
    - EN 50131-1 Všeobecné požadavky
    - EN 50131-2-1 Společné požadavky pro detektory (čidla) atd.
- EN 50132 Poplachové systémy – Systémy televizních okruhů CCTV
    - EN 50132-1 Systémové požadavky
    - EN 50132-2-1 Černobílé kamery atd.

- EN 50133 Poplachové systémy – Systémy kontroly a řízení vstupu
- EN 50134 Poplachové systémy – Systémy přivolání pomoci
- EN 50135 Poplachové systémy – Systémy tísňové
- EN 50136 Poplachové systémy – Systémy přenosové
- EN 50137 Poplachové systémy – Systémy kombinované nebo integrované
- EN 54 Elektrická požární signalizace

Dle normy EN 14383 (Plánování městské výstavby a navrhování budov) je dáno 5 úrovní zabezpečení pro 5 úrovní rizika. Úroveň zabezpečení udává odolnost jednotlivých zabezpečovacích zařízení a předpokládanou hodnotu zcizeného nebo poškozeného majetku. [10] Jednotlivé úrovně jsou zobrazeny v následující tabulce:

Tabulka 1: Úrovně rizika a způsoby zabezpečení

Úroveň zabezpečení	Úroveň rizika	Preventivní opatření
1	velmi nízké	jednoduché mechanické zabezpečení
2	nízké	zvýšené mechanické zabezpečení
3	střední	zvýšené mechanické zabezpečení a minimální elektronické zabezpečení
4	vysoké	rozsáhlé mechanické zabezpečení a střední elektronické zabezpečení
5	velmi vysoké	rozsáhlé mechanické zabezpečení a vysoké elektronické zabezpečení

Zdroj: [10]

Kromě požadavků na technická zařízení definuje zákon také odbornou způsobilost, kterou musí vykazovat každý, kdo by chtěl podnikat v oboru IBS. Podnikatel musí vlastnit koncesovanou živnost skupiny číslo 314 – Technické služby k ochraně majetku a osob. Tato skupina obsahuje dle nařízení vlády č. 278 Sb.,: „Projektování, montáž, kontrola, údržba a opravy elektrických zabezpečovacích systémů (zejména systémů zabezpečovacích, tísňových,

protipožárních, kontroly vstupu, přivolání pomoci, integrovaných a kamerových), určených k ochraně majetku a osob před neoprávněnými zásahy, včetně poplachových systémů a zařízení umožňujících sledování pohybu a projevů osob v objektech a okolí. Montáž, opravy, údržba, revize a správa mechanických zábranných systémů, dostatečně zvyšujících účinnost běžných standardů zabezpečení majetku a osob.“ [16]

V souvislosti s výše uvedenou skupinou je vyžadována odborná a jiná zvláštní způsobilost podle § 27 odstavce 1 a 2 živnostenského zákona ve znění zákona č. 356/1999 Sb. a č. 167/2004 Sb. [10]:

- vysokoškolské vzdělání v příslušné nebo příbuzné oblasti + 1 rok praxe v oboru nebo
- dokončené střední odborné vzdělání v oboru nebo příbuzném oboru + 2 roky praxe v oboru nebo
- vyučení v tříletém učebním oboru nebo příbuzném oboru + 3 roky praxe v oboru.

K této způsobilosti může být vyžadována např. i odborná způsobilost dle vyhlášky č. 50/1978 Sb., o odborné způsobilosti v elektrotechnice a další. Roku 2018 došlo ke 2 úpravám živnostenského zákona, které stanovují upravené podmínky pro podnikatele ve formě nutnosti prokázání bezúhonnosti všech jeho pracovníků výpisem z rejstříku trestů [16].

1.3 Typy informačních bezpečnostních systémů

Do oblasti IBS patří velké množství technologií, které se postupem času rychle rozvíjejí a zdokonalují. Na trhu působí desítky firem, které se snaží poskytovat komplexní služby v oboru bezpečnosti, přes návrh zabezpečení daného objektu až po instalaci a následný servis těchto zařízení. Nejrozšířenějšími bezpečnostními systémy jsou poplachové zabezpečovací a tísňové systémy, elektrická požární signalizace a kamerové systémy. Dále např. perimetrické systémy, docházkové a přístupové systémy aj.

1.3.1 Poplachový zabezpečovací a tísňový systém

Poplachový zabezpečovací a tísňový systém (PZTS) byl dříve známý jako elektrická zabezpečovací signalizace (EZS). Je to ucelený soubor všech technických prostředků, které zajišťují ochranu objektu proti neoprávněnému vstupu [11]. Pokud je rozpoznáno neoprávněné vniknutí nepovolanou osobou do objektu, je toto vniknutí včas rozpoznáno a signalizováno, čímž systém zabrání případným škodám. Signalizace má nejčastěji formu sirény (vnitřní či vnější), SMS zprávy, která je odeslána na předem daná telefonní čísla, anebo posláním poplašné zprávy na dohledové a poplachové přijímací centrum. PZTS systém je tvořen ústřednou (řídící počítač se specifickými periferiemi), detektory (elektrická zařízení, která odhalují vzniklý incident a následně tuto událost hlásí ústředně), ovládací klávesnicí a koncovými zařízeními, a často se kombinuje s dalšími technologiemi (např. s CCTV) [3].

Rozdělení PTZS je téměř shodné s rozdělením fyzické ochrany, tedy z hlediska prostorového zaměření [11]:

- obvodová (perimetrická) ochrana – k signalizaci dojde v případě narušení obvodu střeženého území a prostoru kolem střeženého objektu (obvod je obvykle tvořen katastrálními hranicemi, které tvoří umělé nebo přírodní bariéry),
- plášťová ochrana – signalizuje narušení pláště budovy (pláštěm rozumíme okna, dveře, šachty apod.),
- prostorová ochrana – zajišťuje zabezpečení vnitřního prostoru chráněného objektu; reaguje převážně na pohyb potenciálního pachatele a jiné podezřelé jevy ve vnitřním prostoru,
- předmětová ochrana – signalizace se spustí při napadení či neoprávněné manipulaci s daným předmětem (chráněným předmětem můžou být umělecké předměty, klenoty aj.); s touto ochranou se můžeme nejčastěji setkat v bankách, muzeích a galeriích,
- tísňová ochrana – slouží k signalizování ohrožení života nebo zdravotních problémů osob (ohrožení způsobené buď přírodními živly,

nebo mimořádnými událostmi – teroristický útok); poplašný signál se v tomto případě vyvolá:

- automaticky – příkladem je využití hlásiče nehybnosti,
- manuálně – stisknutí tlačítka,
- předem definovaným způsobem manipulace – nášlapná tísňová lišta.

1.3.2 Elektrická požární signalizace

Elektrická požární signalizace (EPS) je požárně bezpečnostní zařízení, které se stará o včasnou detekci požáru a následnou signalizaci tohoto požáru prostřednictvím hlásičů požáru. Signály z hlásičů požáru přijímá ústředna EPS, což je zařízení, které shromažďuje informace ze všech hlásičů připojených k tomuto systému. [10] U ústředny by měla být zajištěna 24hodinová obsluha, která by v případě požáru přivolala hasičský záchranný sbor. V případě nepřítomnosti obsluhy musí být systém EPS připojen zařízením dálkového přenosu (ZDP) k centrálnímu dohledovému pultu příslušné jednotky požární ochrany (v tomto případě je střežený objekt navíc vybaven obslužným polem požární ochrany a klíčovým trezorem, ve kterém je uložen generální klíč k objektu) [10].

Kromě ústředny se EPS skládá ze samočinných a tlačítkových hlásičů požáru (tlačítkové hlásiče, samočinné hlásiče, ionizační hlásiče, opticko-kouřové hlásiče, hlásiče teplot, speciální hlásiče – lineární hlásiče tepla, lineární optické hlásiče, systémy nasávání kouře, hlásiče pro vzduchotechniku, hlásiče detekce oxidu uhelnatého), požárního poplachového zařízení, adaptérů, požárních kabelů a jiného příslušenství [11]. Elektrickou požární signalizaci dělíme na [11]:

- jednostupňové EPS – jedna nebo i více ústředen, na které jsou napojeny samočinné a tlačítkové hlásiče požáru; tyto EPS nemají vedlejší ústřednu,
- vícestupňové EPS – hlavní a vedlejší ústředny, na které jsou připojeny samočinné a tlačítkové hlásiče požáru, ale také vedlejší ústředny nižšího stupně,

- EPS s individuální adresací – identifikuje stav jednotlivých hlásičů na hlásicí lince,
- EPS s kolektivní adresací – ústředna je schopna rozlišit, ze které hlásicí linky přišel poplašný signál, ale nedokáže zjistit, od kterého konkrétního hlásiče tento signál přisel – tím může dojít k prodloužení doby zásahu.

1.3.3 Kamerové systémy

Kamerové systémy, dnes známé pod zkratkou CCTV, můžeme definovat jako elektronický systém, který umožňuje sledovat aktivitu v kontrolované oblasti. Pozorovatel (neboli oprávněná osoba) sleduje danou oblast z místa, kterému říkáme dohledové centrum. V dohledovém centru jsou signály z kontrolovaných míst prezentovány oprávněné osobě formou dynamického obrazu, který lze sledovat buď v reálném čase, nebo využít zpětného přehrávání. [3]

CCTV lze využívat samostatně (např. pro monitorování bank, veřejných prostranství, obchodů) nebo je lze používat spolu s dalšími systémy do komplexnějších celků. Ve většině případů jsou kamerové systémy spojovány s PZTS, docházkovými systémy, perimetrickým zabezpečením a dalšími technologiemi. Při výběru vhodného typu kamer bychom měli zvažovat především tyto vlastnosti [10]:

- rozlišení kamery,
- druh – digitální, analogový, AHD,
- úhel záběru kamery,
- obraz – barevný/černobílý,
- konstrukce kamery (např. odolnost vůči vlhkosti),
- napájení – síťové/nízkovoltové st/nízkovoltové ss,
- synchronizace – interní/externí/line-lock,
- dodatkové nebo jiné speciální funkce (WDR funkce, IR osvětlení…).

V oblasti kamerových systémů rozeznáváme například standardní kamery, IP kamerové systémy, bezdrátové kamery, dome kamery, deskové kamery, speciální skryté kamery, antivandal kamery, PTZ kamery, termovizní kamery aj.

