Univerzita Tomáše Bati ve Zlíně
Ústav bezpečnostního inženýrství

Sborník
6. ročníku mezinárodního online workshopu
SECULIN 2021

Možností matematizace a využití modelování v oboru bezpečnosti.

(tématické zaměření workshopu)

pod záštitou
děkana Fakulty aplikované informatiky
doc. Mgr. Milana ADÁMKA, Ph.D.

Sborník je věnován památce doc. Ing. Luďka Lukáše, CSc.

Zlín
11. listopadu 2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Nad Stráněmi 4511
76005 Zlín
Česká republika
https://fai.utb.cz

Sborník 6. ročníku mezinárodního online workshopu SECULIN 2021
Editor: doc. Ing. Martin Hromada, Ph.D.

Oponenti:
Ing. Jan Valouch, Ph.D.
doc. Ing. Martin Hromada, Ph.D.

Workshop SECULIN 2021 se uskutečnil za podpory interního výzkumného projektu Univerzity Tomáše Bati ve Zlíně „Analytické bezpečnostní modely na bázi teorie řízení a dalších matematických disciplín“ (30216003025).

ISBN 978-80-7678-067-5

Vědecký výbor mezinárodního online workshopu

Předseda:
doc. Mgr. Milan Adámek, Ph.D. – Univerzita Tomáše Bati ve Zlíně

Členové:
prof. Ing. Zdeněk Dvořák, PhD. – Žilinská univerzita v Žilině
prof. Ing. Ladislav Hofreiter, CSc. – Žilinská univerzita v Žilině
doc. Ing. Martin Hromada, Ph.D. – Univerzita Tomáše Bati ve Zlíně
Ing. Peter Lošonci, PhD. – Vysoká škola bezpečnostného manažérstva v Košiciach
Ing. Stanislav Lichorobiec, Ph.D. – Vysoká škola báňská – technická univerzita v Ostravě
prof. Ing. Tomáš Loveček, PhD. – Žilinská univerzita v Žilině
doc. Ing. Luděk Lukáš, CSc. – Univerzita Tomáše Bati ve Zlíně
doc. Ing. Jiří Pokorný, Ph.D. – Vysoká škola báňská – technická univerzita v Ostravě
prof. Ing. Josef Reitšpís, PhD. – Vysoká škola bezpečnostného manažérstva v Košiciach
doc. RNDr. Jaroslav Tureček, Ph.D. – AMBIS Praha
Ing. Jan Valouch, Ph.D. – Univerzita Tomáše Bati ve Zlíně
doc. Ing. Andrej Velas, PhD. – Žilinská univerzita v Žilině

Oponenti:
Ing. Jan Valouch, Ph.D.
doc. Ing. Martin Hromada, Ph.D.

Organizační výbor:
Ing. Jan Valouch, Ph.D.. – Univerzita Tomáše Bati ve Zlíně
doc. Ing. Martin Hromada, Ph.D. – Univerzita Tomáše Bati ve Zlíně
Jana Garguláková – Univerzita Tomáše Bati ve Zlíně

OBSAH

Úvodní slovo

Bezpečnostní vzdělávání se stává základním a moderním pilířem odborné přípravy společnosit fenoménem současnosti. Jestliže bylo vzdělávání v oblasti bezpečnosti zaměřeno především na vojenství, za posledních 20 let se stává doménou řady dalších oborů a druhů bezpečnosti. Významním aspektem reflektujícím složitost doby a současně technologickou závislost společnosti je potřeba implementace matematizace a využití modelování v oboru bezpečnosti jako určité společenské výzvy v přípravě odborníků v této oblasti. Mezi vysoké školy, které toto vzdělávání zajišťují a mají ambici impelemtace matematizace a modelování, patří Žilinská univerzita v Žilině, Vysoká škola báňská – technická univerzita v Ostravě, Vysoká škola bezpečnostného manažérstva v Košiciach, Policejní akademie v Praze, Akadémia policajného zboru v Bratislavě, AMBIS Praha a také Univerzita Tomáše Bati ve Zlíně.

Bylo jen přirozeným krokem ve vývoji, že se vysoké školy rozhodly předávat si nejnovější poznatky z oboru. To bylo i impulsem ke vzniku odborných setkávání zástupců vysokých škol. Letošní 6. ročník mezinárodního workshopu SECULIN 2021 pořádala Univerzita Tomáše Bati ve Zlíně. Workshop byl zaměřen na oblast již zmiňované matematizace a využití modelování v oboru bezpečnosti. Cílem workshopu byla diskuze o zkušenostech a praktických příkladech matematizace a modelovaní bezpečnostních problémů v širších souvislostech.

Díky protiepidemiologickým opatřením Covid-19 byl workshop organizován ve formě online s využitím videokonference. I přes ztížené podmínky se nazájem propojil Zlín s Prahou, Košicemi i Žilinou. Aktuální požadavky ve vzdělávání i s využitím aspektu matematizace, že lze být s kolegy v kontaktu i při omezených možnostech cestování. Sborník SECULIN 2021 obsahuje jak příspěvky, které odezněly v rámci online worshopu, tak další odborné výstupy tvůrčí práce autorů z vysokoškolských pracovišť. Věřím, že jednotlivé příspěvky budou pro čtenáře inspirativní a pomohou rozšířit aktuální přístupy k bezpečnostnímu vzdělávání.

Ve Zlíně 11. listopadu 2021 doc. Ing. Martin Hromada, Ph.D.

VYUŽITIE MATEMATICKÝCH METÓD PRI MERANÍ VZDIALENOSTI VYBRANÝCH TRASOVACÍCH SYSTÉMOCH

Martin Boroš[1], Radoslav Kuffa[2]

ABSTRAKT

Trasovacie systémy nám umožňujú určiť smer a trasu pohybu čím sa líšia od lokalizačných systémov, ktoré umožňujú identifikovať na akom mieste sa nachádza v danom priestore. Bežne používané systémy využívajú GPS súradnice, pričom na voľnom priestranstve tieto systémy pracujú relatívne dobre. Problém nastáva ak chceme trasovať v uzavretom priestore kde je GPS signál nepoužiteľný. Jednou z možností je využitie komunikačnej technológie Bluetooth alebo RFID. V takom to prípade však môže nastať problém pri definovaní vzdialenosti, nakoľko tieto systémy určujú svoju polohu v dBm, teda v útlme. Cieľom príspevku je poukázať na využitie matematického modelovania pre určenie vzdialenosti a nie hodnoty útlmu.

Kľúčové slová:
Trasovacie systémy, Bluetooth, matematické modelovanie, útlm, vzdialenosť.

ABSTRACT

Tracing systems allow us to determine the direction and route of movement, which differs from location systems, which allow us to identify where it is in a given area. Commonly used systems use GPS coordinates, and these systems work relatively well in open space. The problem occurs if we want to trace in an enclosed space where the GPS signal is unusable. One option is to use Bluetooth or RFID communication technology. In this case, however, there may be a problem in defining the distance, as these systems determine their position in dB, i.e., in attenuation. The aim of the paper is to point out the use of mathematical modelling to determine the distance and not the attenuation value.

Key words
Tracing systems, Bluetooth, mathematical modeling, attenuation, distance.

[1] Martin Boroš, Ing., PhD., Fakulta bezpečnostného inžinierstva, Univerzitná 8215/1, 010 26 Žilina, +421 41 513 6668,
[2] Radoslav Kuffa, JUDr., Ing., Fakulta bezpečnostného inžinierstva, Univerzitná 8215/1, 010 26 Žilina,

1 TRASOVACIE SYSTÉMY

Trasovacie systémy, alebo sledovacie systémy predstavujú súhrn viacerých technológií, ktoré umožňujú sledovať rôzne predmety či osoby, počas a po trase ktorú absolvovali pre presune z jedného bodu do druhého alebo viacerých. V súčasnosti existuje niekoľko technológií určených na vytváranie systémov sledovania polohy, medzi ktoré patria hlavne nasledovné [1, 2]:

- **Globálny pozičný systém (GPS)** – najpoužívanejší lokalizačný systém, vhodný pre vonkajšie určovanie polohy. U určeniu polohy využíva 27 satelitov krúžiacich okolo Zeme, z ktorých 24 je v prevádzke a zvyšné 3 sú prídavné v prípade zlyhania niektorého zo satelitov. GPS prijímače sú schopné vyhľadať 4 alebo viac satelitov, zistiť vzdialenosť ku každému a určiť svoju polohu prostredníctvom trilaterácie.
- **Geografické informačné systémy (GIS)** – jedná sa o systém, ktorý je schopný zachytávať, uchovávať a analyzovať zaznamenané geografické informácie.
- **Rádiofrekvenčná identifikácia (RFID)** – systém pozostáva zo štítkov (tagov) a čítačiek, ktoré vzájomne komunikujú prostredníctvom rádiových vĺn. Súčasťou systému je riadiaci a aplikačný softvér čítačiek. Pasívne RFID systémy nevyžadujú zdroj energie, aktivujú sa iba v prípade priblíženia sa k čítačke. Naopak aktívne systémy využívajú batériu ako zdroj energie.
- **Near Field Communication (NFC)** – jedná sa o typ RFID technológie. Tento systém podporuje väčšinu zariadení so systémom Android a iOS. Ide o technológiu krátkeho dosahu, spravidla niekoľko centimetrov. Implementácia NFC nie je cenovo náročná a funguje s akýmkoľvek bezkontaktným terminálom.
- **WiFi** – jedná sa o využitie možností bezdrôtových WiFi sietí v rámci ktorých sa rozpoznávajú prístupové body WiFi zariadeniami, ktoré sú po zistení viacerých bodov schopné určiť svoju polohu. Výhodou je v mnohých prípadoch použitia existujúca infraštruktúra tejto technológie na rôznych miestach, ktorá dobre funguje s mobilnými zariadeniami.
- **Bluetooth Low Energy (BLE) - Beacony –** jedná sa o nízkoenergetickú technológiu Bluetooth umožňujúcu beaconom určovať vzdialenosť od iných inteligentných zariadení, ako sú napríklad smartfóny. Je však potrebné mať nainštalovanú konkrétnu aplikáciu. Implementácia technológie nie je cenovo náročná. V súčasnosti je mnoho ľudí držiteľmi smartfónov, v dôsledku čoho má nasadenie beaconov vysoké uplatnenie.

2 BEACON

Beacon (z angl. maják) je možné charakterizovať ako malé zariadenie, ktoré v pravidelných, definovaných intervaloch vysiela rádiové signály, ktoré je možné prijímať smartfónmi, prípadne inými prijímacími zariadeniami. Bluetooth beacony využívajú BLE, teda rádiovú technológiu krátkeho dosahu. Je efektívna a užitočná, nakoľko využíva nízke úrovne energie. Beacony je možné napájať prostredníctvom pevného zdroja energie alebo použitím batérií. Je možné využiť ich na navigáciu v priestore, či na upozorňovanie na rôzne akcie či udalosti [3].

V súčasnosti sú beacony používané na rôzne účely. Vykonávajú niekoľko funkcií, ktoré sa neustále zdokonaľujú. Ich použitie je rozmanité a zahŕňa predovšetkým [3]:

- vnútorné polohovanie a navigáciu,
- sledovanie osôb alebo majetku,
- reklamy alebo správy založené na polohe,
- zabezpečenie a automatické odomykanie a zamykanie počítača,
- spúšťanie žiadostí o platby.

Na trhu sú dostupné rôzne typy beaconov, ktoré sa líšia rozmermi, výdržou batérie, spôsobom použitia či schopnosťou odolávať priestorovým podmienkam. Za základné rozdelenie beaconov by sme mohli považovať nasledovné delenie [3, 4]:

- **Štandardný beacon** – rozmermi podobný WiFi smerovaču,
- **prenosný/malý beacon** – veľkosť kreditnej karty alebo nálepky,
- **USB beacon** – malé, prenosné zariadenie veľkosti flash disku,
- **video beacon** – zariadenie je zapojené na zadnú časť obrazovky a poskytuje vizuálne kontextové informácie,
- **al beacon** – je schopný rozpoznávať rôzne pohyby a gestá,
- **sticker beacon** – rozmermi najmenší,
- **nadradený beacon** – podobný ako veľké smerovače WiFi, slúži na sledovanie iných beaconov či na zber údajov a ich ukladanie do cloudu,
- **vyhradený beacon** – zariadenie je odolné voči nepriaznivým podmienkam v priestore, ako je prach, voda a iné faktory.

2.1 TESTOVANIE BLUETOOTH BEACONOV

Aj napriek skutočnosti, že beacony nie sú v rámci komerčnej sféry dlho využívané, ich testovaniu sa celosvetovo venovalo veľmi veľa odborníkov či už ako jednotlivci alebo tímy. Veľký okruh autorov sa venuje testovaniu životnosti beaconov z pohľadu výdrži batérie umiestenej ako v ňom tak v prijímacom zariadení. Podľa [5] je možné u štandardného beaconu s gombíkovou batériou pri vzdialenosti do 100metrov životnosť takmer 6 mesiacov. Dané skúmanie bolo realizované pri použití jedného beaconu a jedného prijímacieho zariadenia, ktorým bol mobilný telefón s operačných systémom IOS. Okrem výdrže energie v beacone sa tím okolo [5]

zameral aj na hodnotu kapacity prijímacieho zariadenia, ktorým bol spomínaný mobilný telefón s operačným systémom ISO. Zistili, že pri trvalo pripojenom jednom zariadení, beacone, je spotreba energie vyššia o 5,75% ako pri bežnom aktívnom stave. V prípade pripojených 10 zariadení, beaconov, na jedno vysielacie zariadenie je to 7%, čo nám predstavuje rozdiel 1,25%. Takéto zistenie je veľmi dôležité nakoľko sa môže jednať o ďalšiu výhodu a možnosť využitia beaconov v rámci IoT sietí.

3 VYUŽITIE BEACONOV K TRASOVANIU

Ako sme poukázali, aj vyššie, beacony sa používajú prevažne na lokalizáciu predmetov v rámci IoT v uzatvorenom priestore. Vďaka svojím výhodám je ich však možné použiť aj na trasovanie, respektíve vykreslenie trasy, ktorú beacon prešiel. Využíva sa pritom práve útlm pomocou hodnoty ktorého je možné vďaka vzorcu 1, vypočítať jeho aktuálnu polohu [5, 6].

$$V = 10\text{^}(\frac{nameraný\ výkon - RSSI}{10 * N}) \quad (1)$$

Kde:

V – vzdialenosť udávaná v metroch,

RSSI – sila signálu závislá od vzdialenosti a hodnoty vysielacieho výkonu, dBm,

N – konštanta určujúca prostredie, teda či sa jedná o obytný priestor v ktorom sa nachádzajú predmety alebo otvorený priestor, rozsah je 2 – 4.

Vzdialenosť vypočítanú podľa vzorca 1, budeme pravidelne pomocou výpočtového programu upravovať, čím zistíme ako, respektíve ktorým smerom sa beacon pohybuje. Údaje budú pravidelne sledované a posielané na server v rámci ktorého bude prebiehať daný výpočet. Následne budeme pomocou pravidelných informácii o vzdialenosti vedieť kde v priestore sa beacon nachádza, a taktiež ktoré beacony sa nachádzajú v jeho bezprostrednej blízkosti. K tomu aby sme efektívne a s určitosťou dokázali povedať, že dva alebo viacej beaconov sa nachádzajú pri sebe alebo sa pohybujú od seba či k sebe, je potrebné využitie minimálne dvoch prijímacích zariadení. Následný pohyb sa určí pomocou rozdielu polôh.

Naše meranie bude spočívať vo vytvorený vlastnej siete v rámci priestorov Fakulty bezpečnostného inžinierstva, Žilinskej univerzity v Žiline. V danej sieti bude pevne inštalovaných 8 prijímacích zariadení, ktoré budú pripojené na nami vytvorený server v rámci ktorého bude prebiehať výpočet polohy a pohybu beaconov v sieti. Pri prvotnom testovaní sme sa rozhodli overiť správnosť výpočtu vzdialenosti pomocou RFID kariet, teda okrem beaconov budú mať pohybujúce osoby k dispozícii aj čipové karty a v prípade priamej blízkosti bude ich úlohou priložiť kartu na prijímacie zariadenie, ktoré bude vybavené čítačkou. Následne bude možné identifikovať

hodnotu vzdialenosti ako pre beacon tak pre čipovú kartu (logicky desiatky cm) a zistiť tak či sa tieto hodnoty zhodujú alebo sú dané údaje diametrálne odlišné.

Rozhodli sme sa pre využitie 8 prijímacích zariadení, ktoré budú postupne rozmiestnené vo vstupnej chodbe, na schodisku a chodbách. Tieto prijímacie zariadenia budú samostatné, nakoľko budú vybavené veľkokapacitnou power bankou, zabezpečujúcou trvalé fungovanie.

ZÁVER

Cieľom príspevku bolo poukázať na možnosti rôzneho využitia beaconu v rámci trasovacích systémov. V úvodnej časti sme vysvetlili čo to beacon je, ako sa používa sa a aké typy môžu byť. V ďalšej časti sme sa zamerali na už realizované experimentálne testy, zaoberajúce sa výdržou batérie ako v beacone tak v prijímacom zariadení. Nakoniec sme sa zamerali na popis trasovacieho systému, ktorý sa vyvíja na Fakulte bezpečnostného inžinierstva, Žilinskej univerzity v Žiline a ktorý umožní pomocou matematickej operácie identifikovať smer pohybu beaconu v priestore z pohľadu vzdialenosti. Experimentálne meranie je momentálne v stave teoretických príprav a nákupu jednotlivých komponentov a s nasadením systému by sa malo začať na jar, prípadne leto tohto roku.

POĎAKOVANIE

Tento článok bol pripravený v rámci podpory projektu APPV-20-0457 Monitorovanie a trasovanie pohybu a kontaktu osôb v zdravotníckych zariadeniach.

LITERATÚRA

[1] BONSOR, K.: How Location Tracking Works. Online.[cit. 2021-12-30]. Dostupné na: https://electronics.howstuffworks.com/everyday-tech/location-tracking1.htm
[2] LOVEČEK, T., VEĽAS, A., ĎUROVEC, M.: Poplachové systémy. EDIS – ŽU 2015. ISBN 9788055411446. 230s.
[3] Al-AlqusairIsra, D., Al-Turaiki, I., Al-Humaimeedy, A., Al-Hudhud, G.: Measuring Patient Experience In Real Time Using IBeacon Technology. Bioscience Biotechnology Research Communications 2019, Vol. 12, Issue 2, s. 230-238
[4] Future of iBeacons in 2021 and beyond, 2021. Online. [cit. 2022-01-06]. Dostupné na: https://iottive.com/2021/01/19/future-of-ibeacons-in-2021-and-beyond/
[5] PUŠNIK, M., Galan, M., Boštjan, Š.: Improved Low Energy Sensor Detection for Indoor Localization Services. Sensors 2020. Vol. 20, Issue 8. doi: 10.3390/s20082336

How to Calculate Distance from the RSSI value of the BLE Beacon. Online. [cit. 2021-12-06]. Dostupné na: https://iotandelectronics.wordpress.com/2016/10/07/how-to-calculate-distance-from-the-rssi-value-of-the-ble-beacon/

EKONOMICKÁ NÁVRATNOSŤ INVESTÍCIÍ DO BEZPEČNOSTI V ZDRAVOTNÍCKYCH ORGANIZÁCIÁCH

doc. Ing. Katarína Kampová, PhD.[3)], Ing. Katarína Mäkká, PhD.[4)], Ing. Zuzaná Zvaková, PhD.[5)], doc. Ing. Bohuš Leitner, PhD.[4)]

ABSTRAKT

Zdravotníctvo patrí medzi najdôležitejšie systémy, ktorých nefunkčnosť spôsobuje závažný dopad na zdravie a život obyvateľov. Poskytovanie zdravotnej starostlivosti a ochrana verejného zdravia sú základné funkcie štátu. Z pohľadu kontinuálneho zaistenia zdravotníckej starostlivosti je nevyhnutné uvažovať o spôsoboch monitorovania a trasovania osôb potenciálne šíriacich infekčné respiračné ochorenie (ako napríklad COVID - 19), prostredníctvom ktorých by sa znížil nápor na zdravotnícke zariadenia a z pohľadu ekonomických prínosov by boli tieto opatrenia relevantné. Predkladaný článok rieši problematiku ekonomickej návratnosti investícií do monitorovania a trasovania osôb a poukazuje na možnosti využitia analýza nákladov a prínosov pri rozhodovaní sa o investícii do systémov monitorovania a trasovania.

Kľúčové slová: monitorovanie, trasovanie, analýza nákladov a prínosov

ABSTRACT

Healthcare is one of the most important systems, the non-functioning of which causes a serious impact on the health and life of the population. The provision of health care and the protection of public health are the basic functions of the state. From the point

[3]) doc. Ing. Katarína Kampová, PhD., FBI, Žilinská univerzita v Žiline, 1. mája 32, 01026 Žilina, e-mail: Katarina.Kampova@uniza.sk

[4]) Katarína Mäkká, Ing., PhD., FBI, Žilinská univerzita v Žiline, 1. mája 32, 01026 Žilina, e-mail: Katarina.Makka@uniza.sk

[5]) Zuzana Zvaková, Ing., PhD FBI, Žilinská univerzita v Žiline, 1. mája 32, 01026 Žilina, e-mail: Zuzana.Zvakova@uniza.sk

[4]) doc. Ing. Bohuš Leitner, PhD., Žilinská univerzita v Žilina, Fakulta bezpečnostného inžinierstva, Katedra požiarneho inžinierstva, Univerzitná 8215/1, 010 26 Žilina, Slovakia, bohus.leitner@uniza.sk

of view of the continuous provision of health care, it is necessary to consider ways of monitoring and tracing persons potentially spreading this infectious respiratory disease (such as COVID - 19), through which the burden on health care facilities would be reduced and these measures would be relevant in terms of economic benefits.
The presented article addresses the issue of economic return on investment in monitoring and tracing of persons and points out the possibilities of using cost-benefit analysis when deciding on investments in monitoring and tracing systems.