1.3.4 Perimetrické systémy

Perimetrické systémy, tj. stacionární perimetrická ochrana označuje obecně venkovní střežení. Tento způsob zabezpečení ovšem nestřeží celý venkovní prostor, nýbrž pouze vytyčené uzlové body, u nichž předpokládáme, že by mohly být při vniknutí do oblasti využity, protože střežit celé rozsáhlé plochy by bylo velmi nákladné [11]. Nejčastější využití perimetrických systémů nalezneme při střežení hranic pozemku (např. plotu). V takové situaci se nejvíce používají infrazávory, mikrovlnné detektory, detektory magnetických anomálií, radiolokační pohybové detektory nebo laserové zabezpečovací systémy. Dále slouží k ochraně venkovních skladových míst nebo zahrad, průmyslových areálů a letištních prostor, obytných zón a parkovišť. V případě, že dojde k včasné detekci pokusu o narušení stráženého prostoru, můžeme následně aktivovat požadovanou reakci. Touto reakcí může být přivolání ostrahy, přivolání jiných příslušných složek, zaktivování světla, kamerových systémů aj. [11]

Infrazávory používají neviditelné záření, které vyzařuje vysílač. Následně je paprsek přijímán optickou soustavou přijímače. Pokud je tento paprsek z nějakého důvodu přerušen, ústředna ho vyhodnotí jako narušení perimetru a dojde k vyhlášení poplachu. Dosah těchto systémů může být až 250 metrů. [18]

Mikrovlnné detektory využívají „Dopplerův jev“. Vysílač těchto detektorů vyzařuje vysokofrekvenční energii, která se odráží od okolních předmětů zpět do přijímače. Pokud v hlídaném prostoru dojde k jakémukoliv pohybu, vrátí se k přijímači vysokofrekvenční energie o jiném kmitočtu a rozdíl způsobí vyhlášení poplachu. [17]

Detektory magnetických anomálií rovněž fungují na principu elektromagnetických vln. Detektory tvoří 2 kabely, které vedou pod zemí, většinou cca 2 metry od sebe, přičemž jeden z kabelů představuje vysílač a druhý přijímač. Mezi kabely se vytvoří elektromagnetické pole a při narušení tohoto pole vznikne vyvolání poplachu. [17]

Radiolokační pohybové detektory jsou také tvořeny vysílačem a přijímačem, mezi kterými je elektronická bariéra z elektromagnetických vln. Při narušení bariéry dojde k poplachu. Přijímače i vysílače se obvykle nachází na sloupcích plotů, mezi stromy apod. [17]

Laserový zabezpečovací systém je nejvhodnější k zabezpečení dlouhých hranic chráněných objektů. Výhoda tohoto systému je především odolnost vůči nepříznivým povětrnostním podmínkám ve dne i v noci. Dosah laserového paprsku může dosahovat až 2 km. [17]

1.3.5 Mechanické zábranné systémy

Mechanické zábranné systémy (MZS) jsou prostředky určené k ohraničení chráněných prostor, vstupní bezpečnostní systémy oken a dveří, bezpečnostní fólie a skla a jiné uzamykací systémy [17]. Nejzákladnější zábrany slouží pouze k upozornění, že se jedná o soukromý pozemek, a tudíž by ho neoprávněná osoba neměla navštěvovat (živý plot, závory, kůly, nízký plot). Pokročilejší mechanické zábranné systémy dělíme na 3 kategorie: prostředky obvodové ochrany, objektové ochrany a individuální ochrany [17].

Prostředky obvodové ochrany zahrnují vnější mechanické zábrany, které ale nejsou součástí vlastního objektu. Jedná se většinou o parcelu objektu, kde zábrany ohraničují fyzicky i právně hranici pozemku. Do této kategorie řadíme ochranné ploty a zdi, zabezpečení průchozích prvků zdí a plotů (dveře, branky, vrata, závory a turnikety), použití visacích zámků a petlic. [10]

Prostředky objektové ochrany zabezpečují vstupy veškerých stavebních otvorů objektu – oken, dveří, vikýřů, šachet, balkónových a sklepních oken a dveří atd. K zabezpečení se využívá dveřních zámků, bezpečnostních dveří, uzávěrů a kování, mříží a mnoho dalších. [10]

Prostředky individuální ochrany mohou být použity v předchozích systémech ochrany, ale i nezávisle jako úschovné objekty. Prostředky individuální ochrany jsou závěrečným místem pro úschovu šperků, cenností, finančních prostředků, cenných papírů a dalších hodnotných věcí. K těmto bezpečnostním systémům

se řadí trezory, trezorové skříně, manipulační schránky, přenosné kontejnery a kufry, příruční pokladny, ohnivzdorné skříně. [10]

1.3.6 Řízené docházkové a přístupové systémy

Docházkové a přístupové systémy označuje zkratka EKV (starší označení ACS) a můžeme je také najít pod pojmem elektronická kontrola vstupu. Jde o přesně vymezené systémy, přičemž každý z nich je zaměřen na jinou problematickou oblast a oba musí splňovat jisté požadavky. Moderní systémy spojují pokročile hardwarové technologie – čtečky a čipové karty, biometrické snímače, programovatelné terminály aj. [12]

Docházkové systémy slouží k evidenci a kontrole pracovní doby zaměstnanců, nočních směn, přesčasů, pracovních cest, dovolených a dalších pracovních povinností. Tuto povinnost ukládá zákoník práce zaměstnavatelům. [12] Docházkový systém vídáme nejčastěji ve formě docházkového terminálu, který je spjat s více či méně propracovaným softwarem, jenž odvádí hlavní práci. Systémy tohoto typu bývají vázány na personální agendu a zpracování mezd a platů. Hardwarové terminály mají podobu od pevně přiřazených nebo programovatelných tlačítek po tablety s dotykovou obrazovkou s operačním systémem Linux či Windows [12]. Stále častěji se můžeme rovněž setkat s terminálem ve formě mobilního klienta, ovládaného smartphonem.

Přístupové systémy využívají elektronickou identifikaci osob a ověřují práva přístupu dané osoby při procesu řízení fyzického přístupu těchto osob do chráněných budov či prostor. Specifikem přístupových systémů je to, že jsou závislé na technickém vybavení. I proto dodavatelé zpravidla nabízejí pouze jednoúčelové systémy, vázané na určitou řadu technického vybavení. V dnešní době mají přístupové systémy hierarchickou architekturu vybavení, kde je na vrcholu nějaká řídící jednotka a pod ní jsou podřazené vyhodnocovací jednotky. Podřazené jednotky jsou spojeny s elektronickými čtečkami, systémem elektronického zámku dveří nebo i jinými komponenty. [11], [12]

1.3.7 Dohledové a poplachové přijímací centrum

Dohledové a poplachové přijímací centrum (DPPC), dříve nazýváno pultem centrální ochrany (PCO), označuje centrální dispečink pro střežení, který přijímá hlášení mimořádných situací ze vzdálených střežených objektů [1]. V DPPC sedí pověřená osoba, která sleduje a vyhodnocuje přijímaná data z připojených zdrojů. Data dále interpretuje a při poplachové události má za úkol adekvátně zasáhnout (přivolání bezpečnostních složek, vyhodnocení planého poplachu), případně tuto mimořádnou událost uzavřít a informovat o ní příslušné osoby. V DPPC však již nejsou shromažďovány jen údaje o havarijních událostech, nýbrž i údaje o teplotách, poruchách výtahů, klimatizací a dalších zařízeních, stavu nejrůznějších měřicích stanic apod. [1] DPPC monitoruje připojené bezpečnostní systémy 24 hodin denně, 7 dní v týdnu, přičemž se počítá s přítomností obsluhy, která má za úkol [1]:

- zasílat denní zprávy o aktivitách, ke kterým v uplynulém dnu došlo,
- komunikovat se zákazníky při vzniku mimořádných událostí, ale i při vzniku planého poplachu,
- komunikovat s příslušnými bezpečnostními sbory v případě mimořádných událostí,
- poskytovat další bližší informace příslušným osobám.

1.3.8 Multifunkční dohledové centrum

Multifunkční dohledové centrum (MDC) je podobné výše zmíněnému dohledovému a poplachovému přijímacímu centru. Hlavní rozdíl je v rozsahu monitoringu a dohledu. Na rozdíl od DPPC, multifunkční dohledové centrum zahrnuje dohled jak nad standardními bezpečnostními systémy, tak i nad kamerovými systémy, ICT a IT systémy, systémy vytápění apod. [7] Je tedy jakýmsi doposud nejvyšším stupněm DPPC, vybaveným nejnovějšími technologiemi a obsluhovanými odbornými kvalifikovanými pracovníky. Trendem těchto technologií je propojení centra s prvky inteligentních budov. MDC jsou ve většině případů spojena s HZS, městskou policií, nebo dokonce

s Policií ČR. Obecně činnost MDC spatřujeme v napojení bezpečnostních systémů na MDC různými dostupnými prostředky, propojení centra se složkami integrovaného záchranného systému, nepřetržitém monitoringu chráněných aktiv, přenosu provozních a technických zpráv, dálkovém dohledu a kontrole neobvyklých technických stavů, poskytování výskytu událostí, zajištění informační bezpečnosti, poradenství aj. [11]

1.3.9 Další informační bezpečnostní systémy

Kromě již zmíněných informačních bezpečnostních systémů se můžeme setkat i s dalšími systémy, které nejsou tolik rozšířené, ale přesto s nimi přicházíme do styku téměř každý den, aniž bychom o tom měli tušení. Mezi takové se řadí například domovní telefony a videotelefony, se kterými se setkáváme při vstupu do objektu, kdy po stisknutí tlačítka vyzveme příslušnou osobu k ověření naší identity prostřednictví audio nebo videohovoru a odemčení dveří. Dále do této oblasti řadíme elektronický monitoring osob (nejčastěji ve formě náramku na kotníku či zápěstí), elektronické zabezpečení automobilů, kontrolu pohybu vozidel a nákladu. Masivnímu rozšíření se dostalo ochraně zboží (kombinace bezpečnostní brány a bezpečnostních prvků, uvolňovače a deaktivátory, bezpečnostní zrcadla, počítadla zákazníků aj.). Při ochraně lidských životů jsou velmi důležité evakuační rozhlasy a ozvučovací systémy, sloužící k potřebě řízené evakuace osob, pokud dojde k jejich ohrožení. Poměrně novou skupinou bezpečnostních systémů jsou biometrické systémy, zaměřující se na fyziologické a behaviorální charakteristické znaky lidí. Některé publikace do oblasti IBS dále řadí např. systémy nouzového osvětlení, pochůzkové systémy, průmyslovou havarijní signalizaci aj.

2 ANALÝZA TRHU PRÁCE

Následující kapitola se zaměřuje na analýzu trhu práce, především na výuku informačních bezpečnostních systémů v ČR, souhrn profesí, které souvisí s oborem informačních bezpečnostních systémů, a aktuální stav trhu práce. Součástí kapitoly je i průzkum požadavků a nároků vybraných firem na uchazeče o práci v oboru bezpečnostních systémů.

2.1 Výuka informačních bezpečnostních systémů v ČR

Kvalitní příprava je základ dobrého uplatnění v budoucím zaměstnání. Obory zaměřující se na bezpečnostní systémy můžeme nalézt nejen na středních a vyšších odborných školách, ale i na některých vysokých školách. Ve většině případů je výuka IBS spojena s výukou informačních technologií nebo s výukou slaboproudu. Níže jsou uvedeny některé z nich. Veškeré informace jsou převzaté z webových stránek konkrétních škol k roku 2020/2021.

2.1.1 Střední školy

Název školy, město: Střední škola elektrotechniky a strojírenství, Praha 10
Název a kód oboru: Sdělovací a zabezpečovací systémy, 26-59-H/01
Dosažené vzdělání, délka studia: Střední vzdělání s výučním listem, 3 roky
Popis oboru: Po absolvování oboru by měl student vědět, jak fungují počítačové i telefonní sítě, bude umět zprovoznit bezpečnostní systémy (např. kamerové systémy či požární hlásiče) a dozví se také o slaboproudé technice (modemy, počítače).
Odborné předměty: základy elektrotechniky, technická dokumentace, elektronika, elektrická měření, sdělovací sítě, spojovací technika, odborný výcvik
WWW stránky školy: https://www.ssesp10.cz

Název školy, město: Střední průmyslová škola dopravní, a.s., Praha 5
Název a kód oboru: Mechanik elektrotechnik – Informační a zabezpečovací systémy, 26-41-L/01

Dosažené vzdělání, délka studia: Střední vzdělání s maturitní zkouškou, 4 roky
Popis oboru: Student se naučí navrhování, montáž a uvádění zařízení do provozu, následnou diagnostiku a testování v oblasti bezpečnosti. Ovládat bude též servis instalovaných zařízení.
Odborné předměty: základy elektrotechniky, elektronika, automatizace, číslicová technika, elektrická měření, technická dokumentace, počítačové sítě a síťová zařízení, programové vybavení, zabezpečovací systémy, odborný výcvik
WWW stránky školy: https://www.sps-dopravni.cz

Název školy, město: Střední škola techniky a služeb Karviná
Název a kód oboru: Mechanik elektrotechnik – Zabezpečovací, protipožární a regulační systémy, 26-41-L/01
Dosažené vzdělání, délka studia: Střední vzdělání s maturitní zkouškou, 4 roky
Popis oboru: Student získá kromě všeobecných znalostí a dovedností z oboru elektroniky i znalosti z oboru zabezpečovacích, regulačních a protipožárních systémů budov i automobilů.
WWW stránky školy: https://sstas-karvina.cz

Název školy, město: Střední škola informatiky, poštovnictví a finančnictví Brno
Název a kód oboru: Mechanik elektrotechnik – Informační a zabezpečovací technika, 26-41-L/01
Dosažené vzdělání, délka studia: Střední vzdělání s maturitní zkouškou, 4 roky
Popis oboru: Absolvent tohoto oboru bude umět instalovat, montovat a provádět servis zabezpečovací a výpočetní techniky. Při studiu je možné získat vyhlášku č. 50/1978 Sb.
Odborné předměty: základy elektrotechniky, elektronika, automatizace, elektronické systémy, elektrická měření, technické kreslení, informační sítě, odborný výcvik
WWW stránky školy: https://www.cichnovabrno.cz

Název školy, město: Střední škola a Mateřská škola Liberec
Název a kód oboru: Mechanik elektrotechnik, 26-41-L/01
Dosažené vzdělání, délka studia: Střední vzdělání s maturitní zkouškou, 4 roky
Popis oboru: Studenti si osvojí základy z oblastí číslicové techniky, programování, elektrických měření, sdělovacích a zabezpečovacích systémů, audiovizuální techniky aj.
Odborné předměty: základy elektrotechniky, technická dokumentace, materiály a technologie, elektronická měření, číslicová technika, elektronika, automatizace, řídicí systémy a mikropočítače, bezpečnostní systémy, odborný výcvik
WWW stránky školy: https://www.ssams.cz

Název školy, město: Střední škola elektrotechniky, multimédií a informatiky Praha 9
Název a kód oboru: Elektrotechnika – Zabezpečovací technika a bezpečnostní technologie, 26-41-M/01
Dosažené vzdělání, délka studia: Střední vzdělání s maturitní zkouškou, 4 roky
Popis oboru: Studium je zaměřeno na výuku budování kamerových, přístupových, bezpečnostních i biometrických systémů. Studenti se naučí navrhovat, realizovat a provádět následný servis bezpečnostní techniky.
Odborné předměty: základy elektrotechniky, elektrotechnologie, elektrická měření, elektronika, praktická elektronika, přenosové a informační systémy, technické kreslení, datové sítě – hardware, software, praxe
WWW stránky školy: https://www.ssemi.cz

V ČR se výuce spojené s informačními bezpečnostními systémy věnuje poměrně velké množství škol. Dle počtů nově otevíraných oborů tohoto směru a uchazečů o tyto obory je zřejmé, že je o tento směr výuky velký zájem. Vzhledem k rychle se rozvíjejícím technologiím a zvyšující se potřebě bezpečnostních systémů se tento obor jeví jako lukrativní.

2.1.2 Vysoké školy

Název školy: Univerzita Tomáše Bati ve Zlíně

Název oboru: Bezpečnostní technologie, systémy a management

Typ vzdělání, délka studia: bakalářské, 3 roky, možnost pokračování na magisterském studiu (specializace bezpečnostní technologie) i na doktorském typu studia

Nabízené odborné studijní předměty: datová bezpečnost, kriminalistické technologie, objektová bezpečnost – mechanické zabezpečení/elektronické prvky, technické prostředky bezpečnostního průmyslu, technologie detektivní činnosti, bezpečnostní management a krizové stavy a management jejich řízení ...

WWW stránky školy: https://www.utb.cz

Název školy: Technická univerzita Ostrava

Název oboru: Technická bezpečnost osob a majetku

Typ vzdělání, délka studia: bakalářské, 4 roky + navazující magisterské studium

Nabízené odborné studijní předměty: stroje, zařízení a technologie, technické kreslení, základy práva, bezpečnostní informatika, řízení systému fyzické bezpečnosti, mechanické zábranné systémy, zabezpečovací systémy, ochrana objektu, bezpečnost informací, kriminalistické systémy a technologie aj.

WWW stránky školy: https://www.vsb.cz

Název školy: Vysoké učení technické v Brně

Název oboru: Informační bezpečnost

Typ vzdělání, délka studia: bakalářské, 3 roky + navazující magisterské studium (2 roky) nebo doktorské studium (4 roky)

Nabízené odborné studijní předměty: komunikační technologie, právní nauka, základy informačních a komunikačních technologií, aplikovaná kryptografie, bezpečnost ICT, elektrotechnika, zabezpečovací systémy, číslicové zpracování signálů, konstrukce elektronických zařízení atd.

WWW stránky školy: https://www.vutbr.cz

V roce 2020 požádala Fakulta informatiky a managementu Univerzity Hradec Králové o udělení akreditace akademického bakalářského studijního programu Aplikovaná informatika se specializacemi Kybernetická bezpečnost a Softwarové inženýrství (v českém i anglickém jazyce). [19]

Výběr vysokých škol s výukou bezpečnostních systémů je značně omezený. Pokud chce absolvent střední školy vykonávat práci bezpečnostního technologa, tak není nutné pokračovat ve vysokoškolském studiu. V případě, že by rád zastával pozici například specialisty bezpečnostního a krizového řízení, je žádoucí, aby pokračoval ve studiu na některé takto zaměřené škole. Tyto vysoké školy mají také výhodu v tom, že jsou spojeny s dalšími směry – kriminalistikou, kybernetickou bezpečnostní, právem aj.

2.2 Číselníky profesí

Oficiální klasifikaci zaměstnání najdeme pod označením CZ-ISCO. Klasifikace CZ-ISCO je národní statistická klasifikace vypracována na základě mezinárodního standardu International Standard Classification of Occupations (ISCO-08), jehož tvůrcem je Mezinárodní organizace práce. [13] Díky této klasifikaci můžeme sledovat např. mzdovou úroveň vybraných zaměstnání. Práce s informačními bezpečnostními systémy spadá pod hlavní označení povolání „3 – Techničtí a odborní pracovníci“. Data k jednotlivým povoláním jsou čerpána z Národní soustavy povolání, která je spravována Ministerstvem práce a sociálních věcí ČR. [13]

2.2.1 Bezpečnostní technolog

CZ-ISCO 33434 Odborní pracovníci bezpečnostních systémů a ochrany údajů
Odborný směr: ochrana majetku, zdraví a osob
Odborný podsměr: technické bezpečnostní služby
Charakteristika a pracovní náplň: Bezpečnostní technolog tvoří návrhy technického zabezpečení objektů za účelem ochrany majetku, informací a osob a řídí jejich realizaci.

- Provádí analýzu a bezpečnostní posouzení zabezpečení majetku, informací a osob.
- Zpracovává návrhy technické ochrany majetku, informací a osob.
  Provádí zkoušky systémů požární signalizace, poplachových systémů a jiných zabezpečovacích systémů.
- Řídí servis a montáže požární signalizace, poplachových systémů a mechanického zabezpečení.

Kvalifikace k výkonu povolání:

- legislativní
  - povinné: vyhláška č. 202/1995 Sb., o požadavcích k zajištění bezpečnosti a ochrany zdraví při obsluze a práci na elektrických zařízeních při hornické činnosti a při činnosti prováděné hornickým způsobem
  - doporučené: činnost autorizovaného stavebního projektanta, činnost autorizovaného stavbyvedoucího
- školní
  - nejvhodnější: požární ochrana; střední vzdělání s maturitní zkouškou – obor elektrotechnika; střední vzdělání s maturitní zkouškou (bez vyučení) – obor elektrotechnika
  - vhodné: střední vzdělání s maturitní zkouškou – obory elektrotechnika; telekomunikační a výpočetní technika; střední vzdělání s maturitní zkouškou – obor telekomunikace; střední vzdělání s maturitní zkouškou (bez vyučení) – obor telekomunikace

2.2.2 Bezpečnostní referent

CZ-ISCO 34113 Odborní bezpečnostní pracovníci bezpečnostních a detektivních agentur

Odborný směr: ochrana majetku, zdraví a osob

Odborný podsměr: ostraha majetku a osob

Charakteristika a pracovní náplň: Bezpečnostní referent má v popisu práce

ostrahu a ochranu majetku i osob a jiných chráněných zájmů klienta dle rámcových pokynů a norem.

- Identifikuje personální, materiální a technické potřeby zabezpečení.
- Kontroluje vstup a pohyb osob, vjezd a výjezd vozidel.
- Provádí činnosti spojené se zajištěním ochrany zdraví, bezpečnosti práce a bezpečnosti informací.
- Zajišťuje činnosti k minimalizaci nebezpečí nebo redukci škody a ztrát na majetku a zdraví osob.
- Vede a vyhodnocuje služební záznamy, situační hlášení a protokoly.

Kvalifikace k výkonu povolání:

- nejvhodnější: střední vzdělání s maturitní zkouškou (bez vyučení) v oboru bezpečnostně právní činnost; střední vzdělání s maturitní zkouškou v oboru bezpečnostně právní činnost; požární ochrana
- vhodné: střední vzdělání s maturitní zkouškou (bez vyučení) v oboru obecně právní činnost; střední vzdělání s maturitní zkouškou (bez vyučení) v oboru provozní služby

2.2.3 Specialista bezpečnostního a krizového řízení

CZ-ISCO 21416 Specialisté v oblasti bezpečnostních systémů a ochrany údajů (kromě zabezpečení IT)

Odborný směr: ochrana majetku, zdraví a osob

Odborný podsměr: technické bezpečnostní služby

Charakteristika a pracovní náplň: Odborník v této pozici má na starosti bezpečnostní politiku organizace, formuje ji, řídí a dohlíží na její realizaci.

- Provádí posouzení bezpečnosti.
- Realizuje a obstarává provoz protipožárních technologií.
- Navrhuje a zavádí monitorovací a dohledové služby, spravuje bezpečnostní technologie.
- Posuzuje úroveň fyzické ochrany i administrativních bezpečnostních opatření.

- Formuluje bezpečnostní politiku firmy, definuje aktiva společnosti z hlediska potřeby jejich ochrany, provádí management rizik, provádí odborná školení zaměstnanců aj.