Key words: monitoring, tracing, cost-benefit analysis

1 ÚVOD

Zásadná úloha zdravotníctva je a vždy zostane poskytovanie zdravotnej starostlivosti obyvateľom, pričom táto povinnosť vymedzuje v Slovenskej republike Zákon č. 576/2004 o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov. Vo vzťahu k zdravotníckym zariadeniam a epidemiologickej situácií z dlhodobého hľadiska je nevyhnutné definovať a vytvoriť také ochranné opatrenia, ktoré by boli dlhodobo udržateľné a nenarúšali existujúci systém svojimi obmedzeniami, a taktiež by zabezpečili kontinuálne zabezpečovanie zdravotnej starostlivosti. Kontinuálne zabezpečenie zdravotnej starostlivosti je primárne podmienené personálnym zaistením zdravotníckych zariadení. Personál v zdravotníckych zariadeniach je priamo vystavený hrozbe nákazy. Jedna z možností ako ochrániť a minimalizovať dopady šírenia SARS-CoV-2, resp. iných infekčných ochorení na personál v rámci zdravotníckych zariadení, je monitorovanie a trasovanie ich pohybu a kontaktu s osobami. Investícia do takéhoto opatrenia je zásadným rozhodnutím vedenia organizácie z pohľadu hodnotenia jeho nákladov a prínosov ale aj z pohľadu zaistenia poskytovania zdravotníckej starostlivosti.

2 MONITOROVANIE A TRASOVANIE OSÔB

Monitorovanie pohybu osôb patrí medzi jeden z nástrojov boja proti šíreniu sa pandémie a jeho základným cieľom je dohľad nad pohybom osôb. Vo všeobecnosti je možné klasifikovať monitorovanie na dve základné skupiny z pohľadu monitorovanej osoby, a to pasívne a aktívne monitorovanie. Medzi pasívne typy monitorovania je možne zaradiť, tie ktoré sú založené na kontrole osôb v určitom časovom intervale (napr. telefonát z Úradu verejného zdravotníctva, resp. samo-trasovanie v prípade pozitivity jedinca). Aktívne monitorovanie, resp. aktívny systém monitoringu predstavuje neustálu kontrolu monitorovanej osoby v danom priestore a čase. Vo vzťahu k prebiehajúcej pandémii aktívny monitoring predstavuje flexibilný nástroj, ktorý umožňuje, resp. by umožnil zefektívniť trasovanie osôb a prispieť k minimalizácií dopadov pandémie v danom subjekte.

Základným cieľom trasovania osôb je urýchlene identifikovať potenciálne nakazeného človeka a izolovať ho do karantény. Význam tohto opatrenia spočíva v ochrane iných, zdravých členov spoločnosti a zmiernení opatrení, ktoré sa prijímajú

vo vzťahu k riadeniu epidémie. Toto tvrdenie podporujú aj výsledky výskum Stanford univerzity, kde vedci vyvinuli matematický model na skúmanie potenciálu sledovania kontaktov na zníženie šírenia koronavírusu. Modelovali programy sledovania kontaktov v kontexte uvoľneného fyzického odstupu, pričom menili percento hypotetických symptomatických infekcií zistených v komunite od 10% do 90% v porovnaní so scenármi bez sledovania kontaktov. Zistili, že detekcia prípadov v komunite a úspešné oslovenie kontaktov musia pri sledovaní kontaktov prekročiť 50%, aby sa výrazne znížil prenos. Tiež zistili, že najúčinnejšie programy - programy s vysokou úrovňou účinnosti testovania, sledovania, izolácie a karantény - by mohli znížiť celkový prenos takmer o polovicu. Táto výhoda by umožnila značné uvoľnenie fyzických dištančných opatrení a obmedzení verejného zdravia a zároveň by pomohla kontrolovať šírenie COVID-19 [1].

Z pohľadu zaistenia kontinuity poskytovania zdravotnej starostlivosti v zdravotníckych organizáciách je vhodné implementovať v rámci organizácie systém monitoringu, ktorý by vytvoril základ pre program ochrany zamestnancov pred nákazou COVID-19 a taktiež vytvoril predpoklady na výrazné zníženie celkového prenos ochorenia. Investícia do takéhoto opatrenia je strategickým rozhodnutím vedenia organizácie z pohľadu hodnotenie jeho nákladov a prínosov, ale aj z pohľadu zaistenia poskytovania zdravotníckej starostlivosti. Jeden zo spôsobov ako vyhodnotiť a porovnať náklady a prínosy rôznych investičných projektov je analýza nákladov a prínosov.

3 ANALÝZA NÁKLADOV A PRÍNOSOV (CBA)

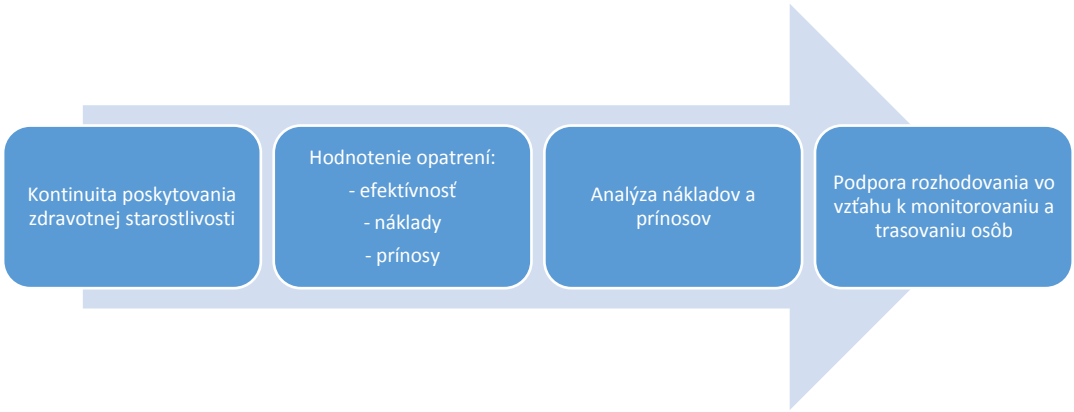
Analýza nákladov a prínosov predstavuje proces porovnávania plánovaných alebo odhadovaných nákladov a prínosov s cieľom rozhodnutia o tom, či je vytváraný projekt efektívny alebo neefektívny. Svojim priebehom postupne odpovedá na základnú otázku: „Čo komu realizácia investičného projektu prináša a čo komu berie?“. Náklady (ang. costs) označujú veľkosť zdrojov, ktoré sú potrebné pri realizácií daného projektu. Prínosy (ang. benefits) označujú hodnotou zisku, ktorý možno očakávať pri realizácií daného projektu. Náklady aj prínosy sú vyjadrované v peňažných jednotkách [2]. Medzi základné pojmy, ktoré sú využívané v analýze nákladov a prínosov patria:

- efekty plynúce z investície označujú všetky dopady, ktoré projekt prináša,
- náklady (costs) sú všetky negatívne dopady,
- prínosy (benefits) sú všetky pozitívne dopady,
- beneficient označuje subjekt, na ktorý dopadajú efekty plynúce z investície,
- hotovostný tok (Cash Flow) predstavuje finančný tok, ktorý má podobu príjmov alebo výdavkov,
- čistý hotovostný tok (Net Cash Flow) označuje rozdiel príjmov a výdavkov,
- kriteriálne ukazovatele sú ukazovatele, ktoré plnia funkciu rozhodnutia, či je alebo nie je projekt prijateľný [3].

V rámci analýzy nákladov a prínosov sa z časového hľadiska rozlišujú dva typy analýz. Prvým je analýza ex-ante, ktorá sa využíva v období pred realizáciou projektu, kedy je potrebná pri rozhodovaní o danom projekte alebo pri rozhodovaní o ďalších možnostiach riešenia. Druhým je analýza ex-post, ktorá sa využíva v období po ukončení projektu na zhodnotenie, pričom cieľom je spresnenie dosahov daného projektu v porovnaní s predpokladanými výsledkami pred jeho realizáciou [4].

Z pohľadu obsahu sa analýza nákladov a prínosov skladá z troch hlavných častí: technická časť, finančná analýza a ekonomická analýza. Technická časť je zameraná na definovanie účelu investície - projektu a jeho technickú charakteristiku. Finančná analýza sa zaoberá finančnými nákladmi a výnosmi a jej hlavným cieľom je vyhodnotiť daný projekt z hľadiska finančnej efektívnosti pre investora. Ekonomická analýza súvisí s finančnou analýzou a jej cieľom je hodnotenie prínosov projektu pre všetky subjekty, ktoré sú do neho zapojené [5][6].

Analýza nákladov a prínosov je využiteľná aj v rámci procesu rozhodovania zdravotníckych organizácií o investovaní do nástroja na monitorovanie a trasovanie osôb a to konkrétne v procese zaobchádzania s rizikom prerušenia kontinuity poskytovania zdravotnej starostlivosti. Grafické znázornenie využitia tejto metódy v rámci rozhodovacieho procese je možné vidieť na obrázku č. 1.



Obrázok č. 1. Proces analýzy nákladov a prínosov v rámci ochrany objektov [3]

V rámci prvého kroku je nevyhnutné sa zamerať na proces posudzovania rizika prerušenia poskytovania zdravotnej starostlivosti, ktorý je základným problémom zdravotníckych zariadení v súčasnosti. V druhom kroku je potrebné vyhodnotiť účinnosť vybraných opatrení pre jeho zníženie (efektívnosť, výpočet nákladov, výpočet výnosov) vo vzťahu k využívaniu nástroja monitorovania a trasovania osôb. Tento nástroj je možné využívať v užšom a širšom zmysle. V užšom zmysle sa zameriava iba na zamestnancov zdravotníckych zariadení a znižuje riziko prerušenia poskytovania zdravotnej starostlivosti vo vzťahu k nedostatku kvalifikovaného personálu a v širšom zmysle sa zameriava na monitorovanie a trasovanie všetkých osôb pohybujúcich sa v areáli zdravotníckeho zariadenia.

Hodnotenie efektívnosti monitorovania a trasovania osôb je vyjadrené takou mierou, s ktorou bude riziko odstránené alebo znížené prostredníctvom zavedenia navrhnutých opatrení. Nákladnosť opatrení závisí od porovnania výdavkov a

očakávaných prínosov, pričom je potrebné posúdiť efektívnosť vynaložených prostriedkov na uskutočnenie týchto opatrení. Náklady na zavedenie opatrení by mali byť vyčíslené čo najpresnejšie. V poslednom kroku je potrebné vytvoriť analýzu nákladov a prínosov pre vybrané riziko. Z výsledkov z analýzy nákladov a prínosov je možné získať znalosť o tom, aké efektívne by bolo riešenie daného problému a rozhodneme sa, či tento projekt zrealizujeme alebo nie [7] [3].

4 MODELOVÝ PRÍKLAD APLIKÁCIE ANALÝZY NÁKLADOV A PRÍNOSOV

Predmetom záujmu je zdravotnícke zariadenie, ktoré poskytuje služby v oblasti diagnostiky a zdravotnej starostlivosti. V rámci zdravotníckeho zariadenia je zamestnaných 30 špecializovaných doktorov, 50 zdravotných sestier a 25 osôb iného obslužného personálu. Predmetom investície v rámci projektu je nástroj monitorovania a trasovania osôb, ktorého cieľom je minimalizácia šírenia choroby COVID – 19 medzi týmto personálom. Beneficientom bude v rámci tohto projektu spoločnosť predmetná spoločnosť, štát, zamestnanci, ale hlavne pacienti, ktorý využívajú toto zdravotnícke zariadenie.

Prvým krokom je vytvorenie nulového variantu, ktorý predstavuje súčasný stav. Spoločnosť nemá implementovaný aktívny nástroj na monitorovanie a trasovanie osôb. Zamestnanci spoločnosti dodržujú všeobecne prijaté usmernenia a odporúčania Úradom verejného zdravotníctva Slovenskej republiky. V priebehu sledovaného intervalu jeden rok bolo pozitívne identifikovaných 50 osôb, z čoho bolo 25 doktorov, 15 zdravotných sestier a 10 zamestnancov ostatného personálu. Priebeh ochorenia personálu neviedol k žiadnemu úmrtiu a zamestnanci nemajú trvalé následky po prekonaní. Celkové náklady zamestnávateľa, ktoré súviseli s práceneschopnosťou zamestnancov, ich zastupovaním a zvýšením počtu služieb a nadčasov bolo vypočítaných na 107 250 Eur.

Okrem už popísaných finančných dopadov boli následkom danej situácie definované aj nepriame finančné dopady vo forme obmedzenia poskytovania zdravotnej starostlivosti, ktorá súvisela s nedostatkom špecializovaných zamestnancov anestéziológie a resuscitácie, týmto výpadkom boli straty definované v hodnote 55 000 Eur, ktoré by zdravotnícke zariadenie získalo, ak by úkony boli realizované. Ostatné vzniknuté náklady súvisiace s odkladom, resp. presmerovaním operácií na iné zdravotnícke zariadenia, a nesúviseli s výpadkom anestéziológa ale s výpadkom špecialistu v potrebnom odbore, v sledovanom období boli ohodnotené v hodnote 30 000 Eur.

Tab. 1 Odhadované finančné dopady

Dopad	**Typ dopadu**	**Suma v EUR**
Priame dopady	Náklady súvisiace s práceneschopnosťou	107 250
Nepriame dopady	Nemožnosť vykonávať plánované operácie	55 000
	Presmerovanie operácií	30 000
Suma celkom		192 250

Predmetom investície v rámci projektu zameraného na monitorovanie a trasovanie osôb je zníženie šírenia ochorenia COVID-19 medzi zamestnancami zdravotníckeho zariadenia a tým zaistenia kontinuálneho poskytovania zdravotnej starostlivosti bez obmedzujúcich faktorov. Systém monitorovania a trasovania bude realizovaný zákazkovým systémom reflektujúci špecifické potreby tohto zariadenia a jeho zamestnancov. Systém bude založený na technológií RFID a celkové odhadované investičné náklady pre zdravotnícke zariadenie sú 25 000 Eur a náklady s vývojom a implementáciou systému monitorovania a trasovania do prostredia organizácie sú odhadované na 15 000 Eur.

Okrem spomínaných nákladov je nevyhnutné uvažovať i o personálnom zaistení, ktoré bude vykonávať obslužné činnosti a vyhodnocovať údaje získané týmto systémom. Celkové ročné odhadované náklady na obslužný personál sú 20 000 Eur a náklady na údržbu sú vyhodnotené priemerne na každý rok 500 Eur.

Tab. 2 Odhad finančných nákladov systému monitorovania a trasovania osôb

Náklady súvisiace s investíciou	**Popis**	**Suma Eur**
Technológie	Technológií RFID a súčasti systému	25 000
Vývoj a implementácia	Zákazkový projekt	15 000
Personálne obsadenie	Obslužný personál rok	20 000
Údržba	Opravy, straty za rok	500

Ďalšou časťou návrhu systému monitorovania a trasovania osôb je porovnanie finančných dopadov pred a po zavedení tohto systému. V nasledujúcej tabuľke je uvedený možný finančný dopad po zavedení tohto systému do zdravotníckeho zariadenia, ktoré sa opiera o štúdiu Stanford univerzity [1].

Tab. 3 Odhad možných finančných dopadov po zavedení systému monitorovania a trasovania osôb

Dopad	**Typ dopadu**	**Suma v EUR**
Priame dopady	Náklady súvisiace s práceneschopnosťou	53 625
Nepriame dopady	Nemožnosť vykonávať plánované operácie	27 500
	Presmerovanie operácií	15 000
Suma celkom		96 125

Na základe kvantifikácie nákladov a prínosov navrhnutého projektu monitorovania a trasovania osôb je možné vypočítať čistú súčasnú hodnotu (NPV) projektu pre každý rok [4].

$$NVP = \sum_{t=0}^{n} \frac{CF_t}{(1+r)^t}, \quad (1)$$

kde :

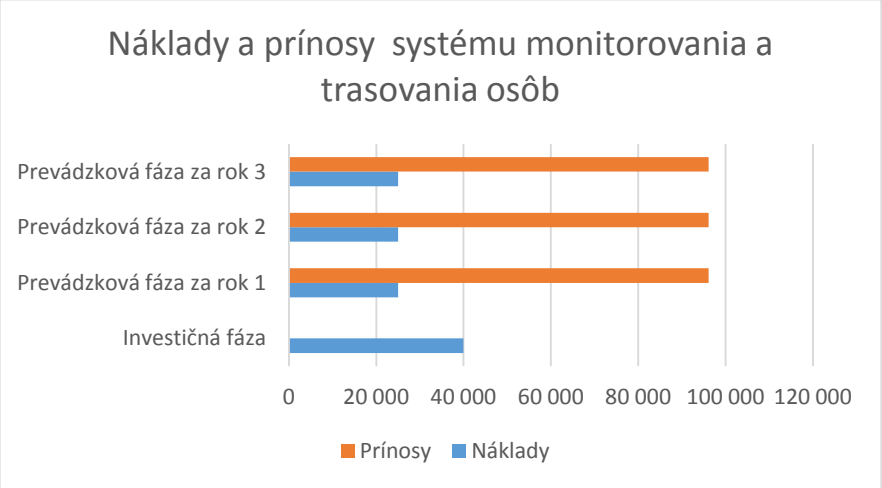
- NVP - čísta súčasná hodnota investície,

- CFt - hotovostný tok plynúci z investícií v období t,
- r - diskontná sadza.

Aby bol projekt efektívny musí byť výsledná čistá súčasná hodnota (NPV) kladná, prípadne rovná nule. Kladné hodnoty budú v tomto prípade predstavovať finančné prínosy získané prostredníctvom projektu. V prípade, že by konečná hodnota bola nulová, bude to znamenať, že projekt je prijateľný ale neprináša žiadne finančné prínosy.

Table 4. Kvantifikácia nákladov a prínosov v investičnej a prevádzkovej fáze projektu

Suma v Eurách	**Investičná fáza**	**Prevádzková fáza za rok**
Náklady	4 0000	25 000
Prínosy	0	96 125



Obrázok č. 2 Grafické znázornenie nákladov a prínosov systému monitorovania a trasovania osôb

Konečný výsledok výpočtu čistej súčasnej hodnoty (1) porovnáme s kritériami prijateľnosti – čistá súčasná hodnota NPV ≥ 0. Čistá súčasná hodnota (NPV) nám v prípade tohto projektu vyšla v sume 150 765 Eur za sledované 4 ročné obdobie pri diskontnej sadzbe 5%. Navrhovaný projekt vo vzťahu k definovaným priamym i nepriamym nákladom a prínosom a zhodnotení čistej NPV bude efektívny.

5 ZÁVER

Cieľom predkladaného článku bolo poukázať na možnosti využitia metódy analýzy nákladov a prínosov v procese rozhodovania sa pri investovaní do nástroja znižujúceho šírenie ochorenia COVID – 19 a to monitorovania a trasovania osôb. Na modelovanom príklade bolo poukázané na možnosť využitia metódy analýzy nákladov a prínosov v procese rozhodovania sa o takomto type investícii.

Tento článok bol pripravený v rámci podpory projektu APPV-20-0457 Monitorovanie a trasovanie pohybu a kontaktu osôb v zdravotníckych zariadeniach.

LITERATÚRA

[1] Salomon, J. A., et al.: The US COVID-19 Trends and Impact Survey: Continuous real-time measurement of COVID-19 symptoms, risks, protective behaviors, testing, and vaccination. Proceedings of the National Academy of Sciences of the United States of America 1800; 118 (51).

[2] Stobierski, T.: How to do a Cost-benefit Analysis & why it is important, 2019. Dostupné na: https://online.hbs.edu/blog/post/cost-benefit-analysis.

[3] Kampova, K., Makka, K., Zvarikova, K.: Cost benefit analysis within organization security management. 19th International Scientific Conference Globalization and Its Socio-Economic Consequences 2019 – Sustainability in the Global-Knowledge Economy, 74. https://10.1051/shsconf/20207401010.

[4] Kampova, K., Makka, K.: Economic Aspects of the Risk Impact on the Fuel Distribution Enterprises. Proceedings of the International Conference - Transport Means, Lithuania, 2018, 231-235.

[5] Dvorsky, J., Belas, J., Gavurova, B., & Brabenec, T. (2021). Business risk management in the context of small and medium-sized enterprises. Economic Research-Ekonomska Istraživanja, 34(1), 1690-1708.

[6] Rowland, Z., Krulicky, T., Oliinyk, O.> Capital cost quantification model in business activity planning: the evidence of the middle Europe countries. Ekonomicko-manazerske spektrum, 2020: 14(1), 30-42.

[7] Buganova, K., Luskova, M., Kubas, J., Brutovsky, M., Slepecky, J.: Sustainability of Business through Project Risk Identification with Use of Expert Estimates. Sustainability, 13(11). Dostupné na: http:// 10.3390/su13116311.

VPLYV EKONOMICKÉHO ASPEKTU NA ODOLNOSŤ OBJEKTOV REGIONÁLNEJ SAMOSPRÁVY

Jakub Ďurica[6], Andrej Veľas[7]

ABSTRAKT

Prielomová odolnosť nám určuje do akej miery je konštrukcia objektu odolná voči fyzickému ataku zo strany narušiteľa. Cieľom narušiteľa je častokrát nájsť najrýchlejšiu a najslabšiu cestu do chráneného objektu. Nakoľko pokúšať sa prekonať alebo vytvoriť otvor v stene je časovo, priestorovo a fyzicky náročné, narušitelia sa pokúšajú vniknúť do chráneného objektu cez otvorové výplne, teda okná a dvere. Práve ním je potrebné venovať patričnú pozornosť pri realizácii objektovej bezpečnosti.

Článok je zameraný na vyjadrenie finančných potrieb potrebných pre vytvorenie dostatočnej úrovne bezpečnosti objektov v správe samosprávy.