Kvalifikace k výkonu povolání:

- nejvhodnější: magisterský studijní program – obor požární ochrana a průmyslová bezpečnost; magisterský studijní program – technická bezpečnost majetku a osob
- vhodné: magisterský studijní program – obor bezpečnostně právní studia; magisterský studijní program – obor ochrana vojsk a obyvatel; bakalářský studijní program – obor požární ochrana a průmyslová bezpečnost

2.2.4 Bezpečnostní systémový analytik

CZ-ISCO 33434 Odborní pracovníci bezpečnostních systémů a ochrany údajů

Odborný směr: ochrana majetku, zdraví a osob

Odborný podsměr: technické bezpečnostní služby

Charakteristika a pracovní náplň: Bezpečnostní systémový analytik navrhuje bezpečnostní politiku firmy ve vztahu k aktivům.

- Připravuje postupy pro následnou správu poplachových, přístupových, kamerových, protipožárních i dalších systémů.
- Vymýšlí koncepce pro bezpečnost lidských zdrojů, fyzickou bezpečnost a zabezpečení úniků informací.

Kvalifikace k výkonu povolání: vyšší odborné vzdělání – obor požární ochrana a průmyslová bezpečnost; bakalářský studijní program – požární ochrana a průmyslová bezpečnost; informační technologie

2.2.5 Pracovník bezpečnostního dohledového IS

CZ-ISCO 25290 Specialisté v oblasti bezpečnosti dat a příbuzní pracovníci

Odborný směr: ochrana majetku, zdraví a osob

Odborný podsměr: technické bezpečnostní služby

Charakteristika a pracovní náplň: Pracovník bezpečnostního dohledového

centra informačních systémů obstarává dohled nad bezpečností chráněných informačních systémů.

- Nepřetržitě sleduje a vyhodnocuje výstupy ze systémů.
- Monitoruje a analyzuje mimořádné incidenty.
- Komunikuje s příslušnými osobami a navrhuje řešení aktuálních incidentů.
- Navrhuje způsoby předcházení možných událostí.

Kvalifikace k výkonu povolání:

- nejvhodnější: vyšší odborné vzdělání v oboru výpočetní technika a informační technologie
- vhodné: střední vzdělání s maturitní zkouškou (bez vyučení) v oboru výpočetní technika; informatické obory

Technik bezpečnostních systémů

podřízené specializace: technik poplachových systémů, technik požární signalizace

Odborný směr: ochrana majetku, zdraví a osob

Odborný podsměr: technické bezpečnostní služby

Charakteristika a pracovní náplň: Technik bezpečnostních systémů zařizuje montáže, uvádění do provozu, kontroly i servisy kamerových, komunikačních, přístupových, poplachových, řídicích a signalizačních systémů, které souvisejí s ochranou majetku, informací a osob.

- Montáž a zprovoznění EPZ a autonomní detekce požáru.
- Montáž a zprovoznění kamerových, poplachových a další systémů.
- Zřízení ústředen, dohledových a přijímacích center.
- Oprava, servis a údržba bezpečnostních systémů.

Kvalifikace k výkonu povolání: spojový mechanik – vhodné

2.3 Významné certifikace v oboru IBS

V oboru informačních bezpečnostních systémů existuje, stejně jako v jiných oborech, množství certifikací, kurzů či školení, které by mělo svědčit o odborných znalostech a dovednostech jejich držitele. Existuje však jen malé množství

mezinárodně uznávaných certifikátů, pro jejichž získání vynaloží uchazeč nemalé výdaje, ale hlavně měsíce příprav k jejich úspěšnému získání.

2.3.1 CPP

Certified Protection Professional vystavuje organizace ASIS. Jedná se o nejstarší bezpečnostní certifikát na světě a je považován za nejvyšší uznání v bezpečnostním průmyslu (správy zabezpečení). K získání certifikátu je nutné prokázat alespoň 9 let praxe z oblasti bezpečnosti nebo získat bakalářský a vyšší titul v oboru a nastřádat 7 let zkušeností. [4] Následně musí žadatel podstoupit zkoušku čítající 200 otázek složených ze 7 domén [4]:

- Bezpečnostní zásady a postupy (váha: 22 %)
- Podnikové zásady a postupy (váha: 15 %)
- Vyšetřování (váha: 9 %)
- Personální bezpečnost (váha: 11 %)
- Fyzická bezpečnost (váha: 16 %)
- Informační bezpečnost (váha: 14 %)
- Krizový management (váha: 13 %)

CPP certifikace stojí $335 členy ASIS a $485 ostatní žadatele [4]. Organizace ASIS také vytváří studijní materiály, pořádá vzdělávací kurzy, semináře, konference i setkání pro členy dané země. Snaží se tím o rozvoj bezpečnosti formou vzdělávání, certifikací atp.

PSP

PSP certifikát úzce souvisí s výše uvedeným CPP – vydává ho stejná organizace, ale je více zaměřený na fyzické bezpečnostní systémy a zavádění bezpečnostních opatření. K získání je potřeba mít 4 roky zkušeností s fyzickou bezpečností a bakalářské či vyšší vysokoškolské vzdělání. Zkouška trvá 2,5 hodiny a obsahuje 125 otázek ze tří domén: posouzení fyzické bezpečnosti, aplikace, design, a integrace systémů fyzického zabezpečení, implementace opatření fyzické bezpečnosti. Cena je jako u CPP certifikátu $335 pro členy ASIS a $485 pro ostatní žadatele. [4]

2.3.2 CISSP

Certified Information Systems Security Professional (CISSP) je celosvětově nejuznávanějším certifikátem v oblasti informační bezpečnosti. Řadí se k nejpřísnějším, nejnáročnějším a nejvyhledávanějším certifikacím v průmyslu IT. Certifikace spadá pod vedení neziskové organizace International Information System Security Certification Consortium. K úspěšnému absolvování zkoušky nestačí pouze rozsáhlé znalosti v oboru kybernetické bezpečnosti, ale i praktické zkušenosti v tomto oboru (minimálně 5 let práce ve 2 nebo více z 8 oblastí CISPP). Zkouška probíhá v angličtině, trvá 3 hodiny a obsahuje 100–150 otázek s možností volby z několika možností. Po absolvování zkoušky je odborník připraven zajišťovat: architekturu, navrhování, řízení a kontrolování bezpečnosti prostředí organizace. [5]

Zkouška zahrnuje 8 domén (okruhů) [5]:

- doména 1 – Zabezpečení a řízení rizik (váha: 15 %)
- doména 2 – Zabezpečení majetku (váha: 10 %)
- doména 3 – Bezpečnostní architektura a inženýrství (váha: 13 %)
- doména 4 – Komunikace a zabezpečení sítě (váha: 14 %)
- doména 5 – Správa identit a přístupu (IAM) (váha: 13 %)
- doména 6 – Posouzení a testování bezpečnosti (váha: 12 %)
- doména 7 – Bezpečnostní operace (váha: 13 %)
- doména 8 – Bezpečnostní požadavky na vývoj softwaru (váha: 10 %)

Cena CISSP se pohybuje okolo $699 [5]. K získání tohoto certifikátu se však většina lidí neobejde bez profesionálního školení, které probíhá po dobu cca 5 dní. Cena školení je přibližně 60 000 Kč bez DPH. Školení v ČR nabízí například tyto organizace: Počítačová škola GOPAS, Anywhere s.r.o., ALEF Training, PC-DIR.

2.3.3 ISO 27001

Norma ISO 27001 (Management bezpečnosti informací) je mezinárodně platný standard, jenž určuje požadavky řízení bezpečnosti informací. Jedná se o standard, který požaduje po organizaci, aby se všemi interními i sdílenými informacemi

zacházela tak, aby nedošlo k jejich odcizení, zneužití, ztrátě. Rovněž zaručuje zachování důvěrnosti, integrity i dostupnosti informací. Přínosy této normy tkví především v získání důvěry ostatních firem (obchodních partnerů) při sdílení informací s danou organizací. Dále dochází k zefektivnění činnosti týkající se klasifikace rizik souvisejících se zneužitím nebo ztrátou dat, snížení rizik vyšších nákladů při možné neočekávané události, redukci nákladů na údržbu a rozvoj IT ve firmě. [8]

Zavedení ISO 27001 v organizaci zaručuje pokrytí požadavků zákazníků a zákonů v oblastech [9]:

- GDPR
- zneužití
- poškození/požár
- vandalismus
- porušení osobních údajů
- kybernetické zločiny
- virové úroky aj.

Norma 27001 se uděluje na základě podrobného auditu firmy. Ke splnění podmínek pro získání standardu lze využít podrobné dokumentace, jejíž cena je 445 Kč/norma včetně změn. Dále pak školení, jež se pohybuje kolem 25 000 Kč. V ČR školení nabízí mnoho organizací, například: 3EC International s.r.o., CIS s.r.o., AZ Cert EU s.r.o., CERTLINE s.r.o.

2.4 Aktuální stav trhu práce

Na základě informací zveřejňovaných na webových stránkách Českého statistického úřadu lze říct, že byla situace na trhu práce v minulých letech v oblasti informačních bezpečnostních systémů v České republice spíše nepříznivá (pro standardní povolání – celková poptávka nepokrývala nabídku). Opakem tomu je u vyšších pracovních pozic, u kterých je požadováno vysokoškolské vzdělání či dlouhodobá praxe v oboru. Dlouhodobě příznivá situace pro uchazeče o práci v oboru je v krajích Vysočina, Pardubickém a Královéhradeckém. Nepříznivá situace pak například v kraji Středočeském.

2.4.1 Nabídka a poptávka

Z dat zveřejněných na stránkách Ministerstva práce a sociálních věcí ČR lze vyčíst počty nabídek i poptávek z většiny krajů ČR. Tato práce zobrazuje údaje týkající se klasifikace CZ-ISCO 33434 Odborní pracovníci bezpečnostních systémů a ochrany údajů z roku 2018 a 2019, protože uplynulý rok 2020 byl ovlivněn pandemií covid-19, která trh práce výrazně ovlivnila. Statistiky nabídky a poptávky pro Hlavní město Praha a Jihomoravský kraj nejsou k dispozici. V konkrétních číslech jednotlivých krajů jsou zaneseny všechny hodnoty nabídek a poptávek, které byly daný rok zveřejněny (tj. i opakující se nabídky/poptávky).

Nejvyšší poptávka po pracovní síle v oblasti IBS byla v obou zobrazených letech jednoznačně v Kraji Vysočina – nabídka práce zde nepokrývala ani polovinu poptávky. Nejpříznivější situace (rozdíl poptávky a nabídky) pro uchazeče o zaměstnání byla v krajích: Vysočina, Královéhradecký, Pardubický. Naopak nejméně příznivá situace byla ve sledovaných letech ve Středočeském kraji. Konkrétní údaje zobrazují tyto tabulky:

Tabulka 2: Nabídka a poptávka práce v roce 2018

	Nabídka	Poptávka
Jihočeský kraj	9	2
Karlovarský kraj	16	18
Kraj Vysočina	5	26
Královéhradecký kraj	4	22
Liberecký kraj	17	14
Moravskoslezský kraj	21	2
Olomoucký kraj	14	10
Pardubický kraj	10	17
Plzeňský kraj	7	9
Středočeský kraj	31	2
Ústecký kraj	4	1
Zlínský kraj	10	5

Zdroj: [2]

Tabulka 3: Nabídka a poptávka práce v roce 2019

	Nabídka	Poptávka
Jihočeský kraj	13	5
Karlovarský kraj	15	0
Kraj Vysočina	12	25
Královéhradecký kraj	1	12
Liberecký kraj	14	3
Moravskoslezský kraj	10	19
Olomoucký kraj	1	12
Pardubický kraj	4	15
Plzeňský kraj	12	13
Středočeský kraj	23	1
Ústecký kraj	8	1
Zlínský kraj	15	1

Zdroj: [2]

2.4.2 Finanční ohodnocení

Veškeré údaje pro níže uvedená povolání jsou čerpány z webových stránek Národní soustavy povolání, což je otevřená databáze povolání spravovaná Ministerstvem práce a sociálních věcí ČR. Tabulka zobrazuje střední hodnoty a rozmezí středních hodnot mezd (soukromý sektor) i platů (státní sektor). Konkrétní hodnoty jsou udávané většinou jen pro nadřazenou kategorii CZ-ISCO, a tudíž jsou pro uvedená povolání pouze orientační.

Všechny hodnoty jsou uvedeny v českých korunách.

Tabulka 4: Finanční ohodnocení vybraných povolání v roce 2019

	Mzda			Plat		
	Střední hodnota	**Od**	**Do**	**Střední hodnota**	**Od**	**Do**
Bezpečnostní technolog (CZ-ISCO 33434)	40 616	24 240	75 148	37 492	30 098	50 540
Bezpečnostní referent (CZ-ISCO 3411)	29 290	16 065	71 023	34 939	26 141	49 866
Specialista bezpečnostního a krizového řízení (CZ-ISCO 21416)	55 150	34 304	90 430	48 384	34 483	75 002
Bezpečnostní systémový analytik (CZ-ISCO 33434)	40 616	24 240	75 148	37 492	30 098	50 540
Pracovník bezpečnostního dohledového IS (CZ-ISCO 2529)	70 811	45 022	125 212	46 434	34 198	69 717

Zdroj: [13]

2.5 Průzkum požadavků zaměstnavatelů

V rámci kapitoly analýzy trhu práce bylo osloveno několik firem, které aktuálně působí v oblasti IBS. Cílem průzkumu bylo zjistit, jaké služby firmy nejčastěji poskytují, jaké vzdělání u uchazečů o práci preferují a zda by přijaly i čerstvého absolventa. Stěžejní otázky zjišťovaly, jaké teoretické znalosti a praktické dovednosti zaměstnavatelé očekávají od svých budoucích zaměstnanců a jaké jsou současné trendy v oblasti IBS. Dále respondenti zodpovídali, zda a případně kolik nových zaměstnanců v uplynulých 3 letech přijali, a jestli při hledání nových posil přihlíží na certifikace či školení a kurzy. Odpovědi

na tyto otázky slouží jako podklady pro následující kapitolu, která hodnotí výuku IBS na fakultě ekonomicko-správní Univerzity Pardubice, a na jejichž základě byly vytvořeny doplňkové studijní materiály k podpoře této výuky.

K uskutečnění sběru odpovědí byla použita metoda dotazníkového šetření, ve které respondenti zodpovídali 12 otázek. Šetření se zúčastnilo celkem 11 respondentů, zastupující firmy z různých krajů ČR, různých velikostí, které poskytují komplexní služby spojené se zabezpečovací technikou. Mezi tyto organizace, které si přály zveřejnit své jméno, patří např.: SAFECOM s.r.o., MICROCOMP Plus, s.r.o., elektronickésystémy s.r.o., Jan Chmelař – CMELDA alarms, ELSI CZ s.r.o., FOXDOT s.r.o. či Sistel International. Mezi tázanými disponují menší firmy, které mají do 5 zaměstnanců. Jsou zde i zástupci firem, kteří mají 6–10 zaměstnanců, 11–15 zaměstnanců nebo také 16 a více zaměstnanců.

První část průzkumu byla zaměřena na zjištění jednotlivých a nejčastěji poskytovaných služeb, které firmy nabízí. Všechny tázané firmy zajišťují kombinaci služeb PTZS a CCTV. Více než polovina firem nabízí s těmito službami i elektronickou požární signalizaci. Další nejčastěji nabízené služby jsou detektory narušení, perimetrické detekční systémy, mechanické zábrany či strukturované kabelážní systémy a domácí telefony. Za nejčastěji žádané a poskytované služby jsou jednoznačně označeny kamerové systémy s poplachovým a tísňovým zabezpečovacím systémem. Každá organizace musela označit jen jednu nejvíce poskytovanou službu – 6 firem označilo CCTV, zbylých 5 označilo PTZS.

Následně bylo zjišťováno, jaké vzdělání organizace preferují (mohli vybrat i více odpovědí), zda přijímají i čerstvé absolventy a zda jsou ochotni si nového zaměstnance zaškolit, či spoléhají na jeho znalosti a dovednosti. Celkem 9 respondentů by upřednostnilo střední vzdělání s maturitní zkouškou před jinými formami vzdělání. Střední vzdělání s výučním listem preferuje pět tázaných firem. Dvě firmy by raději přijaly uchazeče s vyšším odborným či vysokoškolským vzděláním. Pouze dvě organizace z jedenácti by absolventa nepřijaly.

Naopak 3 firmy absolventy přijímají, a dokonce je preferují. Zbylých 6 tázaných by sice absolventa přijalo, nýbrž nepreferovalo. Překvapivý výsledek měla otázka, zda firmy spoléhají na dostatečné znalosti a dovednosti nového zaměstnance, nebo zda si ho raději zaškolí sami. Jen 3 organizace by nerady zaměstnance zaškolovaly, zbylých 9 si rádo nováčka zaškolí a naučí ho vše, co bude v dané práci potřebovat.

Dále se průzkum zaobíral otázkami: kolik nových zaměstnanců organizace přijaly v posledních 3 letech a zda tyto organizace přihlížejí při výběru nových pracovníků na certifikace/školení/kurzy. Z průzkumu vyplývá, že 5 firem nepřijalo za poslední uplynulé 3 roky žádnou novou posilu týmu. Ve všech těchto případech se jednalo o rodinné či malé firmy. Zbylé organizace přijaly od 1 do 5 nových pracovníků. K certifikacím, školením nebo kurzům přihlížejí 2 firmy z 11. První certifikací, která by u dané firmy uchazeče zvýhodnila, je EZS certifikace v jakékoliv podobě. Druhým zvýhodňujícím prvkem je osvědčení podle vyhlášky č. 50/1978 Sb. (odborná způsobilost v elektrotechnice) – nejčastěji získané na základě absolvování studia v elektro oboru.

Jaké teoretické znalosti by měl uchazeč mít? Zde se nejčastěji objevovaly tyto odpovědi:

- základy PC sítí, práce s VLAN, programování, obecně přesah do IT oborů,
- automatizace,
- základní principy zapojení (pravidla pro instalaci systémů), znalost základních obvodů,
- všeobecný přehled v oboru, technický přehled,
- elektroinstalace,
- představa o fungování slaboproudé elektroniky a její využití v praxi,
- znalost měřicí techniky,
- zájem o obor.

A jaké praktické dovednosti by měl uchazeč ovládat?

- montážní a manuální zručnost, technické dovednosti,
- orientování se ve stavebních výkresech,
- řešení kabelových rozvodů,
- pájení, drobné „modelářské“ práce, práce s elektrickým nářadím,
- práce s PC, nastavení připojení k internetu,
- programování ústředen a jejich komponent.

Jaké jsou současné trendy v oblasti bezpečnostních systémů?

- AI kamerové systémy,
- smart systémy,
- instalace EZS s ovládáním přes mobil a napojení na chytrou domácnost,
- snímání obličeje, snímání registračních značek automobilů,
- monitoring a ovládání všech bezpečnostních systémů pomocí jedné aplikace,
- inteligentní videoanalýza u CCTV, sledování objektů,
- různé způsoby automatizace.

3 TVORBA STUDIJNÍCH MATERIÁLŮ

Poslední kapitola této práce je zaměřena na porovnání výuky informačních bezpečnostních systémů na Fakultě ekonomicko-správní Univerzity Pardubice s aktuálními požadavky zaměstnavatelů, vyplývající z výše uvedeného průzkumu, a nabídek práce zveřejněných na webových stránkách úřadu práce. Dále tato kapitola obsahuje popis doplňkových studijních materiálů, které byly v rámci práce vytvořeny a mohou sloužit k doplnění výuky předmětu Úvod do informačních bezpečnostních systémů.

3.1 Výuka informačních bezpečnostních systémů na FES UPa

Oblast informačních bezpečnostních systémů je na Fakultě ekonomicko-správní Univerzity Pardubice (FES UPa) vyučována v rámci oboru Informační a bezpečnostní systémy v prezenční i kombinované formě. Je obsahem předmětu Úvod do informačních bezpečnostních systémů, v prezenční formě označeném jako FUIBS, v kombinované formě jako CUIBS. Tento předmět se na FES UPa vyučuje od akademického roku 2019/2020, po úpravách sylabu předmětu předcházejícího Úvod do IBS, a jeho cílem je seznámit studenty s problematikou IBS a v obecné rovině s problematikou soukromých bezpečnostních služeb. Po úspěšném absolvování předmětu student umí definovat základní pojmy z oblasti soukromých bezpečnostních služeb a bezpečnostního průmyslu, popsat základní problematiku hlídacích služeb se zaměřením na ochranu osob a majetku, popsat základní metody a nástroje využívané bezpečnostními specialisty v oblasti soukromých detektivních služeb a konkurenčního zpravodajství. Hodnocení upraveného předmětu studenty je velice pozitivní. Studenti ocenili především ucelenou a promyšlenou koncepci předmětu, poskytnuté množství literatury a technického vybavení, zajímavě pojaté prezentace či srozumitelnost výkladu. Nejvíce však ocenili nadšení a přístup vyučujících, kteří jim bezpochyby studium tohoto předmětu zpříjemnili a ulehčili.

Hlavním kritériem pro přijetí uchazeče je dle aktuálních nabídek práce a i výše

popsaného šetření všeobecný přehled v oboru, což předmět FUIBS jednoznačně splňuje. Dále se v podmínkách přijetí často objevuje předpoklad přesahu vědomostí do IT oborů, především fungování počítačových sítí a základy programování. I tento předpoklad je splněn díky ostatním odborným předmětům, které se na daném oboru vyučují. Dalším požadavkem bývá schopnost tvořit a orientovat se v technických výkresech a jiné dokumentaci. Technické kreslení sice v osnovách zmíněného studijního oboru není, ale univerzita umožňuje studovat i předměty z jiných fakult. Je tedy možné si tento předmět zapsat jako volitelný a docházet na výuku např. na Dopravní fakultu Jana Pernera. Ostatní požadavky typu znalosti principů zapojení, základních obvodů, práce se slaboproudou technikou či automatizace nejsou předmětem osnov oboru, nýbrž oborů elektrotechnických. V případě, že by se student rozhodl studovat tuto problematiku více do hloubky, ale přitom by chtěl studovat předměty oboru Informační a bezpečností systémy, je zde opět možnost zapsat si tyto předměty na jiné fakultě, v tomto konkrétním případě na fakultě elektrotechniky a informatiky.