Kľúčové slová: prielomová odolnosť, výplne stien, finančné náklady, úroveň bezpečnosti

ABSTRACT

Breaktrhrought resistance determines extent to which construction of object resistant to physical attack by attacker. Attacker looking for the shortest and the weakness to break inside of object. Trying to overcome the walls is time, space and physically demendig, therefore attacker try break into objcet through overcoming walls fills – windows and doors. It is necessary due attention in the implementation of object security to walls fills.

The article focus on expressing the financial costs necessary for create a sufficient level of security of buildings in the administration of self-government.

Key words: breakthrough resistance, walls fills, financial costs, level of security

[6] Jakub Ďurica, Ing., Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, Katedra bezpečnostného manažmentu, Univerzitná 8215/1, Žilina, jakub.durica@uniza.sk

[7] Andrej Veľas, doc. Ing. PhD., Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, Katedra bezpečnostného manažmentu, Univerzitná 8215/1, Žilina, andrej.velas@uniza.sk

ÚVOD

Tanveer a Jeffrey hovoria, že samosprávy sú vytvorené štátom prostredníctvom charty, zákonov alebo iných prostriedkov, ktoré poskytujú verejnú správu pre definovanú oblasť s určitými vlastnosťami, akou je urbanizácia alebo vysoká hustota obyvateľstva [1]. Obce sú integrované do relatívne stabilného súboru formálnych pravidiel, neformálnych praktík a štruktúr zdrojov [2]. Slovensko, Česká republika a Francúzsko patria medzi európske krajiny s najvyšším počtom samospráv [3]. V súčasnosti sa na Slovensku nachádza 2 891 samospráv. Medzi samosprávy radíme mestá, dediny alebo štvrte [4]. Svetlík a spol. (2016) uviedol, že samosprávy v Slovenskej republike sú právnické osoby [5]. Na čele obce je starosta, ktorý je zodpovedný za správu majetku obce [6]. Mukhtar-Landgrena hovorí že, samosprávy majú rôznorodé úlohy vo fungovaní a riadení života obyvateľov [2].

Budovy samosprávy by mali byť obecný úrad, stanica mestskej polície – súčasť obecného úradu alebo samostatná budova, sklad obecnej techniky, kultúrny dom a športoviská (futbalový štadión, workoutové ihrisko, detské ihrisko a pod.). Takáto klasifikácia budov je však pomerne náročná, keďže v reálnej situácii to môže v obci vyzerať tak, že všetky vyššie popísané budovy sú centrálne umiestnené v jednej budove. Tak či onak je potrebné venovať zabezpečeniu a ochrane týchto objektov náležitú pozornosť.
Primárnou formou ochrany objektov vo všeobecnosti sú mechanické zábranné prostriedky, ktoré slúžia na ochranu osôb a majetku pred narušiteľmi a rizikami ľudského pôvodu [7]. Mechanické zábranné prostriedky tvoria základnú ochranu objektu a predmetov, ktoré sa v objekte nachádzajú [8]. Mechanické zábranné prostriedky sú prvé časti ochrany, s ktorými sa narušiteľ dostane do kontaktu, a preto ho majú najmä odradiť, spomaliť alebo zadržať.

Mechanické zábrany vytvárajú 4 všeobecné bezpečnostné zóny:

- obvodová ochrana - zabezpečuje bezpečnosť perimetra, ktorý môže byť vymedzený prirodzenou alebo umelou hranicou (plot, múr a pod.). Vo väčšine prípadov ide o rôzne typy oplotení, ale aj vjazdy a vjazdy do chráneného územia,
- plášť budovy – považuje sa za najdôležitejší. Ochranu plášťa tvoria samotné stavebné prvky - steny budovy a otvorové výplne, ktoré sú všeobecne definované ako otvorený priestor alebo „diera“ v plášti budovy,
- priestorová ochrana - je vnútorná ochrana budov, ktorá zabezpečuje interiér chráneného záujmu v budove, ide predovšetkým o interiérové dvere,
- objektová ochrana – pozostáva najmä z opatrení, ktorých úlohou je zabrániť krádeži a neoprávnenej manipulácii s chráneným majetkom – cennosťami, umeleckými dielami, patentmi a pod. [8].

Stavebné prvky alebo konštrukcia budovy patria k základným prvkom plášťovej ochrany, no v praxi sa im nevenuje veľká pozornosť. Kým prvky obvodovej ochrany

oddeľujú verejný priestor od súkromného, prvky plášťovej ochrany oddeľujú vnútorný a vonkajší priestor.
Medzi základné stavebné prvky patria:

- výrobky zo stavebnej hliny,
- skaly a kamene,
- drevo a drevené výrobky,
- betón a betónové výrobky,
- železné kovy,
- neželezné kovy,
- keramické materiály,
- polyméry [9].

Otvorové výplne
Otvorové výplne patria k najslabším miestam v plášťovej ochrane, preto je potrebné sústrediť sa na ich zabezpečenie. Základnou funkciou dverí je umožniť vstup a výstup z/do objektu. Funkciou dverí vo fyzickej bezpečnosti je zabezpečiť dostatočnú bezpečnosť v mieste vstupu alebo výstupu. Takáto bariéra, však musí byť nepriechodná pri útoku bežnými prostriedkami a ponúkať maximálny čas oneskorenia.
Účelom okien je okrem estetiky aj prepúšťanie slnečného žiarenia, zabezpečenie viditeľnosti a vetranie. Pri oknách je najslabšie miesto zasklenie. V súčasnosti poznáme niekoľko druhov bezpečnostných skiel:

- vrstvené sklo
- tabuľové sklo
- plavené sklo,
- tvrdené sklo,
- nepriestrelné sklo.

Okrem bezpečnostných skiel je možné použiť bezpečnostnú fóliu na zvýšenie prielomovej odolnosti [10].
Z daných informácií môžeme konštatovať, že vzhľadom na to, že každý objekt samosprávy môže byť špecifický, je potrebné sa naň pozerať samostatne a z hľadiska chráneného záujmu. Môže totiž nastať situácia, že dve obce majú sklady techniky, ale hodnota chráneného záujmu v nich je iná, a teda aj zabezpečenie by malo byť iné.

METÓDY

Spomalenie alebo zdraženie páchateľa patrí medzi základné funkcie MZP. To, ako dlho sa páchateľ zdrží na danom prvku MZP, teda čas, za ako dlho môže byť prekonaný MZP sa nazýva čas prielomovej odolnosti. S časom prielomovej odolnosti sa spája pojem ,,bezpečnostná odolnosť objektu‘‘, ktorá predstavuje vlastnosť objektu odolávať páchateľovi dosiahnuť jeho cieľ [11, 12].
Prielomová odolnosť závisí od mechanických vlastností materiálov, z ktorých je MZP vyrobený. Prielomovú odolnosť prvku MZP vypočítame na základe vzorca

$$T_p = t_2 - t_1$$

Pričom:
T_p – čas potrebný na prekonanie MZP,
t_1 – čas začiatku útoku,
t_2 – čas ukončenie útoku [11].

Technická norma EN 1627 stanovuje časy prielomových odolnosti otvorových výplní – dvere, okná, závesné steny, mreže a uzávery [13]. Časy prielomových odolnosti pre ručné pokusy o vlámanie podľa EN 1627 sa nachádzajú v tabuľke 1.

Tabuľka 1 Časy prielomových odolnosti [13].

Bezpečnostná trieda	Sada náradia	Čas prielomovej odolnosti [min]	Celkový čas [min]
1	Bez pokusu o prekonanie		
2	A	3	15
3	B	5	20
4	C	10	30
5	D	15	40
6	E	30	50

Pre dané bezpečnostné triedy sú definované konkrétne sady náradia spolu s časom, za ktorý by mala byť bezpečnostná trieda prekonaná danou sadou náradia. Technická norma nestanovuje časy, ako by jednotlivé bezpečnostné triedy odolávali iným triedam náradia. Cylindrické vložky sú štandardným doplnkom pri ochrane plášťovej ochrany, avšak cylindrické vložky 1. bezpečnostnej triedy sú veľmi ľahko prekonateľné aj bežne dostupnými nástrojmi. Je potrebné si uvedomiť, že otvorové výplne je potrebné otestovať komplexne a zamerať sa nielen na samotné kolíkové zámky, ale aj na kľučku, zárubňu a konštrukciu výplne steny [14]. Nakoľko neexistuje odporúčanie do akej bezpečnostnej triedy zaradiť jednotlivé stavebné prvky budov samospráv. Tie možno zaradiť do niekoľkých bezpečnostných tried podľa hodnoty chránené záujmu. Avšak, pri stanovení úrovne ochrany objektu je najlepšie vychádzať z funkčnosti systému t.j. využitie prielomových odolnosti a pravdepodobnosti detekcie a aplikovať kvantitatívny prístup a použiť takú triedu odolnosti, prípadne také množstvo MZP aby bol útočník zadržaný obecnou políciou ešte pred dosiahnutím cieľa [12]. V takomto prípade hovoríme o účinnom ochrannom systéme, v ktorom čas napadnutia - T_N, je väčší ako čas reakcie OP – T_{FO}. V prípade detekcie útočníka EZS je možné koeficient účinnosti vypočítať

$$Q_{ochr} = \frac{T_N}{T_{FO}} = \frac{T_P + T_{PRES} + T_{út} + T_{ún}}{T_{pop} + T_{ver} + T_{pres} + T_{zás}}$$

Pričom:
Q_{ochr} - koeficient účinnosti ochranných opatrení,
T_p – celkový čas prielomovej odolnosti,

T_{PRES} – celkový čas potrebný na presun,
$T_{út}$ – celkový čas útoku,
$T_{ún}$ – celkový čas úniku,
T_{pop} – čas poplachu,
T_{ver} – čas verifikácie,
T_{pres} – čas presunu na miesto zásahu,
$T_{zás}$ – čas zásahu [11].
Tu však treba počítať s tým, že obecný úrad pracuje s osobnými údajmi, ktoré môžu byť zneužité, a preto sa čas napadnutia nesmie započítavať do času úteku a pracovať len s časom prieniku do cieľa - TPRL (Tp+TPRES). V tomto prípade vypočítame koeficient účinnosti ochranných opatrení [11]:

$$Q_{ochr} = \frac{T_{PRL}}{T_{FO}}$$

VÝSLEDKY

Kryt civilnej ochrany

Pri objektoch civilnej ochrany platia požiadavky podľa viacerých osobitných predpisov, napr. [16,17]. V stručnosti je možné konštatovať, že pri objektoch CO sa nepoužívajú MZP (security barriers) ale safety barriers. Sklet hovorí, že safety barriers sa používajú na ochranu ľudí a ich majetku proti mimoriadnym udalostiam [7].

Obecný úrad

Zabezpečenie plášťovej ochrany budovy obecného úradu nie je určené. Obecný úrad je možné z hľadiska normy EN 14383-4 zaradiť do 1-2. bezpečnostnej triedy [18]. Teda podľa tabuľky 1 by to znamenalo, že prielomová odolnosť otvorových výplní by nemala byť kratšia ako 3 minúty.

Sklad obecnej techniky, kultúrny dom

Pri zabezpečovaní týchto zariadení, rovnako ako pri obecnom úrade, treba brať do úvahy vzdialenosť od objektu obecnej polície, z dôvodu včasného zásahu.
Pri objektoch, v ktorých sa osobné údaje nespracúvajú, sa pri výpočte koeficientu zohľadňuje aj doba úniku.
V nasledujúcom výpočte určíme, aký by mal byť optimálny čas zásahu pre každú odporovú triádu. Budeme predpokladať, že koeficient účinnosti ochranných opatrení je rovný 3.

Druhá bezpečnostná trieda

V prípade úniku s chráneným záujmom:

$$T_{FO} = \frac{600}{3} = 200\ s$$

V prípade druhej bezpečnostnej triedy musí byť čas zásahu kratší ako 200 sekúnd.

V prípade zničenia objektu alebo úniku informácií:

$$T_{FO} = \frac{480}{3} = 160\ s$$

Ak má útočník záujem objekt zničiť alebo získať informácie, je potrebné do 160 sekúnd zasiahnuť.

Tretia bezpečnostná trieda
V prípade úteku s chráneným záujmom:

$$T_{FO} = \frac{720}{3} = 240\ s$$

Pre tretiu bezpečnostnú triedu musí byť zásah vykonaný do 240 sekúnd.

V prípade zničenia objektu alebo úniku informácií:

$$T_{FO} = \frac{600}{3} = 200\ s$$

Ak má útočník záujem objekt zničiť alebo získať informácie, je potrebné do 200 sekúnd zasiahnuť.

Štvrtá bezpečnostná trieda
V prípade úteku s chráneným záujmom:

$$T_{FO} = \frac{1020}{3} = 340\ s$$

Pre štvrtú bezpečnostnú triedu musí byť zásah vykonaný do 340 sekúnd.

V prípade zničenia objektu alebo úniku informácií:

$$T_{FO} = \frac{900}{3} = 300\ s$$

Ak má útočník záujem objekt zničiť alebo získať informácie, je potrebné do 300 sekúnd zasiahnuť.

Piata bezpečnostná trieda
V prípade úteku s chráneným záujmom:

$$T_{FO} = \frac{1320}{3} = 440\ s$$

Pre piatu bezpečnostnú triedu musí byť zásah vykonaný do 440 sekúnd.

V prípade zničenia objektu alebo úniku informácií:

$$T_{FO} = \frac{1200}{3} = 400\ s$$

Ak má útočník záujem objekt zničiť alebo získať informácie, je potrebné zasiahnuť do 400 sekúnd.

Šiesta bezpečnostná trieda
V prípade úteku s chráneným záujmom:

$$T_{FO} = \frac{1620}{3} = 540\ s$$

Pre piatu bezpečnostnú triedu musí byť zásah vykonaný do 540 sekúnd.

V prípade zničenia objektu alebo úniku informácií:

$$T_{FO} = \frac{1500}{3} = 500\ s$$

Ak má útočník záujem objekt zničiť alebo získať informácie, je potrebné zasiahnuť do 500 sekúnd.

Pri týchto výsledkoch je potrebné poznamenať, že jednotlivé časy zásahov sú vypočítané pre možnosť, že by bol objekt zabezpečený len jednou bariérou. Ak teda stanovisko mestskej polície nie je dostatočne blízke na vykonanie zásahu v určenom čase, je potrebné zvýšiť počet zábran tak, aby bol čas útoku dlhší.

VÝSLEDKY

Pre jednotlivé objekty je potrebné, aby bola minimálna úroveň ochranný dostatočná, vzhľadom na funkčnosť systému. Funkčnosť systému dosiahneme tak, ako už bolo spomínané, že čas zásahu bude kratší ako čas útoku [18]. Avšak, v súčasnosti neexistuje databáza vstupných údajov, resp. vstupné údaje môžu byť len približné hodnoty, ktoré nemusia byť zhodné s hodnotami, ktoré budú zodpovedať realite. Pokiaľ nedisponujeme všetkými vstupnými údajmi je potrebné sa riadiť pokynmi tretích strán – štát, normalizačný úrad, poisťovne [19].

Aj pre absenciu údajov je potrebné pristupovať k hodnoteniu odolnosti pre každý objekt samostatne. Vzhľadom na veľkú rôznorodosť a nejednotnosť rozmiestnenia budov regionálnej samosprávy je ešte dôležitejšie samostatné posúdenie. Pomocou samostatného vyhodnotenia bude možné efektívne nastaviť bezpečnostné podmienky objektu. Oveľa jednoduchšie by sa dalo určiť komplexné zabezpečenie budov regionálnej samosprávy, keby všetky budovy mali rovnaké parametre, mechanické zábranné prostriedky, bezpečnostné triedy a podobne.

Samostatnou skupinou bezpečnostných požiadaviek sú finančné náklady. Mnohé samosprávy disponujú relatívne nízkym rozpočtom, ktorý postačuje na vynakladanie bežných nákladov samosprávam a odkladanie finančných rezerv na zlé obdobie. Ak by sme sa riadili odporúčaním brať ako bezpečnostnú triedu 3 pre obecný úrad, náklady by sa pri počte okien a dverí zvýšili o niekoľko stoviek eur. Finančné rozdiely napríklad pri cylindrických vložkách sú len nízke, pričom bezpečnostná trieda 2 stojí rádovo 15€, tretia bezpečnostná trieda rádovo 25€, čo predstavuje rozdiel 10€. Pri štyroch dverách to bude mať napríklad hodnotu 40€, čo nie je veľa, ale z hľadiska bezpečnosti to má veľký význam pri ochrane chráneného záujmu.

ZÁVER

Cieľom príspevku bolo poukázať na rôznorodosť pohľadov na bezpečnosť objektov samospráv. V mnohých prípadoch sa opatreniam otvorových výplni nevenuje dostatočná pozornosť, čo je vzhľadom na dôležitosť chráneného záujmu nesprávne. Práve dôležitosť chráneného záujmu je veľmi významná, keďže v prípade obecných úradov môže ísť o osobné údaje obyvateľov obce, prípadne o technické vybavenie úradu. Obe možnosti sú veľmi dôležité, nakoľko zneužitie osobných údajov obyvateľov môže priamo ovplyvniť ich finančnú situáciu a podobne. Na druhej strane v prípade krádeže technického zariadenia je len veľmi malá pravdepodobnosť, že obec bude mať dostatok financií na obstaranie nových technických zariadení Rovnako je to aj so záhradnou či inou technikou určenou na zveľadenie obce.

Hoci neexistujú priame postupy, odporúčania, ako by mal byť objekt regionálnej samosprávy zabezpečený, naše odporúčanie vychádzajúce z výpočtov v článku by sa dalo zhrnúť do dvoch kľúčových bodov. Prehliadnite si a zhodnoťte každú budovu samostatne s prihliadnutím na hodnotu chráneného záujmu a zvýšenú bezpečnosť obecných úradov minimálne na úrovni bezpečnostnej triedy 3, napriek tomu, že ide o kancelárske priestory, ktorým by stačila trieda 2.

POĎKAKOVANIE
Príspevok bol spracovaný v rámci grantového projektu KOR/7729/2021 Vplyv teploty prostredia na čas prielomovej odolnosti

LITERATÚRA

[1] TANVEER, I., JEFFREY, R.: Hazard Mitigation in Emergency Management Hazard Mitigation in Emergency Management. Butterworth-Heinemann. 2016. ISBN: 9780124201347.
[2] KRONSELL, A., MUKHTAR-LANDGREN, D.: Experimental governance: the role of municipalities in urban living labs. 2018. In: European Planning Studies Volume 26. 988-1007
[3] SPAC, P.: Reversing the Past. Municipal Splits in Slovakia After 1989. Wydział Geografii i Studiów Regionalnych Uniwersytetu Warszawskiego 2020. 28-36. In.: Miscellanea geographica – regional studies on development Vol. 25.
[4] SEBOVA, M., PETRIKOVA, D.: Impact of municipality size on economic performance. Evidence from Slovakia. 2015. 885-888. In.: Journal of applied economic sciences Issue No. 36.
[5] SVETLIK, J., KUTAJ, M., VELAS, A.: The safety training in the municipality. 2016. 1350-1355 EDULEARN16 Proceedings.
[6] KUTAJ, M., BOROS, M.: Development of educational equipment and linking educational process with research. 2017. 5172-5177. In.: 9th International Conference On Education And New Learning Technologies (Edulearn17).
[7] SKLET, S.: Safety barriers: Definition, classification, and perfirmace. 2006. In.: Journal of Loss Prevention in the Process Industries 19.
[8] MACH, V.: Bezpečnostné systémy - Mechanické bezpečnostné prostriedky, Košice, Multiprint 2010. ISBN978-80- 970410-6-9.
[9] DUGGAL, S.K.: Building Materials, First edition. USA 1998.
[10] FENNELLY, L. J.: Effective Physical Security. 5. vyd. Butterworth-Heinemann. 2017. ISBN 978-0-12-804462-9.
[11] LOVEČEK, T., REITŠPÍS J.: Projektovanie a hodnotenie systémov ochrany objektov. 1. vyd. Žilina: EDIS – vydavateľstvo ŽU 2011. ISBN 978-80-554-0457-8.
[12] VELAS, A., LENKO, F., BOROS, M., MOLOVCAKOVA, N.: Skill needs of physical security labor market in Slovakia. 2019. 8189-8194. In: ICERI 2019: Conference proceedings: 12th International conference of education, research and innovation.
[13] EN 1627 - Dvere, okná, závesné steny, mreže a uzávery. Odolnosť proti vlámaniu. Požiadavky a triedenie.

[14] SISER, A., MARIS, L., REHAK, D., PELLOWSKI, W.: The use of expert judgement as the method to obtain delay time values of passive barriers in the context of the physical protection system. 2018 In: 2018 IEEE International Carnahan Conference on Security Technology: conference USB proceedings.
[15] KAMPOVA, K.: Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republik,. 2020. In.: International Journal of critical infrastructure protection.
[16] Vyhláška Ministerstva životného prostredia Slovenskej republiky č. 453/2000 Z. z.
[17] Vyhláška Ministerstva životného prostredia Slovenskej republiky č. 532/2002 Z. z.
[18] EN 14383-4 - Predchádzanie zločinnosti. Územné plánovanie a navrhovanie. Časť 4: Obchodné a administratívne priestory.
[19] ZVAKOVA, Z., VELAS, A., MACH, V.: Security in the transport of valuables and cash. 2018. 1209-1214. In: Transport Means - Proceedings of the International Conference.
[20] LOVECEK, T.: Bezpecnostne systemy - Planovanie a projektovanie systemov ochrany objektov. Zilina: EDIS 2018. ISBN: 97-80-554-1482-9.

MATEMATICKÁ PREDIKCIA ŠÍRENIA PANDÉMIE COVID-19 NA SLOVENSKU – DOSTUPNÉ ZDROJE

prof. Ing. Zdeněk Dvořák, PhD. a Ing. Peter Piala, PhD.