3.2 Studijní materiály

Součástí této bakalářské práce jsou doplňkové studijní materiály zaměřené na trendy v oblasti informačních bezpečnostních systémů. Témata byla zvolena na základě provedeného dotazníkového šetření a rozhovoru s dlouholetým pracovníkem v oblasti IBS. Těmito tématy jsou:

- kamerové systémy a umělá inteligence – v rámci této kapitoly jsou popsány nejnovější trendy vývoje inteligentní videoanalýzy,
- vzdálené ovládání informačních bezpečnostních systémů pomocí aplikace,
- chytrá domácnost a informační bezpečnostní systémy,
- budoucnost informačních bezpečnostních systémů.

Při studiu materiálů se předpokládá základní znalost technologií IBS a s ní související terminologie. Proto mohou materiály sloužit pouze jako doplňkové nebo mohou být náplní poslední přednášky předmětů FUIBS a CUIBS.

ZÁVĚR

Cílem této bakalářské práce bylo vytvořit podklady pro výuku informačních bezpečnostních systémů. Vytvořené studijní materiály mají za úkol seznámit studenty předmětů FUIBS a CUIBS vyučované na Fakultě ekonomicko-správní Univerzity Pardubice s aktuálními trendy v oblasti informačních bezpečnostních systémů. Dílčím cílem bylo vytvořit rešerši informačních bezpečnostních systémů a zanalyzovat trh práce včetně dotazníkového šetření zabývajícího se požadavky zaměstnavatelů v oboru IBS na budoucí zaměstnance.

Z analýzy trhu práce vyplývá, že dlouhodobě příznivá situace pro uchazeče o práci v oboru IBS je v Kraji Vysočina, Pardubickém kraji a Královéhradeckém kraji. Obecně je v tomto oboru u standardních povolání přebytek nabídky nad poptávkou. Aktuálně je spíše nedostatek zaměstnanců vyšších pracovních pozic, po kterých je vyžadováno vysokoškolské vzdělání či dlouholetá praxe.

Průzkumu požadavků zaměstnavatelů se zúčastnilo celkem 11 firem. Tyto firmy se zabývají poskytováním komplexních služeb v oblasti IBS. Většina tázaných by upřednostnila střední vzdělání s maturitní zkouškou před jinými formami vzdělání. Pouze 2 organizace z 11 by nepřijaly čerstvého absolventa. Devět respondentů uvedlo, že si rádi novou posilu týmu zaškolí a naučí ho vše, co bude v dané práci potřebovat. Z teoretických znalostí by měl mít uchazeč: přehled v IT oboru, znalost automatizace a elektroinstalace, všeobecný technický přehled či znalost základních principů zapojení a základních obvodů. Z praktických dovedností se od uchazeče očekává montážní a manuální zručnost, orientace ve stavebních výkresech, programování nebo řešení kabelových rozvodů.

Hlavní část bakalářské práce tvoří příloha v podobě doplňkových studijních materiálů na téma Trendy v oblasti informačních bezpečnostních systémů, které byly vytvořeny na základě výsledků dotazníkového šetření a ve spolupráci s odborníkem na oblast IBS. Materiály popisují kamerové systémy využívající

umělou inteligenci, vzdálené ovládání nástrojů IBS pomocí aplikace, smart homes a IBS, budoucnost informačních bezpečnostních systémů.

Cíl bakalářské práce byl splněn. Studijní materiály seznámí studenty s moderními nástroji využívanými v oblasti bezpečnosti, kterou studují. Průzkum požadavků zaměstnavatelů může sloužit jako podklad pro zkvalitnění výuky IBS na FES UPa tak, aby tato výuka co nejvíce odpovídala požadavkům trhu práce.

POUŽITÁ LITERATURA

[1] Alarm Receiving Centres. *CoESS* [online]. [cit. 2021-03-31]. Dostupné z: https://www.vigilanzaprivataonline.com/download/Dossier/libro-bianco-coess-telesorveglianza.pdf

[2] Analýza poptávky po pracovní síle a nabídky pracovní síly. *Ministerstvo práce a sociálních věcí* [online]. [cit. 2021-03-31]. Dostupné z: https://data.mpsv.cz/web/data/vizualizace13

[3] BURDA, Karel. *Základy elektronických zabezpečovacích systémů*. Brno: Akademické nakladatelství CERM, 2017. ISBN 978-80-7204-967-7.

[4] Certified Protection Professional (CPP). *ASIS International* [online]. Alexandria, Virginia: ASIS International, ©2020 [cit. 2021-03-31]. Dostupné z: https://www.asisonline.org/certification/certified-protection-professional-cpp

[5] CISSP – The World's Premier Cybersecurity Certification. *(ISC)²* [online]. (ISC)², ©1996-2021 [cit. 2021-03-31]. Dostupné z: https://www.isc2.org/Certifications/CISSP

[6] DOBDA, Luboš. *Ochrana dat v informačních systémech*. Praha: Grada, 1998. ISBN 80-7169-479-7.

[7] Dohledové centrum. *Interconnect* [online]. Křenice: Interconnect, 2018 [cit. 2021-03-31]. Dostupné z: https://business.interconnect.cz/bezpecnostni-systemy/dohledove-centrum

[8] ISO 27001. *Iso.cz* [online]. [cit. 2021-03-31]. Dostupné z: http://www.iso.cz/iso-27001

[9] ISO 27001. *NQA* [online]. NQA, ©2021 [cit. 2021-03-31]. Dostupné z: https://www.nqa.com/cs-cz/certification/standards/iso-27001

[10] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. aktualiz. vyd. Blatná: Blatenská tiskárna, 2006. ISBN 80-902938-2-4.

[11] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.

[12] Moderní docházkové a přístupové systémy. *ATP Journal* [online]. HMH, ©2021 [cit. 2021-03-31]. Dostupné z: https://www.atpjournal.sk/buxus/docs/idb%20journal%202%202011%2021-23.pdf

[13] *Národní soustava povolání* [online]. Praha: Ministerstvo práce a sociálních věcí, ©2017 [cit. 2021-03-31]. Dostupné z: https://nsp.cz

[14] Osm tipů na vykradení domu od profesionálních zlodějů. *Jablotron* [online]. Jablotron, ©2021 [cit. 2021-03-31]. Dostupné z: https://www.jablotron.com/cz/o-jablotronu/blog/chytre-tipy/8-tipu-na-vykradeni-domu-od-profesionalnich-zlodeju

[15] Pojem informačního systému. *MUNI FI* [online]. Brno: MUNI FI [cit. 2021-03-31]. Dostupné z: https://www.fi.muni.cz/~smid/mis-infsys.htm

[16] Předpisy související s poskytováním technických služeb k ochraně majetku a osob. In: *Ministerstvo vnitra České republiky* [online]. Praha: Ministerstvo vnitra České republiky, ©2021 [cit. 2021-03-31]. Dostupné z: https://www.mvcr.cz/clanek/dokumenty-prevence-aktuality-predpisy-souvisejici-s-poskytovanim-technickych-sluzeb-k-ochrane-majetku-a-osob.aspx

[17] ŘÍHA, Milan, Ladislav SIEGER a Pavel PIKOLA. *Bezpečnostní systémy 1. díl.* Čtvrté aktualizované. Praha: Námořní akademie České republiky, 2011. ISBN 978-80-87103-32-6.

[18] VEĽAS, Andrej. *Elektrické zabezpečovacie systémy* [online]. Žilina: EDIS, 2010 [cit. 2021-03-31]. ISBN 978-80-554-0224-6. Dostupné z: http://fsi.uniza.sk/kbm/wp-content/uploads/2013/12/Velas_EZS.pdf

[19] Zápis z Vědecké rady FIM UHK konané dne 9.12. 2020. In: *Univerzita Hradec Králové* [online]. Hradec Králové: Univerzita Hradec Králové, ©2021[cit. 2021-03-31]. Dostupné z: https://www.uhk.cz/file/edee/fakulta-informatiky-a-managementu/fim/samospravne-organy/vedecka-rada/2020/zapis-vr-fim_9_12_2020.pdf

SEZNAM PŘÍLOH

Příloha A *Doplňkové studijní materiály*

Trendy v oblasti informačních bezpečnostních systémů

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

IS	Informační systém
AI	Umělá inteligence (z angl. Artificial Intelligence)
PIN	Osobní identifikační číslo (z angl. Personal Identification Number)
VIP	Velmi důležitá osoba (z angl. Very Important Person)
CCTV	Kamerový systém (z angl. Closed-circuit television)
IBS	Informační bezpečnostní systémy
OS	Operační systém (z angl. Operating System)

PŘEDMLUVA

Tyto doplňkové studijní materiály vznikly v rámci bakalářské práce a dávají si za úkol seznámit studenty Fakulty ekonomicko-správní Univerzity Pardubice s aktuálními trendy v oblasti informačních bezpečnostních systémů.

Oblast těchto technologií se neustále rozvíjí a stává se běžnou součástí našich životů. To má v jistých směrech svá pozitiva. Technologie s nástroji umělé inteligence dokážou například včas identifikovat nadcházející nebezpečí a zabránit tak neočekávané hrozbě. Projekty chytrých domů s komplexním zabezpečením ovládaným přes aplikaci v mobilu zase umožní pohodlné a rychlé vyhodnocování hrozeb, i když jste zrovna na druhém konci světa. Tyto technologie s sebou ale rovněž přináší negativa, která bychom mohli spatřovat především ve ztrátě soukromí.

Obsah vznikl na základě poskytnutých informací a materiálů od zaměstnance společnosti Euroalarm spol. s r.o. Pokud není uvedeno jinak, informace pocházejí především z prezentací firem AxxonSoft a Hikvision.

1 PROČ STUDOVAT INFORMAČNÍ BEZPEČNOSTNÍ SYSTÉMY?

Proč studovat informační bezpečnostní systémy? Jak jistě víte, zabezpečovací technika se dnes nachází opravdu všude a dochází k jejímu neustálému rozvoji. S tímto rozvojem stoupá i zájem o odborníky v této oblasti. U vyšších pozic je vyžadováno vysokoškolské vzdělání, i proto jste si pravděpodobně vybrali studium na této škole. Významnost pracovní pozice pochopitelně ovlivňuje výši finanční odměny. Tabulka zobrazuje střední hodnoty a rozmezí středních hodnot mezd (soukromý sektor) i platů (státní sektor). Konkrétní hodnoty jsou udávané většinou jen pro nadřazenou kategorii CZ-ISCO, a tudíž jsou pro uvedená povolání pouze orientační. Všechny hodnoty jsou uvedeny v českých korunách.

Tabulka1: Finanční ohodnocení vybraných povolání v roce 2019

	Mzda			**Plat**		
	Střední hodnota	**Od**	**Do**	**Střední hodnota**	**Od**	**Do**
Bezpečnostní technolog (CZ-ISCO 33434)	40 616	24 240	75 148	37 492	30 098	50 540
Bezpečnostní referent (CZ-ISCO 3411)	29 290	16 065	71 023	34 939	26 141	49 866
Specialista bezpečnostního a krizového řízení (CZ-ISCO 21416)	55 150	34 304	90 430	48 384	34 483	75 002
Bezpečnostní systémový analytik (CZ-ISCO 33434)	40 616	24 240	75 148	37 492	30 098	50 540
Pracovník bezpečnostního dohledového IS (CZ-ISCO 2529)	70 811	45 022	125 212	46 434	34 198	69 717

Zdroj: [4]

2 KAMEROVÉ SYSTÉMY A UMĚLÁ INTELIGENCE

Asi nejvíce se rozvoj týká softwarových nástrojů, které se implementují do kamerových systémů. Ty přitom využívají umělou inteligenci (AI) a v oblasti bezpečnosti zastupují nejžádanější funkce. Nástroje slouží především k identifikaci neočekávaných hrozeb, které by mohly způsobit újmu na životech, zdraví či majetku. Dále mohou být navrženy pro analytické účely nebo pro ulehčení každodenních aktivit.

2.1 Analýza chování

Nástroje analýzy chování jsou založeny na principu hlubokého učení a slouží k rozpoznávání potenciálně nebezpečných situací na základě behaviorálního chování (konkrétních lidských pozic). Umožňují rozpoznávání anomálního, podezřelého a deviantního chování. Může se jednat například o osobu držící zbraň, osobu krčící se u bankomatu, zvednuté paže detekovaných osob či detekci ležící osoby, upozorňující na její zhoršený zdravotní stav. Všechny tyto události jsou detekovány v reálném čase, což umožňuje okamžitou reakci příslušných složek, a tím i minimalizování rizik. Výhodou použití těchto nástrojů je také to, že příslušná osoba nemusí hlídat permanentně všechny připojené kamerové záznamy, nýbrž jen ty záznamy, které jsou označeny za neobvyklé a na něž je operátor včas upozorněn.

Obrázek 12: Detekce střelce

Zdroj: prezentace AxxonSoft

2.2 Filtr neuronové sítě

Filtr neuronové sítě se využívá při funkci sledování objektů. Filtr zajistí přesné detekování konkrétních typů pohybujících se objektů – lidé, vozidla aj. Díky přesnosti dokáže filtr odfiltrovat falešné poplachy v rušných scénách (velké množství pohybujících se objektů v jednom čase na stejném místě). Princip této technologie je následující: nejprve sledovač objektů detekuje všechny pohybující se objekty. Následně část záznamu s objektem předá neuronové síti za účelem analýzy. Veškeré objekty, které neodpovídají předem definovanému typu, jsou ignorovány a nespouštějí alarm. Příkladem použití může být situace, při které se spustí alarm, pokud neoprávněná osoba vstoupí do nebezpečné vymezené oblasti.

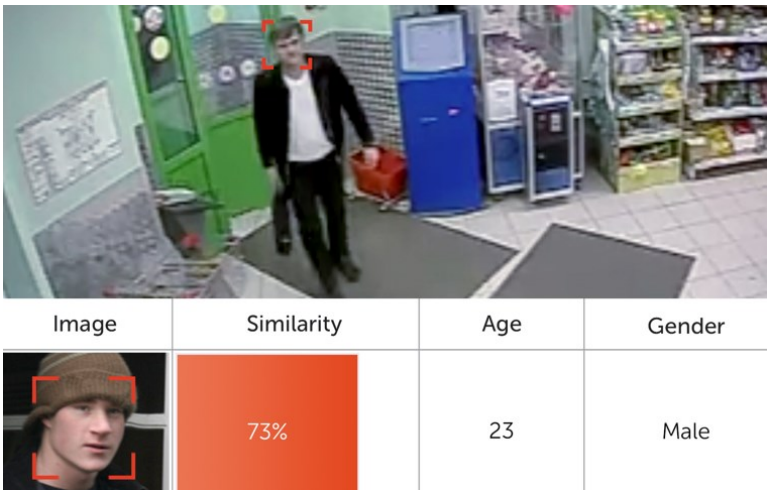
Obrázek 3: Filtr neuronové sítě

Zdroj: prezentace AxxonSoft

2.3 Rozpoznání obličejů a registračních značek automobilů

Funkce rozpoznávání obličejů pomalu ale jistě nahrazuje jiné, zastaralejší identifikační metody. Není již nutné vlastnit čipovou kartu, zadávat PIN či poskytovat otisk prstu. Rozpoznávání obličeje je největším trendem především v oblasti řízení docházky a přístupu. Tato funkce funguje na principu hlubokého učení a nejnovější technologie dokážou rozpoznat osobu již za 0,2 sekundy, a to i při špatném osvětlení či v naprosté tmě [2]. Vše jde samozřejmě ovládat

dálkově pomocí mobilní aplikace. Hlavní funkcí rozpoznávání obličejů je porovnávání s podobami, které jsou předem zařazeny buď na seznam pozitivní, nebo negativní. To umožňuje na jedné straně identifikovat např. VIP zákazníka, aby mu mohly být poskytnuty ty nejlepší služby, a na straně druhé identifikovat známé zloděje, hledané osoby apod. Detekce osoby se může docílit dvěma způsoby – buď můžeme vybranou osobu (její obličej) označit přímo ve videozáznamu, anebo do systému nahrajeme obrázek osoby z mobilního telefonu či jiného externího zařízení. Pokud systém rozpozná shodu, spustí se předem stanovený scénář – upozornění obsluhy, výpis informací o dané osobě aj.



Obrázek 4: Rozpoznávání obličeje

Zdroj: prezentace AxxonSoft

Podobně je tomu u rozpoznávání registračních značek automobilů. K rozpoznání dojde i u jedoucích automobilů a značka je okamžitě porovnána s čísly z databáze. Ve většině případů nejsou zaznamenávána všechna vozidla, ale jen ta, která projíždí určitým úsekem či zónou. Kromě registrační značky je také zaznamenán obraz vozidla, datum, směr vozidla aj. Při nalezení shody je jako u rozpoznávání obličejů spuštěn nadefinovaný scénář.

2.4 Detekce ohně a kouře s využitím umělé inteligence

Detekce ohně a kouře na bázi umělé inteligence (inteligentní detekce požáru a kouře) se využívá v případech, ve kterých jsou jiné typy senzorů neúčinné, příkladem může být využití na otevřených prostranstvích. Tyto technologie zajistí včasné detekování požáru, což vede k výraznému snížení škod. Na otevřených prostranstvích se využívají 360stupňové panoramatické kamery, které poskytují nejširší záběr sledování, a kromě samotného požáru zachytí i stoupající kouř. K identifikaci se nevyužívá jen znalost pohybů a barev připomínající plameny, ale také charakteristika povrchových vzorů, oblak či světelnost. Výhoda videodetekcí kouře, oproti běžným hlásičům požáru, je kromě využití ve velkých či otevřených prostorech také v rychlosti detekce. Zatímco inteligentním nástrojům stačí kouř pouze „zahlédnout“, klasické detektory kouře potřebují, aby kouř vnikl do jejich vyhodnocovací jednotky. Tím je také snížena potřeba množství senzorů, které oblast střeží[9].

2.5 Využití AI CCTV v obchodních centrech

Stále rozšířenějším trendem v obchodních zařízeních je **real-time dohled**, a to nejen kvůli zachycení kriminality ze strany zákazníků, ale i podvodného jednání zaměstnanců. Kamerové systémy s AI se propojí se systémem pokladen a tím je možné v reálném čase sledovat provedené transakce. Pokud je pak např. provedeno storno po odbavení zákazníka, je tato událost hlášena příslušné osobě a vyšetřována. Díky propojení systémů pokladen a CCTV lze vyhledat na záznamu konkrétní naskenované produkty. Pokročilejší technologie dokážou rozpoznat zboží, které je vyloženo na pokladním páse, a pokud toto zboží projde přes pokladnu, ale není naskenováno do systému, je opět spuštěn nadefinovaný scénář.

Nástroj správy front detekuje počet lidí ve frontách. To umožňuje nejen zlepšit zákaznickou péči (informování vedoucího prodejny, otevření další pokladny), ale i dlouhodobě pomoci procesu řízení lidských zdrojů – na základě dat lze například plánovat směny. Tyto nástroje bývají velmi přesné, detekují

pouze ty osoby, které stojí ve vybrané oblasti po určitou dobu. Osoby, které oblastí jen prochází, do počtu nezapočítávají.

Počítadlo návštěvníků nevyužívají jen obchody, ale i muzea, hotely a jiné instituce. Tento nástroj slouží k počítání osob, které vstupují či opouštějí obchod nebo konkrétní vymezenou oblast. Shromážděné informace slouží k nejrůznějším analýzám (celková návštěvnost, kdy je nejvyšší návštěvnost, jak dlouho se zde lidé průměrně zdržují, která oblast je nejoblíbenější) a odhadům (jaký bude očekávaný prodej). Pomáhají také s vylepšením marketingu. Přesnost těchto nástrojů bývá 95–97 %.

Pro marketingové účely jsou využívány **nástroje rozpoznávání obličeje pro odhad věku a pohlaví návštěvníků**. Tyto údaje slouží k podrobným analýzám a úpravám fungování organizací, na jejichž základě mohou obchody měnit sortiment aj.

Dalším oblíbeným trendem je tzv. **heat map**. Heat map představuje grafickou reprezentaci aktivity návštěvníků v různých částech obchodu (počet návštěvníků/čas strávený na daném místě). Na mapě můžeme sledovat buď všechny objekty, anebo si vybereme pouze některé pomocí kritérií forenzního vyhledávání. Tím mohou obchody vyhodnotit, u kterého zboží tráví zákazníci nejvíce času. Na základě těchto map často dochází k reorganizaci interiérů, aby museli zákazníci procházet okolo méně chtěného zboží až do zadní části obchodu, kde se nachází zboží, o které mají zájem.

Obrázek 5: Heat map

Zdroj: prezentace AxxonSoft

2.6 Další trendy s využitím umělé inteligence a CCTV

Mezi další funkce řadíme **sledování a počítání konkrétních typů objektů**, přičemž se nemusí jednat pouze o lidi a vozidla, ale prakticky o cokoliv, co nás napadne. Dále funkce **Tag&Track** umožňuje sledovat konkrétní objekt napříč propojeným kamerovým systémem.

Funkce **detekování opuštěných objektů** napomáhá při hledání ztracených věcí či jejich majitelů, to se hodí především na rušných místech typu vlakové nádraží/letiště.

Velice zajímavou funkcí je **rozpoznávání potenciálně nebezpečných situací**. Příkladem této funkce je vyhlášení poplachu, pokud na staveniště vstoupí osoba bez ochranné helmy, nebo automatická detekce zvýšené vodní hladiny, která přesáhne určitou hodnotu na stupnici.

K ulehčení vyhledávání konkrétních situací či objektů můžeme využít funkci **inteligentního vyhledávání**, kdy nám systém zobrazí např. jen události, při kterých byl spuštěn alarm; záznamy s konkrétní osobou; události v daném časovém rozmezí. K podobnému účelu slouží i funkce **komprese času**, díky které si můžeme hodiny záznamu zobrazit v pár sekundách. I v této funkci lze použít vyhledávání, takže si můžeme zobrazit všechny objekty v jednom obrazu, i když se na sledovaném místě pohybovaly v různou dobu.

V rámci ochrany osobních údajů občas není možné pořizovat záznam všeho, co by mohla kamera obsáhnout. I proto byly vyvinuty nástroje pro **maskování statických i pohybujících se objektů** v zorném poli kamer. Maskování se týká nejčastěji obličejů či soukromých pozemků. Objekty jsou blokovány plnou barvou při prohlížení, zobrazování archivních záznamů i při exportu videí.