ABSTRAKT
Počiatkom roku 2020 sa z Číny postupne začala šíriť pandémia COVID-19. Respiračné ochorenie, ktoré postupne prinášalo ťažké stavy a úmrtia. V Európe sa COVID-19 začas šíriť z viacerých miest. Postupne prenikol i na Slovenskom prvý prípad bo zaznamenaný 19.3.2020. Hneď od počiatku boli vytvárané matematické modely pravdepodobného šírenie pandémie. Cieľom článku je predstaviť analýzu dostupných matematických modelov, ktoré boli a sú používané na predikciu COVID-19.

Kľúčové slová:
COVID-19, matematický model, pandémia, Slovensko

ABSTRACT
At the beginning of 2020, the COVID-19 pandemic gradually began to spread from China. A respiratory disease that gradually brought severe conditions and deaths. In Europe, COVID-19 is currently spreading from several cities. The first case gradually recorded in Slovakia was recorded on March 19, 2020. From the outset, mathematical models of the likely spread of a pandemic have been developed. The aim of the article is to present an analysis of available mathematical models that have been and are used to predict COVID-19.

Key words:
COVID-19, mathematical model, pandemic, Slovakia

1 ÚVOD
Výskum v oblasti monitorovania a trasovania pohybu osôb sa v rôznych výskumných inštitúciách vykonáva dlhodobo. Zameranie článku je zúžené do zdravotníckych zariadení a zároveň pre potreby monitorovania a trasovania osôb nakazených COVID-19. Cieľom riešeného projektu je analyzovať právne možnosti, ekonomické, zdravotnícke a bezpečnostné dopady monitorovania osôb a kontaktov v

zdravotníckych zariadeniach a následne vytvoriť a aplikovať systém na monitorovanie a trasovanie osôb a ich kontaktov v zdravotníckych zariadeniach, s následným možným využitím vo verejne prístupných priestoroch, resp. priestoroch, kde je predpokladaný pohyb veľkého počtu ľudí. V rámci riešeného projektu je definovaných celkom päť cieľov a 16 úloh. Jasne definovaná úloha smerované k matematickej predikcii šírenia pandémie COVID-19 medzi uvedenými úlohami nie je. Aktuálne výskumníci riešia etapu Komplexná analýza a začínajú riešiť etapu Modelovanie systému monitorovania osôb a ich kontaktov – model a metodika. V rámci riešenia je nutné každodenne monitorovať a analyzovať nové informácie, ktoré prináša život a konfrontovať ich s modelmi predikcie, ktoré boli vytvorené skôr. Na ich úspešnosti závisí systém opatrení, ktorý každá jednotlivá krajina v danom čase nastaví [1].

Pandémia COVID-19 veľmi skomplikovala život celej spoločnosti, vznikli obrovské hmotné i nehmotné škody. K aktuálnemu termínu (začiatok roka 2022) PCR testy na Slovensku od začiatku pandémie odhalili takmer 884-tisíc nakazených koronavírusom. K tomuto dátumu si pandémia Covid-19 v SR vyžiadala 17 398 obetí. Aktuálnym problémom je začiatok šírenia nového variantu mikrón. Z dôvodu jeho nástupu začali platiť nové pravidlá pre život slovenskej spoločnosti v blížiacej sa vlne variantu mikrón [2].

Výskum bezpečnosti vyžaduje kvalitné matematické riešenia, hĺbkové analýzy stabilných i pohyblivých premenných. V rámci výskumu sa tímy na Žilinskej univerzite v rámci jednotlivých riešených tém venujú rôznym častiam bezpečnosti (pilierom bezpečnosti), ktoré vychádzajú z teoretických základov – bezpečnosti a ochrany zdravia pri práci, požiarnej bezpečnosti, informačnej bezpečnosti, technickej a technologickej bezpečnosti, ochrany osôb a majetku, resilience a zraniteľnosti objektov.

Predmetný článok je prvým zo série článkov na tému matematická predikcia šírenia pandémie COVID-19. Cieľom článku je prezentácia dostupných informačných zdrojov a analýzy dostupných údajov, ktoré sú aktuálne autorom dostupné. Článok tak predkladá k diskusii možnosti dostupných informačných zdrojov a dostupných údajov.

2 ANALÝZA DOSTUPNÝCH ZDROJOV

Každá analýza dostupných zdrojov musí vychádzať z reálneho právneho prostredia, existujúcich technických noriem a najlepšej praxe s ktorou sa stretávame. Dnešný globalizovaný svet odmieta „naše domáce riešenia“ a vyžaduje všeobecné univerzálne riešenia. V rámci riešenia otázok bezpečnosti a ochrany je veľmi ťažké, niekedy až nemožné opísať všetky teoreticky možné scenáre, ktoré môžu nastať. Autori článku preto dlhodobo diskutujú každý metodický prístup, každé konkrétne riešenie s jeho hranicami.

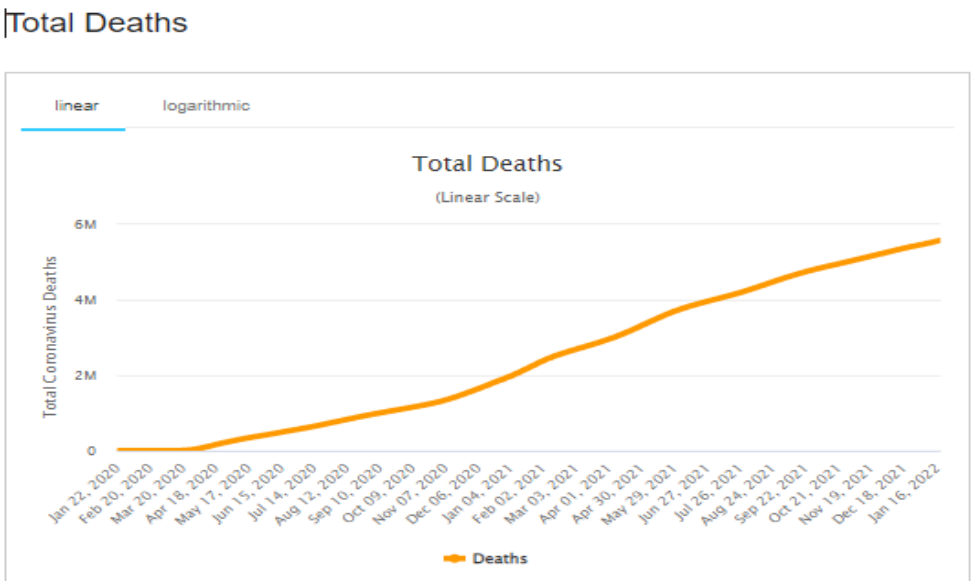
V rámci analýzy dostupných zdrojov tak bola pozornosť sústredená prioritne na informačné zdroje na internete, ďalej na vedecko odborné databázy a na profesijné informačné portály. Ako reálny zdroj informácií boli využité i zdroje bežnej dennej tlače, kde boli jednotlivé informácie konfrontované s ďalšími informačnými zdrojmi.

2.1 ANALÝZA ZAHRANIČNÝCH INFORMAČNÝCH ZDROJOV

Hlavným informačným zdrojom v medzinárodnom meradle je web stránka Svetovej zdravotníckej organizácie (ďalej WHO). Na nej je špeciálna sekcia, ktorá sa venuje COVID-19. V rámci analýzy informačných zdrojov sú tu dostupné plnotextové články v počte 381 303, z toho databáza MEDLINE 230 406 článkov, databáza Scopus 36 842 článkov, databáza Web of Science 30 444 článkov. Ďalej nasledujú ostatné databázy, priamo na stránke WHO je publikovaných 6664 článkov na tému COVID-19. Z celého počtu je 504 článkov venovaných prognostických štúdiám. Najviac článkov na témy prognostické štúdiu uverejnil časopis Sustainability a ďalej International Journal of Environmnetal Research and Public Health. Jednotlivé články boli prevažne zamerané na prognózy rastu COVID-19 v jednotlivých krajinách. Autori nenašli článok, ktorý by prognózoval vývoj počtu nakazených na COVID-19 v globálnom meradle. Podľa ďalej uvedených detailných analýz je zrejmé, že jednotlivé krajiny sveta majú vlastné modely šírenia COVID-19. Vždy má kľúčové postavenie rýchlosť šírenia, stav opatrení v jednotlivých krajinách, kvalita a stav zdravotníctva v danej krajine [3].

Ďalším globálnym informačným zdrojom je web worldometers, ktorý v reálnom čase prezentuje aktuálne zmeny vybraných ukazovateľov. Okrem všeobecných informácií štatistického charakteru o zmenách v počte ľudí, niektorých ekonomických ukazovateľoch sa autori zamerali aj na COVID-19. Podľa uvedeného zdroja v čase spracovania článku (január 2022) na Zemi žije 7,921 miliárd ľudí. Covid-19 bol príčinou prvých oficiálnych úmrtí 23.1.2020, hranica 1 000 mŕtvych za jeden deň bola prekročená 18.3.2020, hranica 5 000 mŕtvych za jeden deň 1.4.2020, hranica 10 000 mŕtvych za jeden deň 17.11.2020, hranica 15 000 mŕtvych za jeden deň 6.2021, zároveň v ten deň bola prekročená hranica 2 milióny mŕtvych globálne, hranica 3 milióny mŕtvych bola prekročená 5.4.2021, hranica 4 milióny mŕtvych bola prekročená 2.7.2021 a hranica 5 miliónov mŕtvych za celé obdobie pandémie bola prekročená 27.10.2021 [4].

V období od septembra 2021 do januára 2022 sa celkový počet za jeden deň globálne pohyboval v rozpätí 5 000 – 10 000 mŕtvych. Globálny rast počtu mŕtvych je graficky znázornený na obrázku č. 1.



Obrázok 1 Grafické znázornenie počtu mŕtvych v období 22.1.2020-16.1.2022 [4]

V článku Quantitative analysis and mathematic modelling of the global outbreak of COVID-19 autori popísali globálny pohľad na šírenie COVID-19. [5].

V článku Overview of Safety Measures at Selected Airports during the COVID-19 Pandemic autorky okrem iného opísali spôsoby hodnotenia merania efektívnosti opatrení proti COVID-19.

2.2 ANALÝZA DOMÁCICH INFORMAČNÝCH ZDROJOV

Právne normy

Údaje a informácie využité v článku boli spracované v súlade so zákonom č. 153/2013 o národnom zdravotníckom informačnom systéme. Uvedený zákon definuje národný zdravotnícky informačný systém: „súbor zdravotníckych informačných systémov v správe národného centra slúžiacich na zber, spracúvanie a poskytovanie informácií v zdravotníctve určených na správu údajovej základne; súčasťou národného zdravotníckeho informačného systému je aj Národný portál zdravia“. Ďalej definuje údajovú základňu, národné zdravotnícke administratívne registre, štandardy zdravotníckej informatiky, elektronický zdravotný záznam a elektronický preukaz zdravotníckeho pracovníka.

Reálny výskum v oblasti matematickej predikcie šírenia pandémie COVID-19 sa opiera o údaje z národných zdravotníckych registrov. Národné centrum zdravotníckych informácií vedie zoznam hlásení o úmrtí a príčinách smrti, o hlásení prijatia do ústavu zdravotníckej starostlivosti. Údaje zo štatistických zisťovaní v zdravotníctve sú dôvernými štatistickými údajmi. Agregované údaje zo zdravotných štatistických zisťovaní sa využívajú v štátnej štatistike a slúžia aj na medzinárodné porovnávanie. Vybrané údaje zo štatistických zisťovaní je možné využívať na vedecké účely [7].

Ďalším významným dokumentom v národnom prostredí je vyhláška č.107/2015 o štandardoch zdravotníckej informatiky a lehoty poskytovania údajov. Jej súčasťou sú exaktne určené číselníky, za ktoré má zodpovednosť Ministerstvo zdravotníctva SR, Úrad verejného zdravotníctva SR, Štátny úrad pre kontrolu liečiv a Národné centrum zdravotníckych informácií [8].

V zákone č. 540/2001 o štátnej štatistike je definovaný postup – „systematická a plánovitá činnosť vo verejnom záujme, ktorej predmetom je získavanie, spracúvanie, šírenie, poskytovanie a hodnotenie údajov o javoch hromadnej povahy, zabezpečovanie ich porovnateľnosti na posudzovanie sociálno-ekonomického vývoja SR“ [9].

Publikácie

V publikácii Verejné zdravotníctvo bol a pozornosť zameraná na stratégie a priority verejného zdravotníctva, prioritne v oblasti epidemiológie. Detailne na ochranu a podporu zdravia v prevencii nadváhy a obezity, v podpore pohybových aktivít, v oblasti informatizácie vyhľadávať rizikové faktory chronických neinfekčných ochorení a v prevencii nadmerného požívania alkoholických nápojov. Vzhľadom na vydanie uvedenej publikácie v roku 2019 nebola pozornosť venovaná epidemiologickým problémom [10].

V publikácii Verejné zdravotníctvo vydanej v roku 2009 sa autor zameral na predstavenie právneho systému verejného zdravotníctva, na priority a vývoj politík v oblasti verejného zdravotníctva. V závere publikácie boli definované odporúčania pre Ministerstvo zdravotníctva SR. Relevantnou k obsahu článkuje časť, ktorá sa venuje výskumu v oblasti verejného zdravotníctva, podpore spoločnej európskej politiky verejného zdravotníctva a myšlienky – myslieť globálne a konať lokálne [11].

Inštitúcie

Reálny a oficiálny zdroj informácií je k dispozícii na webe Národného centra zdravotníckych informácií (ďalej NZCI) [12]. V rámci uvedeného webu vznikla stránka korona.gov.sk, ktorá v šiestich jazykoch prináša aktuálne informácie o vývoji pandémie COVID-19 na Slovensku [13]. Sú tu uvedené denné štatistiky, možnosť generovať grafy za vybrané časové obdobie. Je tu možnosť prihlásiť sa na očkovanie, testovanie, vyplniť formulár eHranica a vyžiadať si Covid preukaz EU. Sú tu dostupné aplikácie na zmenu termínu očkovania, ďalej sú uvedené aktuálne opatrenia a informácie o COVID-19. Následne je dostupná Covid Automat – aplikácie, ktoré sa využíva do určitého stupňa rozšírenia vírusu v spoločnosti. Veľmi dôležitými časťami sú informačné linky COVID-19 a dostupné aplikácie na Google Play, App Store a odpovedi na frekventované otázky.

Ďalším oficiálnym zdrojom sú informácie na stránke Ministerstva zdravotníctva Slovenskej republiky, v časti Inštitút zdravotných analýz SR [14]. Reálne analýzy sú bohužiaľ publikované len do dátumu február 2021.

Tieto zdroje sú využívané aj ďalšími organizáciami a inštitúciami, ktoré si dali za cieľ informovať o pandémii COVID-19. Príkladom dobrej praxe je aktivita nezávislej občianskej iniciatívy Dáta bez pátosu, ktorá v reálnom čase publikuje svoje analýzy a grafy. Bohužiaľ od októbra 2021 prestali publikovať nové informácie a aktuálne ich ponúkajú na svojej facebookovej stránke.

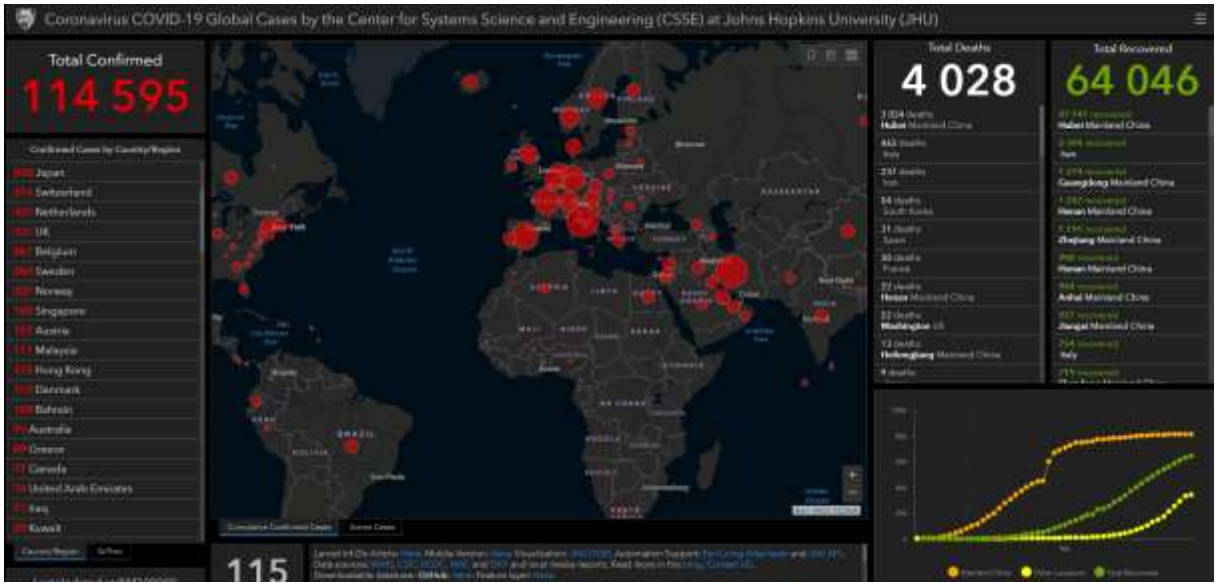
Výskumné projekty

Okrem uvedených oficiálnych štátnych zdrojov boli vo výskume využité informácie o projektoch podporených Agentúra na podporu výskumu a vývoja (ďalej APVV) na výzvu - Podpora výskumu a vývoja so zameraním na zvládnutie pandémie koronavírusu a jej dopadov na obdobie rokov 2020-2021. Prehľad podporených projektov je dostupný na linku https://www.apvv.sk/buxus/docs/vyzvy/programy/COVID2020/vysledky/PP-COVID-2020_rozhodnutia.pdf. Celkovo bolo podporených 24 výskumných projektov rôzneho zamerania s dobou riešenia od 16.9.2020 do 31.12.2021. Prevažne sa jednalo o projekty aplikovaného výskumu s reálnymi výstupmi pre prax.

2.3 ANALÝZA DOSTUPNÝCH ÚDAJOV

Začiatok pandémie

Po analýze právneho a inštitucionálneho rámca, uvedení vybraných publikácií a výskumných projektov riešených v rámci APVV je potrebné prezentovať dostupné údaje. Od počiatku globálnej pandémie údaje o náraste prípadov publikovala Hopkins university. Napríklad 10.3.2020 bol publikovaný tento stav počtu nakazených

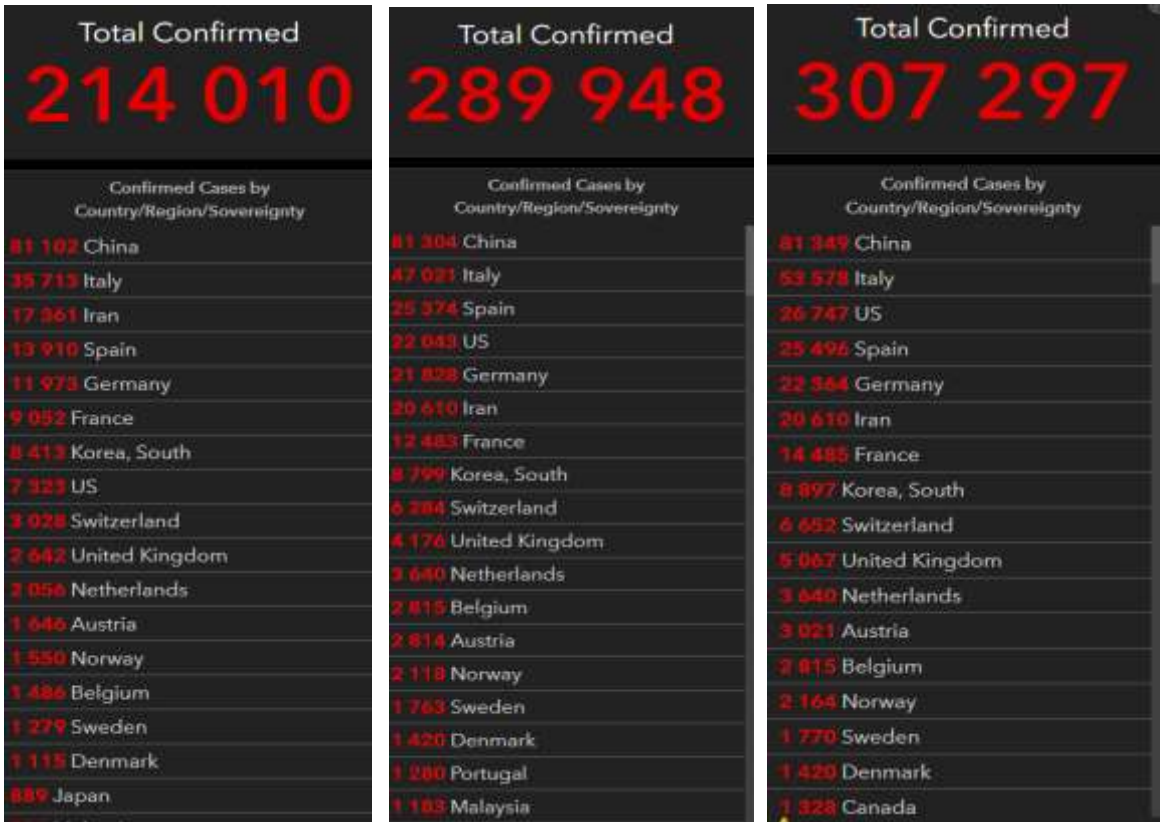


Obrázok 1 Schematické celkové počty nakazených COVID-19 [13]

Z pohľadu rýchlosti šírenia boli dôležité aj prehľady po jednotlivých krajinách, na obrázku 2 je prehľad potvrdených prípadov nákazy COVID-19 ku dňu 15.3.2020.

Obrázok 2 Krajiny s najvyšším počtom nakazených dňa 15.3.2020 [13]

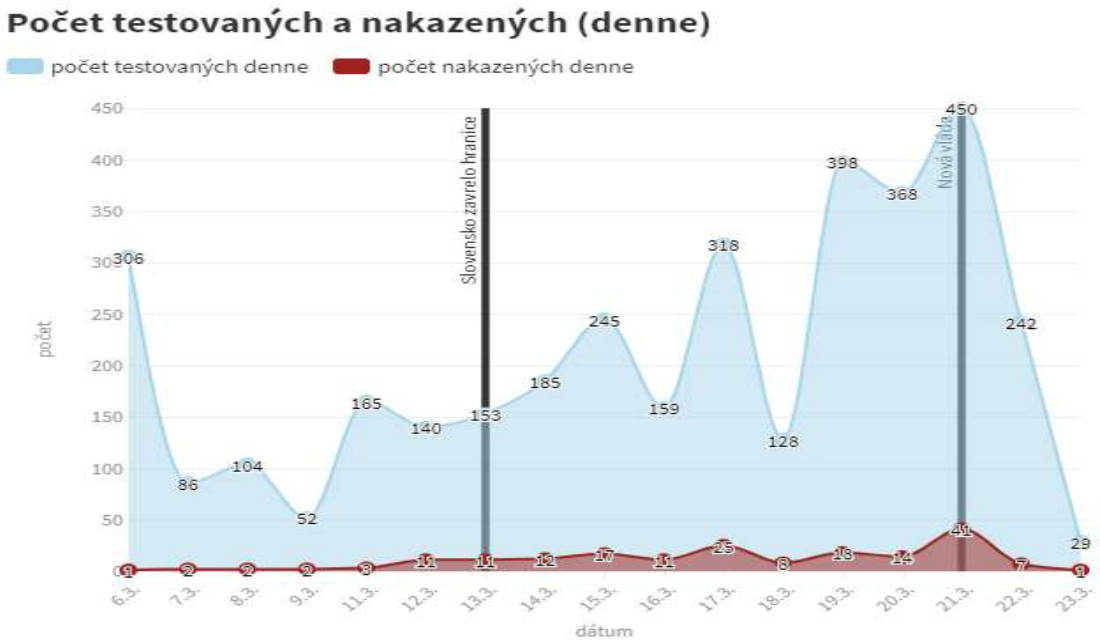
Ďalší nárast počtu infikovaných bol veľmi rýchly, na nasledovnom obrázku sú uvedené tri prehľady najviac zasiahnutých krajín v období od 18.3. do 22.3.2020.



Obrázok 3 Krajiny s najvyšším počtom nakazených v dňoch 18.3., 21.3. a 22.3. 2020 [13]

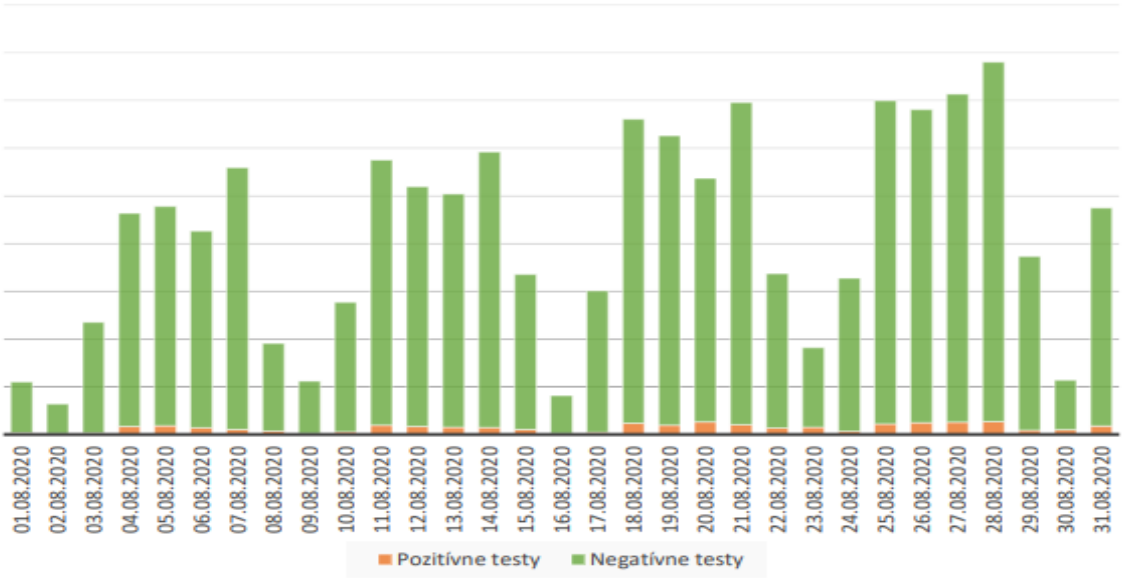
Zreteľný je nástup pandémie v krajinách – Taliansko, Španielsko, a USA, oproti tomu Čína a Južná Kórea uvádzali minimálny prírastok ochorení.

V začiatku pandémie na Slovensku bolo testovaných pomerne málo pacientov, úvodný graf prezentujúci denný nárast testovaných a nakazených ja na obrázku 4.

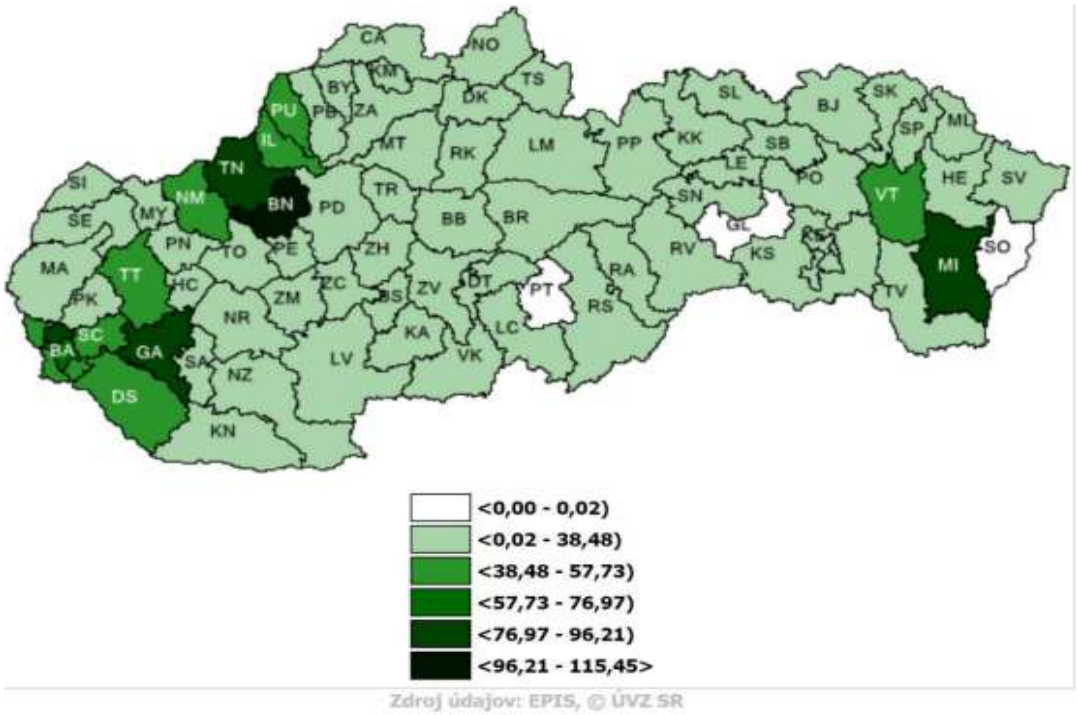


Obrázok 4 Počet testovaných a nakazených na Slovensku v marci 2020 [12]

Prvé týždne a mesiace pandémie boli na Slovensku v znamení prísnych opatrení, vírus sa šíril relatívne pomaly, v medzinárodných porovnaniach patrilo Slovensko minimálnym počtom nakazeným k najlepším v Európe. Napríklad v auguste 2020 bolo celkom vykonaných 73 422 testov, z ktorých bolo pozitívny 1526, t.j. miera pozitivity2,07%. Nasledujúci graf počet vykonaných testov a mieru pozitivity za mesiac august 2020.



Obrázok 5 Počet testovaných a nakazených na Slovensku v auguste 2020 [12]



Obrázok 6 Počet pozitívnych osôb na 100 000 obyvateľov 1.-31.8.2020 Slovensko [12]

Vďaka systematickému do hľadávaniu kontaktov sa COVID-19 šíril prevažne importom z iných krajín. V priebehu mesiaca august bol importovaných nákaz 137 prípadov z Ukrajiny, 58 z Chorvátska, 54 z Českej republiky, 20 zo Srbska, 11 z Rumunska, Maďarska a Afganistanu a 10 z Rakúska. Počet do hľadaných importovaných nákaz z iných krajín bol v rádu jednotiek. Počas mesiaca august 2020 bolo registrovaných celkom 37 úmrtí na COVID-19, z toho štyria pacienti vo veku 55-64 a 33 pacientov vo vekovej skupine 65+.

V období konca roku 2020 boli vykonané plošné testovania obyvateľstva SR. Prvé kolo testovaní prebehlo 7.-8.11.2020 a druhé kolo 21.-22.11.2020. V prvom kole bola miera pozitívnych výsledkov 0,7%, v druhom kole okolo 1%, celková účasť na druhom kole bola 3,625 tisíc t.j 67% všetkých občanov SR.

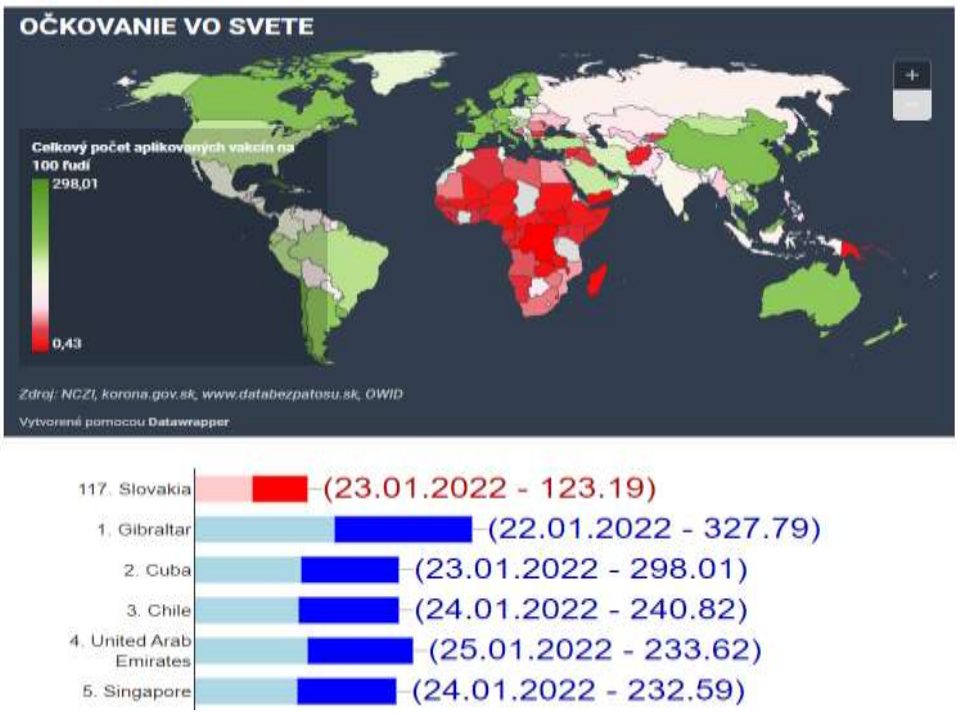
V ďalšom priebehu došlo k výraznej zmene správania obyvateľstva, v súvislosti s očkovaním, vznikla vládna kríza, z riešenia pandémie na Slovensku sa stal politický boj.

Očkovanie pro COVID-19

Výrazný vplav na šírenie COVID-19 vo svete má očkovanie, ktoré sa postupne zaviedlo od konca roku 2020. Dnes jednotlivé krajiny evidujú počty pozitívne testovaných, počty hospitalizovaných, počty pacientov na jednotkách intenzívnej starostlivosti, počty zomretých s alebo na COVID-19. Prvé obdobie bolo zamerané na zaočkovanie maximálneho počtu najohrozenejších občanov. Jednotlivé očkovacie stratégie sa veľmi líšili. Počiatočná eufória počiatkom roku 2021 na Slovensku bola

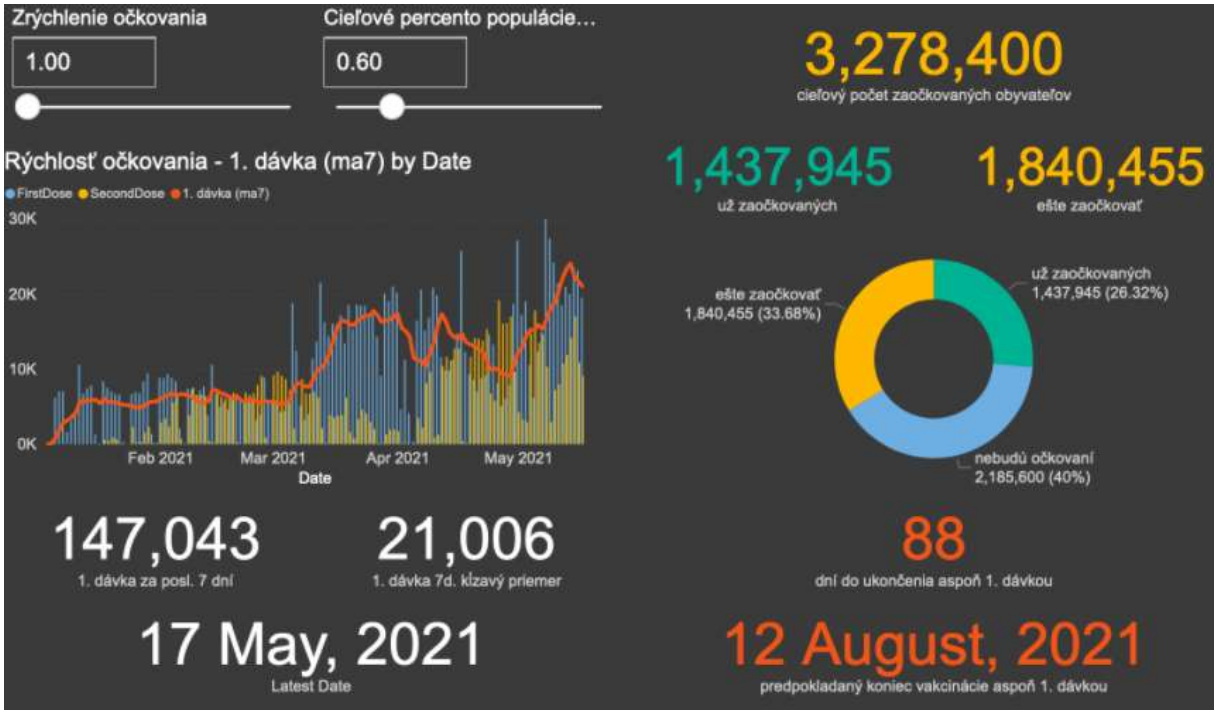
v polovine roku 2021 zmenená na relatívny nezáujem zo strany občanov. Druhá polovina roku 2021 priniesla i možnosť očkovať deti a mladistvých.

Na obrázku 7 je uvedený globálny grafický prehľad aplikovaných očkovacích látok v prepočtu na 100 tisíc obyvateľov. Z uvedeného grafického znázornenia vyplýva záver, že ekonomicky rozvinuté krajiny majú výrazne vyšší podiel počtu zaočkovaných než rozvojové krajiny. K aktuálnemu dátumu je Slovenská republika na 117 mieste, čo nás radí do 2. poloviny krajín.



Obrázok 7 Globálny počet očkovaných proti COVID-19 [17]

Vďaka aktivite neziskovej organizácie Dáta bez pátosu, sme mali možnosť do októbra 2021 pravidelne čítať rôzne zaujímavé porovnania a grafy. Jedným z kvalitných príkladov bol dátový expert publikovaný 18.5.2021, kde bola údajová analýza predpokladaného dosiahnutia 60 percentnej zaočkovanosti v SR. Podľa uvedeného modelu 60 % hranica mala byť dosiahnutá 12.8.2021.



Obrázok 8 Dashbord rýchlosť očkovania zo dňa 18.5.2021 [17]

V čase písania článku podľa Korona.gov.sk bolo dňa 26.1.2022 na Slovensku zaočkovaných 2 791 tisíc občanov a do dosiahnutia 60 % hranice aktuálne chýba 509 tisíc ľudí. Zároveň podľa uvedeného zdroja je aktuálne hospitalizovaných 1505 pacientov a z toho je 81 % nezaočkovaných. Uvedený trend bohužiaľ viedol k vysokému počtu úmrtí na COVID-19 na úrovni 17 725 ľudí od začiatku pandémie v SR.

Aktuálna situácia pandémie vo svete a na Slovensku

Začiatok januára 2022 znamenal vo svete nástup nového variantu COVID-19 s označením Omikrón, ktorý sa po svete rozšíril údajne z Juhoafrickej republiky. Jednotlivé krajiny postupne menia opatrenia, tie ktoré majú vysokú zaočkovanosť. V čase spracovania článku je rozširovanie variantu Omikrón veľmi rýchle, Európske štáty vďaka vysokému počtu vykonaných PCRR testov zaznamenávajú rekordné počty nakazených. V slovenskej republike dochádza z výraznému šíreniu COVID-19, ale stav pozitívnych testov, pre nízky počet testovaných nie je rekordný.

Z pohľadu výskumu dopadov pandémie COVID-19 je dôležité sledovať najmä úmrtnosť na COVID-19. Nasledovný obrázok zachycuje trend priemerného počtu zomretých za obdobie pandémie COVID-19 v porovnaní s priemerom za predošlých päť rokov. Jednoznačne sa v kategórii nad 65 rokov potvrdila zvýšená úmrtnosť

Tabuľka 1 Porovnanie počtu úmrtí na Slovensku v rokoch 2020-2021 [14]

Zomretí v SR podľa mesiaca úmrtia v roku 2021					
Zomretí podľa mesiaca úmrtia, veku, pohlavia a príčiny smrti - SR-oblasť-kraj (mesačne) [om3801mr]					
obdobie	**POROVNANIE**				
	2021	**priemer predošlých 5 r.** (2016 - 2020)	*index zmeny 2021 / priemer predošlých 5 r.**	**rozdiel 2021 k priemeru predošlých 5 r.***	**2020**
	osôb	osôb		osôb	osôb
ROK spolu	**73 121**	54 576	*134,0*	18 545	59 089
január	**9 081**	5 146	*176,5*	3 935	4 991
február	**8 038**	4 763	*168,8*	3 275	4 690
marec	**7 589**	4 891	*155,2*	2 698	4 995
apríl	**5 511**	4 303	*128,1*	1 208	4 282
máj	**4 675**	4 248	*110,0*	427	4 229
jún	**4 444**	4 047	*109,8*	397	4 057
júl	**4 296**	4 220	*101,8*	76	4 276
august	**4 274**	4 265	*100,2*	9	4 436
september	**4 622**	4 185	*110,4*	437	4 327
október	**5 662**	4 624	*122,4*	1 038	5 389
november	**7 471**	4 680	*159,6*	2 791	6 051
december	**7 458**	5 205	*143,3*	2 253	7 366

* Priemer za rovnaké obdobie za roky 2016 — 2020.

Údaje za rok 2020 sú definitívne, údaje za rok 2021 sú predbežné.

Z uvedeného prehľadu jednoznačne vyplýva, že v roku 2021 zomrelo o 32 percent viac obyvateľov Slovenska než tomu bolo v priemere v predošlých piatich rokoch.

4 DISKUSIA VÝSLEDKOV

Výskum v oblasti monitorovania a trasovania pohybu osôb sa vykonáva v rôznych výskumných inštitúciách. Pre všetkých výskumníkov je kľúčové získať hodnoverné údaje, tieto údaje preveriť z viacerých zdrojov a na základe logických postupov definovať hypotézy, ktoré budeme následne potvrdzovať, alebo vyvracať.

Tento článok je vstupom do problematiky, autori si dali za cieľ vytvoriť sériu článkov na tému matematická predikcia šírenia pandémie CVOVID-19. Každý matematický výpočet je nutné oprieť o seriózne údaje. Získavanie hodnoverných a pravdivých údajov v rámci prebiehajúcej explózie informácií šírených po internete je

jednou zo zložitých výziev súčasnej vedy. Ľubovoľne zobrazené údaje je vždy nutné preveriť z viacerých zdrojov. V našom prípade sme cielene zamerali pozornosť na údaje dostupné na stránkach Ministerstva zdravotníctva SR a jeho podriadených súčastí a na stránkach Štatistického úradu SR [14-17]. Zahraničné zdroje boli pre výskum preberané z obvyklých globálnych zdrojov, ktorými sú výskumné články a informačné portály svetových organizácií a významných svetových univerzít. Práve Center for Systems Science and Engineering (CSSE) at Johns Hopkins University sa stalo od začiatku pandémie jedných z overených globálnych zdrojov, ktoré v reálnom čase poskytovali a poskytujú štatistiky o pandémii COVID-19 a globálnej úrovni [18].

5 ZÁVER

Význam matematizácie všetkých činností okolo nás je zásadný. S nástupom internetu vecí je možné predpokladať, že všetky procesy okolo nás budú postupne digitalizované. Oblasť bezpečnostných vied v porovnaní s inými vedami je v matematizáci bezpečnostných procesov v začiatku. Súčasné globálne potreby smerujú meraniu všetkých teoreticky možných veličín za účelom definovanie stavu bezpečnosti. Z uvedeného dôvodu sú merané veličiny bude fyzikálneho charakteru, alebo sú merané pomerovo a prezentované najčastejšie v podobe farieb semafora, kde červená znamená najvyšší stupeň ohrozenia, žltá stredný stupeň a zelená znamená relatívne najlepšie hodnoty.