Detekce neoprávněné manipulace je funkce určená pro kamerové systémy, která upozorní majitele kamery bezprostředně potom, co dojde k ovlivnění schopnosti její funkce záznamu. To se týká především kamer, které mohou být napadeny fyzicky. K oznámení poškození může dojít v situacích, kdy je obraz

rozmazaný, kamera je fyzicky zasažena či poškozena barvou, dojde k pokusu vypnutí napájení nebo k neúmyslnému poškození. [5]

Na konkrétní přání zákazníka vývojáři AI kamerových softwarů vyvíjí systémy, které lze propojit s nejrůznějšími **externími a výstupními zařízeními**. Nejčastěji se jedná o zařízení pro řízení vstupu, bezpečnostní ovládací panely, softwary dalších stran aj.

3 VZDÁLENÉ OVLÁDÁNÍ POMOCÍ APLIKACE

Z provedeného průzkumu vyplývá, že zákazníci čím dál častěji požadují rychlý a snadný přístup k aktuálním datům informačních a bezpečnostních systémů, které chrání jejich majetek. Tak začalo docházet k vývoji mobilních a počítačových aplikací, díky nimž máme okamžitý přehled o všech situacích, které nastanou. Nejnovější aplikace však nenabízí jen přehled o IBS, nýbrž i možnost na dálku ovládat a spravovat všechny připojené technologie. To nám umožňuje sledovat situaci ve střeženém objektu z jakéhokoliv místa a v jakoukoliv dobu. Pokud nastane nějaká nestandardní situace, ihned dojde k informování příslušné osoby a je možné na tuto situaci ve vteřině zareagovat (např. deaktivovat alarm, kontaktovat potřebné složky). Hlavní výhody aplikací jsou:

- okamžitý přehled o všech bezpečnostních zařízeních,
- dálkové ovládání alarmů (aktivování/deaktivování),
- přehledně zpracovaná historie všech událostí,
- sledování teploty, spotřeby energie apod.,
- zobrazení záznamů z kamerových systémů (v reálném čase/ze záznamu),
- použití digitálního zoomu, ovládání kamer,
- ovládání dveří, vrat a dalších vstupů,
- nahrávání maker,
- pro různé typy OS,
- aplikace jsou zabezpečené heslem či přístupovým kódem kvůli minimalizaci rizika zneužití,
- základní verze aplikací bývají často k produktům zabezpečení zdarma.

4 CHYTRÁ DOMÁCNOST A INFORMAČNÍ BEZPEČNOSTNÍ SYSTÉMY

O chytrých domácnostech jste již pravděpodobně slyšeli. Jedná se o budovy, které využívají různá zařízení připojená k internetu, což umožňuje vzdálené sledování a správu těchto systémů a spotřebičů (topení, zabezpečovací systémy, osvětlení, …) [7]. Tyto technologie se běžně spravují pomocí mobilní aplikace či webového rozhraní. Jelikož se tímto směrem ubírají i informační bezpečnostní systémy, tak začalo docházet k propojení systémů smart homes a IBS do jednoho integrovaného systému. Výhoda těchto systémů je v okamžitém přehledu a dálkovém ovládání prakticky všech elektronických zařízeních, pozdější úspoře finančních prostředků a menší ekologické náročnosti. Nevýhodou je jednoznačně vysoká počáteční investice a vyskytující se pochybnosti o celkové bezpečnosti těchto systémů. Jelikož je vše ovládáno přes internet, je zde riziko napadnutí systému hackerem a např. vypnutí určitých funkcí či zcizení dat. I tak se ale tyto systémy dále vyvíjí a zdokonalují. Firma Loxone např. na svých webových stránkách uvádí, že lze jednou aplikací spravovat všechny tyto technologie: osvětlení, teplotu, stínění (rolety, markýzy), ventilaci, alarm a zabezpečení, systém určený k upozornění na požár a únik vody, hudbu, budík, monitoring oken a dveří, ovládání dveří a bran, saunu, bazén a mnoho dalších.

A jak tedy vypadá chytré zabezpečení? Jako příklad může sloužit využití chytrého zámku propojeného se smartphonem, kdy zámek automaticky pozná, že stojíte přede dveřmi a dveře odemkne. Pomocí instalované kamery u dveří pak můžete vidět čekající osobu a odemknout jí dveře, i když zrovna nejste doma. Smart homes také běžně využívají množství alarmů, které vám v případě narušení bezpečnosti okamžitě pošlou oznámení. Stejně fungují i čidla na detekci kouře a úniku vody. [11] Cena systémů smart homes se pohybuje cca od 50 000 Kč pro menší byty se základními funkcemi, ale může se vyšplhat až k 500 000 Kč. Pro představu uvádí firma Loxone porovnání ceny tradičního ovládání (121 000 Kč) a inteligentního ovládání Loxone (137 940 Kč), kdy cena zahrnuje

elektroinstalaci, topení, alarm, rekuperaci (v ceně není zahrnutá montáž komponent). Rozdíl 14 000 Kč představuje systém Loxone, který zahrnuje 33 funkcí, jako je ovládání světel, vzdálená kontrola, centrální ovládání, pokročilé zabezpečení, monitoring, statistiky aj.

5 BUDOUCNOST INFORMAČNÍCH BEZPEČNOSTNÍCH SYSTÉMŮ

Inteligentní budovy, města, automobily, stroje, zabezpečení… kam až vývoj těchto technologií povede? Umělá inteligence se masivně využívá v kombinaci s informačními bezpečnostními systémy i přesto, že se stále častěji objevují případy, kdy se umělá inteligence obrátila proti člověku nebo se modifikovala a převzala nad sebou vládu. Ani zneužití dat z kamerových záznamů již není nic neobvyklého. Možná si ani neuvědomujeme, kolik informací o nás někdo ví jen kvůli využití bezpečnostních systémů s AI. Asi neznámější příklad masivního využití IBS ke sledování lidí za účelem „udržování pořádku a zvýšení bezpečnosti“ najdeme v Číně. Tento systém má bezpochyby svá pozitiva – nejenže působí jako prevence kriminality, ale pomáhá řešit trestnou činnost a jiné neočekávané hrozby a situace v rekordním čase. Na druhou stranu dochází k úplnému potlačení soukromí a stát ví o svých občanech doslova vše. V souvislosti s absolutní kontrolou lidí má v roce 2021 dojít ke spuštění tzv. systému sociálního kreditu, který bude sloužit k hodnocení lidí na základě jejich společenského a ekonomického chování, a právě IBS v něm budou hrát důležitou roli. Přešli jste přechod na červenou? Budou vám strženy kredity. Přesáhli jste povolenou rychlost? Přicházíte o další kredity. Bavíte se s nevhodnou osobou? Opět přicházíte o kredity. Kredity se tedy můžou snižovat či navyšovat podle chování lidí. Na základě množství kreditů bude docházet k různým postihům (při nízkém počtu kreditů) a při vysokém množství kreditů k zvýhodňování a odměnám. [3], [8] Příklady výhod a postihů jsou uvedeny v této tabulce:

Tabulka 2: Čínský systém sociálního kreditu

Výhody vysokého skóre	Postihy za nízké skóre
Daňové úlevy	Znemožnění koupě letenky/jízdenky
Rychlejší poskytnutí nemocniční péče	Veřejné zostuzování
Levnější náklady na dopravu	Odepření některých sociálních služeb
Prioritní přijetí do školy/zaměstnání	Menší možnost získání úvěru
Bezplatné půjčení automobilu	Znemožnění studovat na soukromé škole

Zdroj: [6]

Čína ovšem není jedinou zemí, kde dochází k masivnímu sledování lidí. Další země, které IBS široce nasazují, jsou například Indie, Rusko, USA a Německo.

Dostupné internetové zdroje vidí budoucnost kamerových systémů v dalším vývoji nástrojů využívajících umělou inteligenci. Budou vyvinuty nové technologie, které překonají hranice lidských omezení. Smart homes se stanou standardem a rozpoznávání obličeje bude naprosto běžnou situací. [10]

6 OTÁZKY K ZAMYŠLENÍ

Na závěr se pokuste zodpovědět těchto pár otázek:

- Jaké jsou podle vás výhody chytrých kamerových systémů?
- Jaké jsou podle vás nevýhody chytrých kamerových systémů?
- Chtěli byste si v budoucnu pořídit smart home? Proč ano/proč ne?
- Jaký máte názor na zavedení systému sociálního kreditu v Číně?
- Kam se bude podle vás vyvíjet oblast informačních bezpečnostních systémů?

POUŽITÁ LITERATURA

[1] *AxxonSoft* [online]. AxxonSoft, ©2021 [cit. 2021-04-01]. Dostupné z: https://www.axxonsoft.com

[2] Bezpečnostní terminály s funkcí rozpoznání obličeje. Hikvision [online]. Hangzhou: Hikvision Digital Technology, ©2021 [cit. 2021-04-01]. Dostupné z: https://www.hikvision.com/cz/products/Access-Control-Products/Face-Recognition-Terminals/?q=bezpe%C4%8Dnostn%C3%AD%20termin%C3%A1ly%20s%C2%A0funkc%C3%AD%20rozpozn%C3%A1n%C3%AD%20obli%C4%8Deje&position=1

[3] Čína zavádí sociální kreditní systém. Co to znamená? BusinessInfo.cz [online]. CzechTrade, ©1997-2021 [cit. 2021-04-01]. Dostupné z: https://www.businessinfo.cz/clanky/cina-zavadi-socialni-kreditni-system-co-to-znamena

[4] *Národní soustava povolání* [online]. Praha: Ministerstvo práce a sociálních věcí, ©2017 [cit. 2021-03-31]. Dostupné z: https://nsp.cz

[5] Tamper Detection. VideoSurveillance.com [online]. VideoSurveillance.com, ©2021 [cit. 2021-04-01]. Dostupné z: https://www.videosurveillance.com/tech/tamper-detection.asp

[6] Social Scoring in China: Big Brother squared. In: Smart industry [online]. Smart industry, ©2021 [cit. 2021-04-01]. Dostupné z: https://www.smart-industry.net/social-scoring-in-china-big-brother-squared

[7] Smart home or building (home automation or domotics). IoT Agenda [online]. ©2005–2021 [cit. 2021-04-01]. Dostupné z: https://internetofthingsagenda.techtarget.com/definition/smart-home-or-building

[8] Velký bratr vidí, když jdete na červenou. Sledování v Číně neuniknete. IDNES.cz [online]. MAFRA, a. s., ©1999–2021 [cit. 2021-04-01]. Dostupné z: https://www.idnes.cz/technet/veda/cina-velky-bratr-socialni-skore-kamery.A180405_120258_veda_dvz

[9] Videodetekce kouře. EUROALARM [online]. EUROALARM, spol. s r.o.,

©2020 [cit. 2021-04-01]. Dostupné z: https://www.euroalarm.cz/eshop-zabezpecovaci-technika/pozarni-signalizace/videodetekce-koure

[10] Why AI is the future of home security. The Next Web [online]. Amsterdam: The Next Web, ©2006–2021 [cit. 2021-04-01]. Dostupné z: https://thenextweb.com/plugged/2020/11/30/why-ai-is-the-future-of-home-security

[11] Zabezpečení domácnosti se Smart Home systémem Homematic IP. Conrad blog [online]. Conrad Electronic, ©2018 [cit. 2021-04-01]. Dostupné z: https://blog.conrad.cz/zabezpeceni-domacnosti-se-smart-home-systemem-homematic-ip