Výskumný projekt zameraný na monitorovanie a trasovanie pohybu osôb je smerovaný do priestorov nemocníc, kde sa predpokladá vybavenie vhodnou informačno-komunikačnou technikou, akceptáciou technických a organizačných opatrení vlastnými zamestnancami i pacientami. Projekt je aktuálne v prvotnej fáze riešenie, kde sú zhromažďované všetky dostupné informácie, tie následne sú analyzované a verifikované.

Podpora: vydanie článku bolo podporené projektom APVV-20-0457 Monitorovanie a trasovanie pohybu osôb v zdravotníckych zariadeniach.

LITERATÚRA

[1] Dokumentácia projektu APVV-20-0457 Monitorovanie a trasovanie pohybu osôb v zdravotníckych zariadeniach
[2] SME, 19.1.2022, online https://domov.sme.sk/c/22822867/koronavirus-slovensko-covid-omikron-online-minuta-po-minute-19-januar.html?ref=njct
[3] WHO-Coronavirus, 19.1.2022, online
https://www.who.int/emergencies/diseases/novel-coronavirus-2019
[4] WORLDOMETERS, 19.1.2022, online
https://www.worldometers.info/coronavirus/

[5] YANYAN, J., XUEFENG J., WENJUN T., JINGMING Z.: Quantitative analysis and mathematic modelling of the global outbreak of COVID-19, The Journal of Infection in Developing Countries, 2020, 14 (10):1106-1110.
[6] BLIŠŤANOVÁ, M. TIRPÁKOVÁ, M., BRUNOVÁ, Ľ.: Overview of Safety Measures at Selected Airports during the COVID-19 Pandemic, Sustaiablity, 2021, 13, 8499, doi.org/10.3390/su13158499
[7] Zákon č. 153/2013 o národnom zdravotníckom informačnom systéme
[8] Vyhláška č.107/2015 o štandardoch zdravotníckej informatiky a lehoty poskytovania údajov
[9] Zákon č. 540/2001 o štátnej štatistike
[10] KLIMENT, C. a kol.: Verejné zdravotníctvo, Úrad verejného zdravotníctva Slovenskej republiky, 2019, ISBN 978-80-89057-80-1, 431 s.
[11] ROVNÝ, I.: Verejné zdravotníctvo, Herba, spol.s.r.o. Bratislava, 2009, ISBN 978-80-89171-60-6, 125 s.
[12] Národné centrum zdravotníckych informácií, 21.1.2022, online https://www.nczisk.sk/Pages/default.aspx
[13] Center for Systems Science and Engineering (CSSE) at Johns Hopkins University, marec 2020, online https://gisanddata.maps.arcgis.com/apps/dashboards
[14] Štatistický úrad SR, 22.1.2022, online https://slovak.statistics.sk/
[15] Korona.gov.sk, 21.1.2022, online https://korona.gov.sk/
[16] Inštitút zdravotných analýz, 21.2.2022, online https://www.health.gov.sk/?iza
[17] Dáta bez pátosu, 21.1.2022, online https://databezpatosu.sk/
[18] Hopkins university, 22.1.2022, online https://coronavirus.jhu.edu/map.html

AKTUÁLNÍ PROBLÉMY VZDĚLÁVÁNÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Petr Hrůza *)

ABSTRAKT

Informační systémy na celém světě v současnosti zpracovávají stále více a více důležitých informací. Obecným trendem na celém světě je v současné době kvalitní ochrana informačních technologií před útoky, které by mohly ohrozit jejich fungování. Cílené útoky proti informačním technologiím jsou celosvětovým fenoménem a jejich dopad způsobuje rozsáhlé ekonomické škody ve veřejném i v soukromém sektoru, a to jak v národním tak v globálním měřítku. Nejzranitelnějším prvkem celého systému jsou uživatelé. Proto je potřeba nejen profesionály, ale i uživatele soustavně vzdělávat.

Klíčové slova: kybernetická bezpečnost, počítačová síť, zaměstnanec, školení

ABSTRACT

Information systems around the world are currently processing more and more important information. The general trend around the world today is to provide high-quality information technology protection against attacks that could jeopardize its operation. Targeted attacks on information technology are a global phenomenon and their impact causes extensive economic damage in both the public and private sectors, nationally and globally. Users are the most vulnerable element of the whole system. Therefore, it is necessary not only to systematically educate professionals, but also users.

Key words: Cyber Security, Computer Network, Employee, Training

1 VÝZNAM INFORMACÍ A BEZPEČNOSTI

V dnešní uspěchané době jsou informace pro organizace klíčové. Neexistuje organizace (ať již se jedná o komerční subjekt nebo orgán veřejné správy), která by nějakými důležitými informacemi nedisponovala. Výrazný nárůst zavádění a

*) doc. Ing. Petr Hrůza, Ph.D., Univerzita obrany, Kounicova 65 Brno, petr.hruza@unob.cz

používání informačních technologií vede k vytvoření informační společnosti, urychlení komunikace a velkému rozvoji služeb. Tím ale narůstá závislost společnosti na těchto technologiích. Stále větší část ekonomických aktivit se přesouvá do prostředí kyberprostoru. Vznikem sociálních sítí se z nejznámější části kyberprostoru stává významný celospolečenský jev, jehož prostřednictvím lze společnost výrazně pozitivně nebo i negativně ovlivňovat. Se vzrůstající závislostí společnosti na informačních technologiích stoupá riziko jejich zneužívání, které může vést ke značným škodám. S obrovským rozvojem technologií dnes lidstvo přechází do pátého rozměru, do virtuálního světa. Všechno, co se dnes děje v naší realitě, doprovázejí také aktivity ve virtuálním kyberprostoru. Proto se celosvětovým problémem stávají i rostoucí kybernetické útoky.

Obecným trendem na celém světě je v současné době kvalitní ochrana informačních technologií před útoky, které by mohly ohrozit jejich fungování. Cílené útoky proti informačním technologiím jsou celosvětovým fenoménem a jejich dopad způsobuje rozsáhlé ekonomické škody ve veřejném i v soukromém sektoru, a to jak v národním tak v globálním měřítku. V případech, kdy je útok veden proti prvkům kritické infrastruktury, může být v konečném důsledku ohrožena bezpečnost nebo samotná existence státu. Útoky v kyberprostoru mohou být, jsou a také budou levné a rychlé, ale především velice nebezpečné a ničivé. [1]

Informační systémy na celém světě v současnosti zpracovávají stále více a více důležitých informací. Protože se mnohdy jedná o informace s nezanedbatelnou hodnotou (např. zdravotní záznamy, daňová přiznání, bankovní účty, elektronické platební nástroje, výsledky vývoje nebo výzkumu, obchodní záměry atd.), musí být dostatečně ochráněny před zneužitím či odcizením. Pokud tyto informace nebudeme dostatečně chránit, může dojít k jejich úniku a zneužití neoprávněnou osobou.

V současnosti jsou informace v organizacích vystaveny různým bezpečnostním hrozbám. Bezpečnost informací je zaměřena na širokou škálu hrozeb. Útoky hackerů jsou stále častější, roste jejich nebezpečnost a sofistikovanost. Proto je žádoucí, aby organizace měly stanoveny své bezpečnostní požadavky a odpovídající postupy pro řízení bezpečnostních rizik u informací a pro realizaci opatření určených k zamezení jejich výskytu. Data musí být chráněna před neidentifikovanými závažnými hrozbami. V případě informačních systémů musí jít o opatření směřující k zajištění trvalé dostupnosti nabízených služeb, k řízení přístupu k datům na základě přístupových práv a ochraně přenášených dat. [1]

2 VYTĚŽOVÁNÍ POČÍTAČOVÉ SÍTĚ

Obecně platí, že **kybernetické útoky** se zaměřují na **narušení důvěrnosti, integrity nebo dostupnosti**. Narušení důvěrnosti znamená, že se útočník dostane k citlivým datům společnosti (může jít o interní dokumenty nebo citlivé údaje). Při narušení integrity útočník mění uložené údaje, např. uživatelská oprávnění, zůstatek na účtu, citlivé údaje nebo dokáže smazat soubory. Při narušení dostupnosti je informační systém po určitou dobu mimo provoz nebo neodpovídá na dotazy. [2]

Kybernetické útoky mohou přijít jak z externího prostředí sítě, pomocí hackerů, tak z interní sítě pomocí agentů, lidských chyb nebo podvodných komponentů. Hackeři se také mohou dostat do podnikových systémů tím, že se k nim úspěšně připojí a maskují se jako oprávněný uživatel s určitými právy. V některých případech hackeři postupují dále a maskují se za administrátora sítě. Jako administrátor může hacker libovolně měnit téměř celý systém. Jakmile hacker získá dostatečné oprávnění, může ovládat celý systém. [2]

Internet lze označit za „**prostředí bez zábran**" neboli „**disinhibované prostředí**". Uživatel totiž na Internetu ztrácí zábrany. Má pocit, že je anonymní a ztratí se v davu. A tato skutečnost právě nahrává hackerům na celém světě. První a pravděpodobně nejvíce podceňovaným dostupným nástrojem pro získávání informací je právě **sociální inženýrství**. Jedná se o způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace (na rozdíl od pojetí sociálního inženýrství z hlediska společenské vědy). Termín je běžně používán ve významu podvodu nebo podvodného jednání za účelem získání utajených informací organizace nebo přístup do informačního systému firmy. Jedná se o metodu, kdy se útočník zaměří na svou oběť s cílem získat důvěrné a cenné informace. Získané informace následně zneužije ve svůj prospěch. Ve většině případů útočník nepřichází vůbec do osobního kontaktu s obětí. [3]

Průnik do počítačových systémů není jen čistě technickou záležitostí. **Sociotechnika** hraje v úloze pomocníka pro překonávání bezpečnostní bariéry velkou a významnou roli. Sociální inženýrství je v drtivé většině případů ten nejlevnější a pro znalého člověka i nejjednodušší způsob, jak narušit bezpečnost jinak velmi robustních systémů. Obecně se o sociálním inženýrství dá říci, že útoky mají velmi vysoké procento úspěšnosti a jsou velice zákeřné. Při dobrém skrývání útočníka ho není skoro možné ani vystopovat. Následky těchto útoků mohou být velké, pro firmy někdy i likvidační. [3]

Sociální inženýrství pro svoji sílu lze nazvat smrtící zbraní hackerů. Hacker útočí na nejslabší článek zabezpečení jakéhokoliv systému – na člověka. Útočník tak může pomocí specifické přípravy a psychologické manipulace ovlivnit určitá rozhodnutí člověka k provedení konkrétní činnosti. Sociální inženýrství je velice jednoduchý a efektivní způsob, jak obejít bezpečnostní prvky. Nebezpečí sociálního inženýrství je především v jeho jednoduchosti a nenápadnosti. Proto je sociální inženýrství považováno za nejlepší hackerský způsob pronikání do informačních systémů. Není potřeba se trápit s prolamováním hesel, když je jednodušší někoho donutit, aby heslo sdělil. Navíc při dobře vedeném útoku si oběť v drtivé většině vůbec neuvědomí, že něco útočníkovi vyzradila. Někdy nejjednodušší metody bývají nejspolehlivější. [3]

Sociální sítě jsou velmi lákavým cílem jak pro klasické hackery, tak právě pro sociální inženýrství. Databáze sociálních sítí obsahují nepředstavitelné množství dat a informací (také osobních údajů), které jsou lukrativním zbožím. Sociální sítě jsou však vesměs unikátní systémy, ve kterých neplatí nic univerzálně. Vzhledem k tendenci sociálních sítí otevírat se vyhledávačům musí každý uživatel přemýšlet, které informace o sobě poskytne. Informace zveřejněná na Internetu má zpravidla tendenci

na něm již zůstat a tento trend určitě bude nabývat na významu. Ve vztahu k sociálním sítím panuje mezi uživateli velká důvěra a zároveň jejich uživatelé často nepovažují za nutné hlídat si na nich své soukromí. Některé sociální sítě již dopředu v podmínkách užívání oznamují, že nenesou za vložená data a jejich zcizení žádnou odpovědnost. Tím se kryjí před případným soudním sporem ohledně zcizení dat.

Organizace si může pořídit ty nejlepší a nejdražší bezpečnostní technologie, vyškolit personál tak, aby byla každá důvěrná informace před odchodem domů pod zámkem, najmout si tu nejlepší firmu na noční ostrahu objektů, a přece bude tato organizace stále zranitelná. Soukromé osoby se mohou držet všech nejlepších zásad doporučovaných odborníky, mohou nainstalovat všechny nejnovější produkty vylepšující zabezpečení a odpovídajícím způsobem pozorně zkonfigurovat systém, mohou použít všechna jeho vylepšení či opravy, a přece jsou tyto osoby stále nechráněné. Sociotechnika se tímto nedá zastavit. Sociotechnika je způsob, jak získat různými metodami od lidí potřebné informace. Tato metoda existovala dávno předtím, než se na světě objevily první počítače. [3]

V sociotechnice je nejjednodušší a nejpoužívanější formou komunikace telefonní hovor nebo e-mail, protože se osoby nevidí, a tím pádem je v něm menší riziko odhalení. Naopak osobní kontakt je nejsložitější a nejméně používaný. V těchto konverzacích mají převážně výhodu ženy s klidným hlasem komunikující s mužem. [3]

Hackeři, kteří chtějí fungovat na cílových zařízeních v delším časovém úseku, nebo po určitou dobu, často umístí vir do systému pro pozdější využití. Což lze nazvat implantáty, obvykle jsou spící, dokud nejsou aktivovány činnostmi na cílovém zařízení (např. vzhled nové informace, o kterou by mohl mít hacker zájem), nebo příkazy od hackera. Implantáty mohou fungovat i samostatně. Hledají zařízení v síti, které nemají tyto implantáty a ujistí se, že dlouho bez nich nezůstanou.

Nejčastějším důvodem hackování je zpronevěřit data. Když hacker ukradne někomu data, nazýváme to **vytěžování počítačové sítě** (Computer Network Exploitation - CNE). Bez ohledu na to, jakým způsobem chce hacker odcizit data, narušit nebo poškodit systém, musí provést první a nejtěžší krok. Tím je dostat se do systému (získat oprávnění v daném systému). Z toho důvody vypadají první fáze CNE stejně jako počáteční fáze kybernetické útoku. Z toho plyne, že ti, kteří mají nejvíce zkušeností se získáním přístupů do systému, mohou být nejlépe kvalifikovanými osobami k útoku na počítačové sítě. [4]

Insider je jednoduše řečeno zasvěcená osoba (může jí být i bývalý zaměstnanec) nebo je to interní zaměstnanec s přístupem k informacím souvisejícím s jeho funkčním zařazením a pracovním postavením. Jedná se o člověka uvnitř organizace, který má možnost proniknout do informačních systémů organizace nebo má možnost získat informace, popřípadě nastražit léčku k získání těchto informací. Působení těchto insiderů často nadělá větší škody, než sofistikované počítačové útoky. Nejslabším článkem v oblasti kybernetické bezpečnosti jsou lidé. **Řadový zaměstnanec může způsobit bezpečnostní incident s dalekosáhlými následky.** Manažer rozhoduje, jaká bezpečnostní opatření budou aplikována. [4]

3 NEJSLABŠÍ PRVEK SYSTÉMU

Z důvodu úzkého prolínání kybernetického a reálného prostředí se jedinec stává zranitelnějším vůči kybernetickým hrozbám. Zohledníme-li rychlý vývoj kybernetických útoků a vynalézavost jejich tvůrců, není v lidských silách poskytnout podrobný výčet všech kybernetických hrozeb. Kyberzločinci se snaží neustále hledat nové cesty, jak se dostat firmám a jejich zaměstnancům do počítačů a mobilů.

V současnosti používané technologie pomáhají organizacím ochránit jejich důležitá data a firemní sítě. Musí se ale dobře používat. K tomu je potřeba mít **vzdělané a proškolené zaměstnance (profesionály v oblasti informačních technologií)**, kteří se o správné nastavení sítí a bezpečnosti starají.

Útoky proti informačním technologiím jsou stále sofistikovanější a komplexnější. Útočníci (ve většině případů se jedná o organizované skupiny) jsou však vynalézaví a často se soustředí na nejsnadnější cíl, který jim umožní se k cenným datům dostat s minimální námahou. Tím snadným cílem byl, je a vždy bude **koncový uživatel. Nejzranitelnějším prvkem celého systému jsou proto uživatelé.** Z jejich neopatrnosti pak mohou vyplynout různě vážné problémy rozdílných charakterů. Možností a metod útoků je mnoho a těch právě útočníci využívají.

4 ŠKOLENÍ ZAMĚSTNANCŮ

Jednou z možností, jak zabránit útočníkům průniku do vlastních sítí nebo zneužití vlastních firemních dat, je neustálé vzdělávání vlastních zaměstnanců. Bez neustálého vzdělávání zaměstnanců se v současné době nelze obejít.

Tato vzdělávání lze rozdělit do tří kategorií podle úrovně působení ve firmě. A to vzdělávání pro management firmy, IT specialisty (profesionály) a běžné uživatele. Profesionály je nejlepší vzdělávat/školit u odborných školících společností, které tato školení provádí. Mohou se také samo-vzdělávat, ale to není tak efektivní a není vhodné pro každého. Tento typ školení profesionálů je sice nejdražší, ale firmám se vždy vyplatí do nich finanční prostředky investovat. Vrátí se jim to v udržení bezpečnosti firmy.

Vzdělávání zaměstnanců v rolích manažerů a běžných uživatelů je sice finančně pro firmy méně náročnější, ale o to časově náročnější. Nejlepším řešením v současné době, která je poznamenaná pandemickou situací, nejlépe vychází provádění školení pomocí e-learningových kurzů. Tyto kurzy si lze u specializovaných firem objednat na míru (větší finanční zátěž) nebo si je vytvořit sami vlastními silami (větší časová zátěž). Výhodou e-learningových kurzů je to, že je lze absolvovat kdekoli a kdykoli s přístupem na firemní síť. Výuku a tempo si může každý zaměstnanec přizpůsobit svému tempu studia. Problematice se můžete věnovat podle svých individuálních potřeb. Nad některými částmi kurzu můžete strávit více času, nad jinými méně. Není problém se k některým částem kurzu průběžně vracet a opakovat si nepochopenou problematiku. Tyto kurzy může zaměstnanec absolvovat kdykoli v pracovní době či doma po pracovní době. Lze vidět výsledky průběžných testů a lze kurz podle stanovených pravidel opakovat.

Jako vzorový příklad těchto kurzů doporučuji navštívit vzdělávací portál NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost) a také absolvovat některé z nabízených kurzů pro různé kategorie osob (od dětí na základních školách, přes běžného uživatele až po manažery na kybernetickou bezpečnost). Doporučuji navštívit webovou stránku https://osveta.nukib.cz/local/dashboard/, kde lze uvedené kurzy absolvovat.

LITERATURA

[1] PAVLÍČEK, Antonín, Alexander GALBA a Michal HORA. Moderní informatika. Druhé, rozšířené vydání. Praha: Professional Publishing, 2017. ISBN 978-80-906594-6-9

[2] ČERMÁK, Miroslav. *CIA: Důvěrnost-Integrita-Dostupnost* [online]. [cit. 2022-02-20]. Dostupné z: https://www.cleverandsmart.cz/duvernost-integrita-dostupnost/

[3] MITNICK, Kevin D. a William L. SIMON. Umění klamu. Gliwice: Helion, 2003. ISBN 83-7361-210-6

[4] Richard A. CLARKE, Robert K. KNAKE. *Cyber War - The Next Threat to National Security and What to Do about It.* USA: Ecco Press, 2010, 290 s. ISBN 9780061962233

MONITOROVANIE A TRASOVANIA POHYBU OSÔB V ZDRAVOTNÍCKYCH ZARIADENIACH V ČASE PANDÉMIE COVID-19

Mária Lusková[8], Ladislav Mariš[2]

ABSTRAKT

V súčasnosti, v čase pandémie COVID-19 sa dôraz kladie na dôležitosť prevencie a dodržiavania nastavených opatrení. Významným proaktívnym opatrením je monitorovanie, znižovanie mobility a stretávania sa ľudí v zdravotníckych zariadeniach. Článok sa zaoberá problematikou monitorovania a trasovania pohybu a kontaktu osôb v zdravotníckych zariadeniach počas pandémie COVID -19. Cieľom článku je predstaviť zameranie, ciele a vecnú náplň projektu aplikovaného výskumu a vývoja *Monitorovanie a trasovanie pohybu a kontaktu osôb v zdravotníckych zariadeniach* financovaný Agentúrou na podporu výskumu a vývoja a v súčasnosti riešený na Fakulte bezpečnostného inžinierstva Žilinskej univerzity v Žiline v spolupráci s firmami z praxe.

Kľúčové slová:
Covid-19, pandémia, monitorovanie, trasovanie osôb, zdravotnícke zariadenia.

ABSTRACT

At present, at the time of the COVID-19 pandemic, the emphasis is put on the importance of prevention and compliance with the set measures. An important proactive measure is monitoring and reduction of mobility and meeting of people in health care centers. The paper deals with the issue of monitoring and tracing the movement and contact of persons in health care centers during COVID -19. The aim of the paper is to present the focus, goals and content of the project of applied research and development *Monitoring and tracing of movement and contact of persons in medical facilities f*unded by the Agency for Research and Development and currently

[8] Mária Lusková, Ing., PhD., Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline, Univerzitná 8215/1, 010 26 Žilina, telefón: +421 41 513 6766, e-mail: maria.luskova@uniza.sk

2 Ladislav Mariš, Ing., PhD., Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline, Univerzitná 8215/1, 010 26 Žilina, telefón: +421 41 513 6658, e-mail: ladislav.maris@uniza.sk

solved at the Faculty of Security Engineering of the University of Žilina in cooperation with firms from practice.

Key words:
Video surveillance system, smart city, city camera system, operator

ÚVOD

Zdravotníctvo patrí medzi najdôležitejšie systémy, ktorých nefunkčnosť spôsobuje závažný dopad na zdravie a život obyvateľov. V Slovenskej republike, podobne ako v iných krajinách vo svete, patrí zdravotníctvo medzi sektory kritickej infraštruktúry a jeho význam a dôležitosť potvrdzuje súčasná epidémia Covid-19, ktorá zmenila v dramaticky krátkom čase život i spôsob myslenia takmer celého ľudstva. Ukázala skutočnosť, aká dôležitá je pre celú spoločnosť zdravotná starostlivosť a paradoxne poukázala na výdavky súvisiace so zdravotníctvom ako na investíciu do prosperity a konkurencieschopnosti krajiny v globálnom svete a nielen ako na nutný nákladový faktor.

Z hľadiska riešenia súčasnej situácie, ako aj prípravy na ďalšie pandémie, vystupuje do popredia otázka ďalších investícií, resp. hľadania možností efektívneho vysporiadania sa s takýmito negatívnymi situáciami. Nápor pacientov infikovaných vírusom posunul systémy zdravotnej starostlivosti mnohých krajín na pokraj kolapsu.

Prioritou zostáva zlepšenie existujúcich systémov zdravotnej starostlivosti, ktoré majú potenciál zvýšiť celkovú efektívnosť zdravotného systému a zabezpečiť lekárom a zdravotníckemu personálu (sanitárom, zdravotníckym asistentom, zubným lekárom, laborantom, technikom, fyzioterapeutom a ostatným zdravotníckym pracovníkom) vhodné pracovné prostredie a technológie podporujúce napĺňanie ich poslania.

Poskytovanie zdravotnej starostlivosti a ochrana verejného zdravia sú základné funkcie štátu. Zásadná úloha zdravotníctva je a vždy zostane poskytovanie zdravotnej starostlivosti obyvateľom postihnutých krízovou situáciou, ktorú práve v súčasnosti prežívame. Poskytovanie zdravotnej starostlivosti a služieb súvisiacich s poskytovaním zdravotnej starostlivosti vymedzuje Zákon č. 576/2004 Z. z. Zákon o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov. Tieto zahŕňajú zariadenia ambulantnej zdravotnej starostlivosti, zariadenia ústavnej zdravotnej starostlivosti a zariadenia lekárenskej starostlivosti (§ 7, 576/2004) [1].

Cieľom článku je predstaviť zameranie, ciele a vecnú náplň projektu aplikovaného výskumu a vývoja *Monitorovanie a trasovanie pohybu a kontaktu osôb v zdravotníckych zariadeniach* financovaný Agentúrou na podporu výskumu a vývoja a v súčasnosti riešený na Fakulte bezpečnostného inžinierstva Žilinskej univerzity v Žiline v spolupráci s firmami z praxe.

1 MONITOROVANIE POHYBU OSÔB A SLEDOVANIE KONTAKTOV

V súčasnom období pandémie COVID-19 pohyb osôb v mnohých zariadeniach poskytujúcich zdravotnú starostlivosť nie je obmedzený a ani nie je možné ho vylúčiť, prípadne obmedziť. Ako príklad je možné uviesť nemocnice nadregionálneho významu, ktoré poskytujú ambulantnú a ústavno-preventívnu starostlivosť. Dennodenne navštívi takéto zariadenie množstvo ľudí s cieľom získať potrebnú zdravotnú starostlivosť, pričom nie je možné vylúčiť prípadnú infekčnosť niektorých osôb pohybujúcich sa v priestoroch daného zariadenia.

Monitorovanie pohybu osôb pohybujúcich sa v rámci areálu zdravotníckeho zariadenia sa môže stať významnou pomôckou pri vyhľadávaní kontaktov potvrdených prípadov.

Sledovanie kontaktov je jedným z hlavných nefarmaceutických opatrení pre zabránenie šírenia infekcie [2]. Existujú viaceré štúdie popisujúce proces sledovania kontaktov [3]. V [4] autori považujú sledovanie kontaktov, po ktorom nasleduje liečba alebo izolácia, za kľúčové kontrolné opatrenie v boji proti infekčným chorobám. Ide o formu lokálne cielenej kontroly, ktorá má potenciál byť vysoko účinná pri riešení nízkeho počtu prípadov. V [5] je sledovanie kontaktov opísaný ako viacstupňový proces zahŕňajúci diagnostiku infikovaného človeka, spracovanie všetkých pravdepodobných kontaktov tohto človeka, identifikácia následne infikovaných a opakovanie celého procesu. V [6] autori uvádzajú, že aktuálne nasadené mobilné aplikácie na sledovanie kontaktov zlyhali ako efektívne riešenie v súvislosti s pandémiou COVID-19. Nakoľko sa nepodarilo prilákať počet aktívnych používateľov potrebných na dosiahnutie efektívnej prevádzky, výskumná komunita stojí pred výzvou nájsť nové spôsoby, ktoré povedú k účinným riešeniam na sledovanie kontaktov. Autori taktiež ponúkajú svoje vlastné riešenie na sledovanie kontaktov, ktoré využíva dostupné geolokačné informácie.

Problematikou vyhľadávania kontaktov s využitím mobilných aplikácií a právnymi aspektmi súvisiacich s ochranou osobných údajov sa zaoberajú nasledovné dokumenty vydané v rámci EÚ:

- eHealth Network. Mobile applications to support contact tracing in the EU's fight against COVID-19, Common EU Toolbox for Member States Version 1.0, 15.04.2020 [7].
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [8].
- Commission Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymized mobility data [9].
- Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01) [10].

- COM (2020) 318 final - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Short-term EU Health Preparedness for COVID-19 Outbreaks [11].

2 CIELE A METODIKA RIEŠENIA PROJEKTU

Projekt reflektuje potrebu vyhľadávania kontaktov v prípade pandémie, ale aj iných bezpečnostných hrozieb. V súčasnosti sa neustále zvyšujú nároky na bezpečnosť a ochranu zdravia pri práci a kontrolu vstupu osôb do priestorov firiem či verejne prístupných zariadení, rôznych štátnych inštitúcií, školských zariadení a ďalších súkromných či štátnych objektov. Náročnejšou činnosťou ako je kontrola osôb na vstupe je monitoring a trasovanie pohybu v rámci objektu a jeho jednotlivých priestorov. Napríklad v zdravotníckych zariadeniach by mali návštevníci dodržiavať prísne hygienické opatrenia a mali by navštíviť len ambulanciu či priestory, ktoré sú nevyhnutné a nemali by mať prístup do iných oddelení.

Monitorovanie a trasovanie osôb (pohyb a kontakty s inými osobami) vo verejne prístupných priestoroch, ako napríklad:

- nemocnice a zdravotnícke zariadenia,
- objekty verejnej správy (napr. sociálne poisťovne, daňové úrady, mestské úrady, úrady samosprávnych krajov),
- železničné/autobusové/letiskové terminály, resp. v priestoroch, kde je predpokladaný pohyb veľkého počtu ľudí,

je z hľadiska právneho, ekonomického, technického a bezpečnostného nepreskúmaná oblasť. Preto je dôležité tento problém riešiť ako výskumný problém s využitím najnovších postupov a technológií, pretože nasadzovanie monitorovacích a sledovacích systémov vo verejne prístupných priestoroch, resp. priestoroch, kde je predpokladaný pohyb veľkého počtu ľudí, môže mať zásadný vplyv v boji proti šíreniu pandémie COVID-19 alebo iných vírusových a bakteriálnych ochorení.

Jedným z možných riešení je využiť technológie 21. storočia, ktoré uľahčia a hlavne urýchlia vyhľadávanie možných kontaktov. Napríklad v ázijských krajinách sa na tento účel vytvorili aplikácie do mobilných telefónov, cez ktoré následne vyhľadávali možné kontakty (napr. STAYAWAY COVID). Podobné aplikácie sa objavili aj na Slovensku - napr. ZostanZdravy. Ich nevýhodou je potrebná inštalácia softvérovej aplikácie do mobilného telefónu, a to na dobrovoľnej báze, čo znižuje ich účinnosť. To môže byť hlavne problém v prípade seniorov, ktorí nemajú "smartphone", ale majú zväčša seniorské mobilné telefóny bez možnosti inštalovania spomínaných aplikácií.

Hlavným cieľom projektu je analyzovať právne možnosti, ekonomické, zdravotnícke a bezpečnostné dopady monitorovania osôb a kontaktov v zdravotníckych zariadeniach a následne vytvoriť a aplikovať systém na monitorovanie a trasovanie osôb a ich kontaktov v zdravotníckych zariadeniach, s následným možným využitím vo verejne prístupných priestoroch, resp. priestoroch, kde je

predpokladaný pohyb veľkého počtu ľudí. Dosiahnutie hlavného cieľa projektu je rozdelené do čiastkových cieľov znázornených na obrázku 1.

Podstatou riešenia navrhovaného projektu je posúdenie možnosti monitorovania osôb z hľadiska právneho, ekonomického, bezpečnostného a ostatných relevantných hľadísk s cieľom navrhnúť hardvérové a softvérové riešenie, ktoré bude možné implementovať na vybrané zdravotnícke zariadenie (napr. nemocnica).

Na základe posúdenia budú analyzované technické možnosti aplikácie, pričom sa bude vychádzať najmä z technológie RFID, a zároveň bude vytvorený model ako tento systém môže fungovať presne a optimálne v teoretickej rovine. Získané dáta budú slúžiť na vytvorenie softvérového riešenia systému monitorovania osôb a ich kontaktov.

Ďalším krokom bude navrhované technické riešenie a softvérové riešenie otestovať v laboratórnych podmienkach a následne po odladení implementovať v reálnom zdravotníckom zariadení. Tomu bude taktiež predchádzať podrobná analýza požiadaviek na takýto bezpečnostný systém. Súčasťou toho bude aj návrh grafického rozhrania pre jednoduchšie testovanie s nástrojmi pre notifikáciu, zber nových dát, nastavenie klasifikačných kritérií a pod.

Cieľ 1: Zber dát a analýza prostredia

- Špecifikácia a analýza prostredia zdravotníckych zariadení
- Analýza právneho prostredie
- Analýza ekonomického prostredia
- Analýza bezpečnostného prostredia

Cieľ 2: Návrh modelu systému monitorovania osôb a ich kontaktov

- Analýza funkčných a technických požiadaviek na systém
- Hodnotenie technických limitácií a presnosti technológií dostupných technických zariadení (záznam a čítanie) použiteľných v systéme monitorovania osôb
- Návrh všeobecného modelu (kombinujúci hardvér a softvér) pre realizáciu systému monitorovania osôb a kontaktov so zameraním na použitie v zdravotníckom zariadení
- Návrh spôsob určenia optimálneho rozmiestnenia technických zariadení

Cieľ 3: Návrh softvérového riešenia systému

- Analýza požiadaviek na softvérové riešenie systému
- Návrh architektúry a implementácia softvérového riešenia
- Návrh rozhrania pre testovacie účely
- Testovanie a odladenie softvérového riešenia
- Technická dokumentácia

Cieľ 4: Testovanie v laboratórnych podmienkach

- Testovací polygón v laboratórnych podmienkach
- Testovanie softvérového a technického riešenia v laboratórnych podmienkach

Cieľ 5: Testovanie v reálnych podmienkach zdravotníckeho zariadenia

- Technické riešenie pre vybrané zdravotnícke zariadenie
- Testovanie a odladenie softvérového a technického riešenia v reálnom prostredí vybraného zdravotníckeho zariadenia

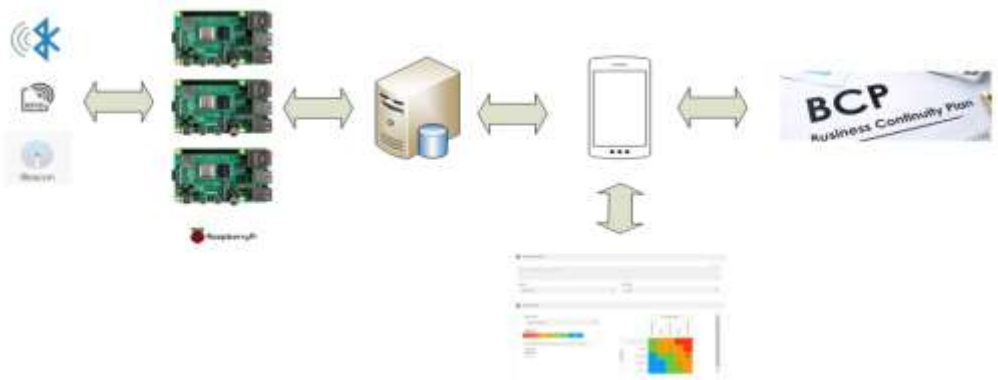
Obrázok 1 Čiastkové ciele pre dosiahnutie hlavného cieľa projektu

Nakoľko bude vývoj a odlaďovanie tohto systému bežať paralelne s etapami pre testovanie v laboratórnych a reálnych podmienkach, bude možné postupne odstrániť chyby a zapracovať všetky potrebné návrhy. Pre testovanie v laboratórnych podmienkach bude vytvorená simuláciu monitorovania osôb v priestoroch Žilinskej univerzity. To umožní vytváranie modelových situácií a real-time testovanie softvérového riešenia už počas vývoja SW. Pre testovanie v reálnych podmienkach bude potrebné vytvoriť modul pre real-time spracovanie dát pre konkrétny monitorovací systém (v konkrétnom zdravotníckom zariadení). Po správnej implementácii bude riešenie v danom prostredí otestované.

3 PRÍNOSY PROJEKTU

Opatrenia zamerané na obmedzenie pohybu a zákazu vychádzania znižujú počet infikovaných ľudí a prinášajú zlepšenie epidemiologickej situácie, avšak sú značne nákladné a nebezpečné pre ekonomiku. Dlhé obmedzenia môžu v niektorých krajinách spôsobiť ešte väčšie problémy ako samotný vírus. Možným nástrojom pre trasovanie kontaktov v zdravotníckych zariadeniach, ktoré majú nezastupiteľnú úlohu a hlavne počas krízových situácií je nevyhnutné zachovať ich kapacitu a akcieschopnosť, je projektom navrhovaný systém na monitorovanie osôb a ich kontaktov s inými osobami v zdravotníckych zariadeniach, s aplikačným použitím vo verejne prístupných objektoch, ale aj v chránených objektoch kritickej infraštruktúry.

Prínosom projektu je realizácia testovania a výber vhodných tagov na monitoring pohybu osôb a to realizáciou praktických testov s dôrazom na vhodné umiestnenie a rozloženie čítacích zariadení vo vybranom referenčnom objekte. Dôraz musí byť kladený na schopnosť bezproblémovej komunikácie v interiéri a exteriéri s možnosťou mechanického úmyselného aj neúmyselného opotrebenia. Prínosom projektu bude taktiež vytvorenie softvéru – informačného systému, ktorý bude obsahovať grafické zobrazenie polohy osôb pohybujúcich sa v referenčnom objekte/areáli, čo prispeje k jednoduchšiemu vyhľadávanie kontaktov a lepšej pripravenosti na zásah, či evakuáciu v prípade potreby. Systém bude patriť medzi inteligentné riešenia, ktoré sú kľúčom k technickému pokroku a napredovaniu. Bloková schéma informačného systému Cov-ID určeného na trasovanie osôb a vyhodnotenia rizikovosti možného kontaktu je znázornená na obrázku 2.



Obrázok 2 Bloková schéma informačného systému Cov-ID určeného na trasovanie osôb a vyhodnotenia rizikovosti možného kontaktu

ZÁVER

Zber dát a návrhu systému bude uskutočňovaný v spolupráci so spoločnosťou DIS, s. r.o., ktorá je v rámci SR jedným z lídrov v oblasti bezpečnostných systémov. Týmto spôsobom sa zabezpečí aplikovateľnosť navrhovaného riešenia v praxi. Výstupy projektu budú mať z ekonomického pohľadu aj merateľné prínosy, pretože v dôsledku navrhovaných opatrení vzniknú spoločenské úžitky súvisiace s

monitorovaním pohybu osôb a s procesom vyhľadávania kontaktov. Tieto úžitky je možné špecifikovať ako zníženie nákladov súvisiacich s vyhľadávaním kontaktov, zvýšenie celkovej presnosti vyhľadávania kontaktov vo vybranom objekte, napr. v zdravotníckom zariadení, zníženie nákladov na realizáciu systémov ochrany štátnych a súkromných objektov, zvýšenie účinnosti navrhovaných systémov ochrany objektov, zníženie nákladov pri procese posudzovania rizík, t. j. pri vypracovaní bezpečnostných správ, havarijných plánov a ostatnej bezpečnostnej dokumentácie, zvýšenie pripravenosti štátu či inštitúcií predchádzať a riešiť závažné krízovým situácie.

Poďakovanie

Tento článok bol pripravený v rámci podpory projektu APPV-20-0457 Monitorovanie a trasovanie pohybu a kontaktu osôb v zdravotníckych zariadeniach.

LITERATÚRA

[1] Zákon č. 576/2004 Zákon o zdravotnej starostlivosti. Dostupný online: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/576/20160102.
[2] Filonets, T.; Solovchuk, M.; Gao, W.; Sheu, T.W.-H. Investigation of the Efficiency of Mask Wearing, Contact Tracing, and Case Isolation during the COVID-19 Outbreak. J. Clin. Med. 2021, 10, 2761. Dostupné online: https://doi.org/10.3390/jcm10132761
[3] Alarabi, L.; Basalamah, S.; Hendawi, A.; Abdalla, M. TraceAll: A Real-Time Processing for Contact Tracing Using Indoor Trajectories. Information 2021, 12, 202. Dostupné online: https://doi.org/10.3390/info12050202.
[4] K. T. D. Eames, M. J. Keeling, Contact tracing and disease control. Proc. Biol. Sci. 270, 2565–2571 (2003). Dostupné online: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1691540/.
[5] Eames, K.T.D. Contact tracing strategies in heterogeneous populations. Epidemiol. Infect. 2007, 135, 443–454. Dostupné online: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2870583/
[6] González-Cabañas, J.; Cuevas, Á.; Cuevas, R.; Maier, M. Digital Contact Tracing: Large-Scale Geolocation Data as an Alternative to Bluetooth-Based Apps Failure. Electronics 2021, 10, 1093. Dostupné online: https://doi.org/10.3390/electronics10091093.
[7] eHealth Network. Mobile applications to support contact tracing in the EU's fight against COVID-19, Common EU Toolbox for Member States Version 1.0, 15.04.2020, Dostupné online: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.
[8] EP and the Council. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data

Protection Regulation) Dostupné online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=SK.

[9] European Commission. COMMISSION RECOMMENDATION of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymized mobility data. Dostupné online: https://ec.europa.eu/info/sites/default/files/recommendation_on_apps_for_contact_tracing_4.pdf.

[10] European Commission. Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01). Dostupné online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN.

[1] European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Short-term EU health preparedness for COVID-19 outbreaks. COM (2020) 318 final. Brussels, 15.7.2020. Dostupné online: https://ec.europa.eu/info/sites/default/files/communication_-_short-term_eu_health_preparedness.pdf.

MOŽNOSTI MODELOVANIA TRASOVANIA POHYBU OSÔB V OBJEKTOCH

Ladislav Mariš[9], Mária Lusková[10]

ABSTRAKT
V príspevku rozoberáme vybrané možnosti ako modelovať trasovanie pohybu osôb pomocou vybraných technických riešení a vybranej metódy simulácie. Definujeme technické a technologické riešenia trasovania osôb a tiež sa bližšie venujeme vybranej metóde simulácii pohybu AntComputing v prostredí programu NetLogo. Pomocou modelovania trasovania pohybu osôb, môžeme získať teoretické poznatky, ktoré nám pomôžu vytvoriť a inštalovať systém monitorovania pohybu osôb v reálnom prostredí s menším počtom chýb a s efektívnejším rozmiestnením technických prvkov. Aplikácia riešenia je nastavená na zdravotnícke zariadenia v dôsledku trasovania kontaktov v boji proti pandémii ochorenia COVID-19.

Kľúčové slová:
trasovanie pohybu osôb, technológie, simulácia, COVID-19

ABSTRACT
In this paper, we discuss selected options for modelling the tracking of people using selected technical solutions and selected simulation methods. We define technical and technological solutions for tracing people, and we also pay more attention to a selected method of motion simulation, the so-called Ant Computing in the NetLogo environment. By modelling the tracking of people's movements, we can gain theoretical knowledge that will help us create and install a system for monitoring the movement of people in a real environment with fewer errors and with a more efficient deployment of technical elements. The application of the solution is set up for medical facilities as a result of contact tracing in the fight against the COVID-19 pandemic.

Key words:
tracking the movement of people, technology, simulation, COVID-19

[9] Ladislav Mariš, Ing., PhD., Žilinská univerzita v Žiline, Univerzitná 8215/1, Žilina, ladislav.maris@uniza.sk
[10] Mária Lusková, Ing., PhD., Žilinská univerzita v Žiline, Univerzitná 8215/1, Žilina, maria.luskova@uniza.sk

ÚVOD

Trasovanie pohybu osôb je za určitých právnych a technických podmienok významným prvkom v oblasti bezpečnosti. Otázka trasovania pohybu osôb je na mieste, ak berieme do úvahy priestory, v ktorých sa vyžaduje dohľad na pohybom osôb, dohľad nad neoprávneným pohybom v chránenom objekte, dohľad nad pohybom osôb z hľadiska šírenia nákazlivej choroby a ďalšie možné scenáre použitia. Napríklad, v čase pandémie COVID-19 je na mieste otázka monitorovania počtu osôb, ich pohybu (napr. v zdravotníckom zariadení), ich priblíženie k inej osobe na menej ako 1,5 m od druhej osoby (resp. 2 m) či ich nadlimitné zhromažďovanie v určitom priestore (maximálna kapacita na plochu priestoru). Technické riešenia na trhu už existujú, resp. sú v rôznych fázach nasadenia, výskumu či vývoja.

Pre akademické, ale aj praktické riešenie nás zaujíma otázka modelovania trasovania pohybu osôb v objektoch. Dôvodom našej snahy je modelovanie a simulácia možných scenárov pohybu osôb. Takýto model resp. simulácia, môže byť nielen zaujímavá, ale aj prínosná pre lepšie pochopenie v reálnom prostredí (napr. v zdravotníckom zariadení). Pomocou modelovania trasovania pohybu osôb, môžeme získať teoretické poznatky, ktoré nám pomôžu vytvoriť a inštalovať systém monitorovania pohybu osôb v reálnom prostredí s menším počtom chýb alebo s efektívnejším rozmiestnením technických prvkov.

1 EXISTUJÚCE TECHNOLOGICKÉ RIEŠENIA TRASOVANIA POHYBU OSÔB

Pokladáme za významné charakterizovať vybrané technologické riešenia, pomocou ktorých je možné trasovať pohyb osoby, resp. viacerých osôb. Neznamená to však, že neexistujú ďalšie technologické možnosti.

GPS - Global Positioning System

Medzi základné technické riešenie trasovania pohybu osôb (objektov) zaraďujeme technológiu GPS, ktorú poznáme pod názvom satelitná navigácia [1]. Určovanie polohy pomocou súradníc GPS je dnes bežnou praxou. GPS lokátor, resp. GPS modul ako súčasť mobilného zariadenia je dnes bežnou súčasťou sledovania polohy osoby, automobilu, tovaru a pod. Problém nastáva v prípade trasovania pohybu bez pokrytia GPS, resp. v priestoroch, ktoré zabraňujú prestup GPS signálu, napríklad vo vnútri budov, v tuneloch či v komplikovanom teréne. Technológia GPS v súčinnosti s aplikáciami GIS (geografický informačný systém) poskytuje geolokačné údaje na mapovom podklade. Podľa [2], aplikácie GIS môžu účinne pomáhať pri mapovaní verejných akcií, ktoré porušujú protipandemické nariadenia ako je napríklad zákaz združovania osôb či iné dynamické mapovanie šírenia ochorenia COVID-19.

RFID - Radio Frequency IDentification

Vysokofrekvenčná identifikácia alebo RFID (z angl. Radio Frequency IDentification) je identifikačný prvok na identifikáciu (nielen) tovaru, pracujúci vo vysokofrekvenčnom pásme [3] . Pre potreby trasovania osôb je riešením inštalácia RFID brán, ktoré sú vybavené čítačkou a anténami RFID, spolu s RFID snímacími

bodmi (čítačky) umiestnené v priestore. Princípom je snímanie RFID tagu s jedinečným identifikačným údajom. Hlavnou požiadavkou je nositeľný tag napr. na oblečení osoby či nálepky na zápästí a pod. Podľa [4] je možné snímať osoby (objekty) pomocou RFID detekcie na tzv. mobilnom robotovi, ktorý sa umiestňuje do priestoru a sníma v 360° okolo seba.

Kamerový dohľadový systém

Kamerové systémy alebo kamerové dohľadové systémy alebo aj obrazové sledovacie systémy (Video Surveillance Systems) [5] sú základným nástrojom na monitorovanie priestorov. Najväčšia výhoda použitia kamerového dohľadového systému je reálne viditeľný obraz sledovaných objektov a následná analýza tejto scény. Analytika na kamere alebo na nahrávacom zariadení, resp. počítači je v prípade trasovania osôb náročná z pohľadu pokrytia sledovaného priestoru.

Ak dokážeme pokryť monitorovaný priestor tak, aby detekčné charakteristiky kamier pokryli monitorovaný priestor, tak dokážeme veľmi efektívne sledovať nielen trasovanie osoby, ale aj vyhodnotiť jej správanie napríklad dodržanie ďalších bezpečnostných opatrení. Na druhej strane je takmer nemožné pokryť veľký, zložitý a členitý priestor, v ktorom trasovanie pohybu osôb by bolo už ekonomicky nevýhodné. Preto aj použitie kamerového dohľadového systému z dôvodu trasovania osôb má svoje limity.

Zároveň je potrebné uviesť, že biometrické údaje sa považujú za osobné údaje v zmysle článku 4 bodu 14 nariadenia GDRP (Zákon o ochrane osobných údajov) a ktoré umožňujú a potvrdzujú jedinečnú identifikáciu fyzickej osoby, napríklad vyobrazením tváre.

Zároveň kamerový systém zachytáva viacero informácií vrátane špecifických znakov (napr. kývajúca chôdza, tetovanie a pod.), a tým pádom vieme identifikovať konkrétnu fyzickú osobu. [6] Z technického hľadiska sa môže jednať len o 1 zariadenia – kameru. Spracovanie dát môže byť priamo na kamere alebo sa posielajú získané dáta na server (počítač, úložisko), na ktorom sa dáta spracúvajú, napr. aj pre potrebu trasovania pohybu osôb. Pre sledovanie osôb bez potreby identifikácie by mohli poslúžiť termálne kamery, ktoré zachytávajú infračervené spektrum osoby. [7]

Bluetooth

Bluetooth môžeme charakterizovať ako komunikačný štandard pre bezdrôtovú komunikáciu na prepájajúcu dve a viac elektronických zariadení s bluetooth technológiou (rozdiel oproti RFID), ako napríklad mobilný telefón, tablet, notebook či iné bezdrôtové zariadenia - napríklad nositeľnú elektroniku. Táto technológia sa používa väčšinou na krátke vzdialenosti (zvyčajne do 10 m, teoreticky až do 4000 m teoretickom nastavení antény, výkone prenosu a pod.) medzi oboma zariadeniami. Dosah môže znižovať prítomnosť prekážok (osoby, kov, steny, elektrotechnické zariadenia a pod.). Technológia Bluetooth využíva frekvenčné pásmo 2,4 GHz ISM (2 400 až 2 483,5 MHz), ktoré umožňuje vhodnú rovnováhu medzi dosahom a priepustnosťou. Pásmo 2,4 GHz je navyše dostupné na celom svete, čo z neho robí skutočný štandard pre bezdrôtové pripojenie s nízkou spotrebou energie. [8]

Nespornou výhodou je prítomnosť Bluetooth rozhrania takmer v každom mobilnom telefóne.

iBeacon

iBeacon je názov pre technologický štandard pre bezdrôtovú komunikáciu spoločnosti Apple. Technológia iBeacon bola uvedená ako ucelený systém slúžiaci predovšetkým pre interiérovú navigáciu. Systém je tvorený sieťou nízkoenergetických Bluetooth vysielačov, tzv. beaconov či spotov, ktoré dokážu mobilným zariadeniam odovzdávať identifikačné informácie. Tie môžu ďalej spracovávať aplikácie nainštalované v mobilných zariadeniach a využívať ich pre následné zobrazenie ľubovoľného obsahu. Technológia našla využitie predovšetkým v marketingu, ale aj v rámci turistického ruchu či na úradoch. [9] Technológia iBeacon sa nikdy nerozbehla ako sa predpokladalo a od roku 2021 je takmer nečinná. Ukázalo sa, že je to príliš veľa problémov pre používateľov, ktorí z technológie nemajú žiadnu skutočnú hodnotu. [10] Existujú ďalšie technologické verzie tzv. beaconov, ktoré komunikujú na princípe technológie Bluetooth.

Wi-Fi (IEEE 802)

WiFi je štandardným označením pre bezdrôtovú komunikáciu v počítačových sieťach. Wi-Fi využíva viacero častí protokolov IEEE 802 (napr. Wi-Fi 802.11ax) a je navrhnuté tak, aby bezproblémovo spolupracovalo s káblovou sieťou (ethernet). Kompatibilné zariadenia sa môžu navzájom prepájať cez bezdrôtové prístupové body (access pointy), ako aj ku káblovým zariadeniam a internetu. Prostredníctvom Wi-Fi je možné vzájomné prepojenie zariadenia a prístupového bodu. [11] Rovnako ako predchádzajúce technológie existuje niekoľko obmedzení, ktoré zabraňujú ideálnemu prenosu dát (napr. steny, kov, smerovanie antény a pod.).

Ostatné technológie

Medzi ostatné technológie môžeme zaraďovať infračervené senzory v kombinácií s iným zariadením napr. kamerovým systémom [12], laserové lúče (napr. technológia LIDAR 3D skenovania) [13], NFC (Near Field Communication), ktorá komunikuje do relatívne malej vzdialenosti 10 centimetrov či kombinácia vyššie uvedených technológií, napr. ToF (Time of Flight) – kombinácia kamery a laserového lúča [14].

Z vyššie uvedených technologických riešení sú niektoré viac a niektoré menej vhodné pre sledovanie pohybu osôb. Každá spomenuté technológia má výhody či nevýhody vo vzťahu ku konkrétnej oblasti použitia, technologickej náročnosti alebo jednoduchosti použitia, cene za implementáciu, nárokom na údržbu a obsluhu a ku ďalším kritériám.

2 MODELOVANIE TRASOVANIA POHYBU OSÔB

Existujúce technologické zariadenia, ktoré použijeme na sledovanie trasovania pohybu osôb nám pri ideálnom prípade poskytnú dáta, ktoré potrebujeme ďalej spracovať, analyzovať a premietnuť do použiteľnej podoby, napr. uviesť do mapového podkladu či priradiť iné geolokačné súradnice či názov miesta. Za týmto účelom je potrebné získané údaje prijať a uložiť.

Princíp trasovania osôb pre potreby simulácie

Pre uloženie aktuálnych údajov poslúži jednoduchá databáza (dataset), ktorý musí obsahovať aktuálne informácie o čase a danom mieste osoby. Je potrebné trasovanej osobe priradiť určité identifikačné údaje. Toto je možné realizovať napríklad priradeným týchto údajov na vstupe osoby do objektu (napr. priradeným konkrétneho nositeľného zariadenia so špecifickým ID (či fyzickú MAC adresu nosiča). Následne je potrebné aby sa pri dátach okrem času a miesta nachádzal konkrétny identifikátor. Ak rozdelíme mapový podklad na sieť súradníc, dokážeme konkrétnej súradnici priradiť čas a ID sledovanej osoby, resp. konkrétnej osobe (ID) priradiť súradnicu a čas v tomto momente. Mapový podklad môže reprezentovať rozmiestnená sieť prijímačov objektoch, s ktorým komunikuje napríklad nositeľný tag (či iné riešenie). Potom konkrétnej osobe (ID) priradíme konkrétny snímač (napr. špecifická MAC adresa snímača a umiestnenie v objekte) a samozrejme čas zosnímania [15]. Takýto zjednodušený princíp nám umožní si lepšie predstaviť pomyslený model trasovania pohybu osôb v objektoch.

Simulačná metóda optimalizácie pohybu AntComputing

Existujú procesy, algoritmy či spôsoby správania človeka, ktoré sa podobajú ostatným živočíšnym druhom. Napodobňovaním biologických procesov ostatnej živočíšnej ríše sa nazýva biomimikry. Mohli by sme povedať, že ľudia sa snažia efektívne fungujúce systémy prírody napodobniť a využívať vo svoj prospech. Ako príklad uvádzame vytváranie mravčích cestičiek za potravou. Zistilo sa, že mravce vedia vytvoriť najkratšiu možnú cestičku v prostredí tak, aby efektívne nachádzali potravu a dostali sa späť do svojho mraveniska. Exituje viacero teórií ako mravce medzi sebou komunikujú a akým spôsobom cestičky vytvárajú. Tieto teórie popisujú pohyb mravcov, avšak nemožno tvrdiť, že by existoval model, ktorý by bol dokonale realistický. Na samotný pohyb mravcov sa môžeme pozerať z dvoch hľadísk. Prvé hľadisko je nereflektovanie vonkajších vplyvov – pohybuje sa rovno za svojim cieľom. Druhé hľadisko vychádza z prijímania vonkajších podnetov z okolia a koncentráciou feromónov ostatných mravcov, ktorá by mala mravca viesť k potrave a späť do mraveniska. Spojením obidvoch pohľadov vzniká celkový pohyb mravcov.

Na tomto základe môžeme predpokladať dve základné zložky pohybu mravca, ktoré prebiehajú súčasne:

- Ide o stochastickú zložku v podobe nepresnosti (a šumu), ktorá sprevádza subjektívny priamočiary pohyb mravca. Mravec si vyberá smer v závislosti od smeru, z ktorého prišiel a podľa detekovanej koncentrácie feromónu, ktorá by

ho mala viesť k cieľu (potrava, mravenisko). Tento subjektívny smer je upravený o náhodnú zložku Y, ktorá reprezentuje výchylku oproti subjektívnemu smeru. Táto výchylka Y vzniká v dôsledku nepresnosti a šumu (nepresnosť orientácie, chôdze a pod.). V každom kroku mravca môžeme sledovať nepresnosť teda odchýlku Y od smeru v predchádzajúcom kroku. Pokiaľ by bola táto odchýlka nulová Y=0, potom by pohyb mravca bol priamočiary. Problém je práve poznanie odchýlky Y.

- Druhou zložkou pohybu mravca je deterministická zložka, ktorej hlavným faktorom je chemická feromónová komunikácia medzi mravcami. Množstvo chemickej látky, ktorú môže mravec extrahovať do prostredia je obmedzené. Rôzne druhy feromónov slúžia na odovzdávanie rôznych druhov informácií, avšak okrem informačnej hodnoty. Táto hodnota a líši dobou vyprchania ako aj celkovou zložkou difúzie (vyprchania) chemických látok. To znamená, že keby mravec ostal mimo mravenisko dostatočne dlhú dobu v podstate nevie, kde sa mravenisko nachádza a pokladáme ho za strateného. Mravec sa môže zachrániť pokiaľ objaví chemickú stopu od ostatných mravcov.

Obe zložky pohybu sú prítomné v rovnakom čase u každého mravca naraz. Čím je však silnejšia stopa nasledovaného feromónu, tým sa znižuje podiel stochastickej zložky Y a zvyšuje sa podiel deterministickej zložky na celkovom pohybe mravca. Z tohto vyplýva jasný trend, že pri silnejšej koncentrácií feromónu je cesta medzi potravou a mraveniskom určená jasnejšie, a tak aj tendencia mravca vybočovať z trasy by mala byť nižšia. Algoritmy pohybu mravcov by mali tiež zohľadňovať prostredie, ktoré v značnej miere determinuje vlastnosti chemických látok – feromónov, ktorými mravce disponujú. Spôsob chemickej komunikácie a vlastnosti produkovaných feromónov pravdepodobne závisia od toho, aké veľké vzdialenosti musí kolónia bežne prekonávať. Jedným z riešení, ktoré pomáha pri efektívnosti hľadania vzdialenejších zdrojov potravy od mraveniska je zvýšenie počtu mravcov, ktoré priestor prehľadávajú. V podstate sa zvýši pravdepodobnosť nájdenia potravy zvýšením počtu nezávislých náhodných pokusov. V prípade nájdenia potravy mravce extrahujú feromóny a pritiahnu tak ostatné mravce k potrave. V prípade nájdenia 2 a viac zdrojov potravy sa mravce preskupia na ten zdroj, ku ktorému vedie kratšia cestička, prípade je viac výdatnejší a zdroj s kratšou cestičkou je už nepostačujúci.

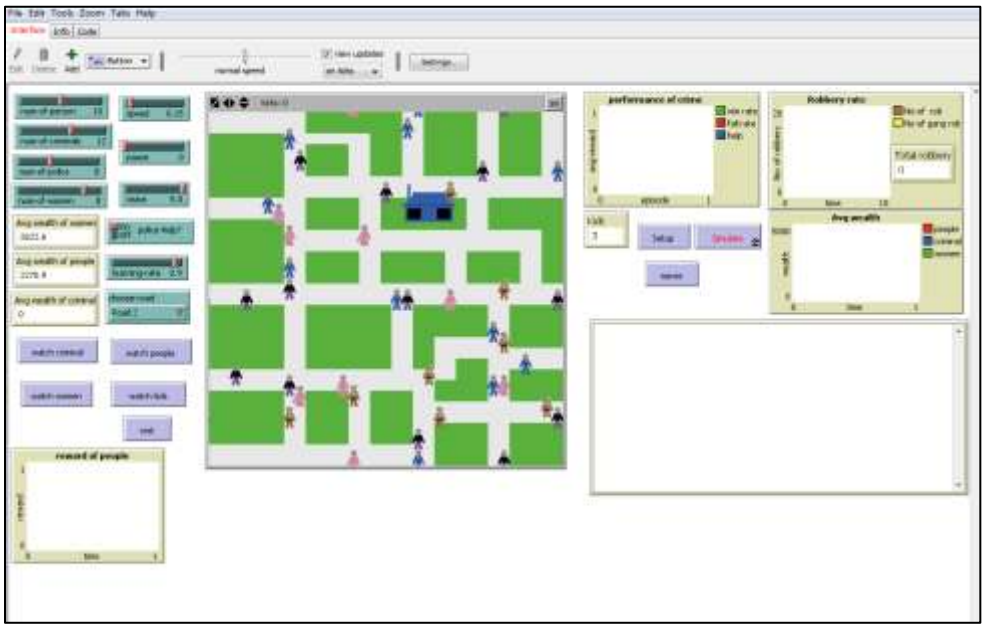
Algoritmus, ktorým mravce prehľadávajú terén je zo skupiny stochastických (skupina prehľadávajúcich algoritmov) a evolučných algoritmov. Zároveň však ide o heuristický algoritmus. Evolučné algoritmy, sú algoritmy určené na prehľadávanie, ktoré sa snažia riešiť problém tak, aby o ňom vedeli čo najmenej. Motiváciu si berú z genetiky a evolúcie. Ich veľká výhoda tkvie v tom, že sú jednoduché. Vďaka čomu sa ľahko implementujú a používajú v praxi. Sú jedným z najlepších nástrojov na hľadanie riešenia zložitých problémov. Tento algoritmus je na báze multiagentového systému. Populáciu v tomto systéme tvorí kolektív – kolónia (množina jednoduchých agentov). Systém je decentralizovaný a samo organizujúci. Populácia sa správa kolektívne, čo je dôsledok nepriamej formy komunikácie (pomocou feromónu). Kolónia rieši úlohu, ktorá je ďaleko za hranicami schopností jej členov.

Multiagentové systémy

Multiagentové systémy sú systémy, v ktorých daná množina inteligentných agentov sa snaží dosiahnuť určitý cieľ. Inteligencia v tomto kontexte znamená použitie algoritmov na hľadanie, nájdenie a vyriešenie problému. Agenti v multiagentových systémoch sú autonómni. Žiadny z agentov sa nepozerá na virtuálny svet globálne. Vnímajú ho len lokálne, pomocou svojich prostriedkov, ktoré im boli pridelené. Agenti na jednej strane disponujú určitými prostriedkami, na druhej strane sú „vsadení“ medzi určité hranice, v rámci ktorých musia daný problém vyriešiť. Ich činnosť je decentralizovaná. Nemajú špeciálneho agenta, ktorý by ich navigoval. Ich správanie je často samoorganizujúce. Vďaka čomu sa snažia nájsť najlepšie riešenie problému, ktorý riešia bez zásahu niečoho iného. Agenti pracujú buď spoločne na vyriešení problému, alebo pracujú samostatne na riešení navzájom súvisiacich problémoch.

Antcomputing v prostredí NetLogo

Ant computing (alebo ant colony optimization) je skupina algoritmov, ktorých predmetom sú modely odvodené na základe pozorovaní mravcov v prírode. Aplikáciou týchto algoritmov do vývojárskeho prostredia môžeme rýchlo a plynule simulovať konkrétne prostredie. Takýmto vývojárskym nástrojom je napr. program Net Logo [16]. Veľkou výhodou Net Loga je, že je to multiplatformové, multiagentové prostredie. Samotné NetLogo je napísané v jazyku Java, model sa píše v jazyku Logo. NetLogo vytvára svet, v ktorom medzi sebou interagujú agenti – mravce. Logo je paralelný programovací jazyk. To znamená, že všetci agenti vykonávajú svoje úlohy súčasne.



Obrázok 1 Simulácia kriminálneho správania v urbanistickom prostredí v programe NetLogo

NetLogo je programovateľné prostredie na modelovanie zložitých dynamických systémov. Zadávaním inštrukcií stovkám až tisíckam nezávislých agentov, ktorí paralelne vykonávajú svoju činnosť, je možné simulovať prírodné i spoločenské javy a skúmať tak súvislosti medzi správaním sa jedincov na mikroúrovni ako aj zložitejších štruktúr vznikajúcich ich interakciou na makroúrovni. Súčasťou prostredia je rozsiahla dokumentácia, návody a knižnica vzorových modelov pochádzajúcich z najrôznejších oblastí prírodných a spoločenských vied, vrátane matematiky a informatiky, fyziky a chémie, biológie a medicíny, ekonomiky a sociálnej psychológie.

V programe NET Logo je preddefinovaný program na simuláciu pohybu agentov (units). Generovanie prostredia zabezpečuje funkcia SETUP a spustenie programu zabezpečuje funkcia GO. Ešte pred spustením simulácie nastavíme veľkosť populácie funkciou POPULATION. Tiež nastavíme difúziu pomocou funkcie DIFFUSION RATE (miera sledovania) a nakoniec nastavíme mieru „vyparovania“ potravy pomocou funkcie EVAPORATION RATE (miera straty záujmu).

Rovnaký princíp ako v simulácií mravcov (agentov) použijeme na simulovanie pohybu osôb. Definovať môžeme aj vlastnosti agentov, napr. vygenerovanému agentovi priradíme vlastnosť, napr. bežná osoba, kriminálnik, policajt, muž alebo žena, rýchlosť pohybu, a tiež mieru učenia sa (vychádza z logiky Antcomputing). Avšak prvé čo potrebujeme definovať je prostredie, v ktorom sa agenti pohybujú. Prostredie bude predstavovať rozmiestnenie možných ciest, po ktorých sa osoba môže pohybovať. Cesty môžu znamenať aj vnútorné členenie budovy.

3 DISKUSIA

V súčasnom období pandémie COVID-19 pohyb osôb v mnohých zariadeniach poskytujúcich zdravotnú starostlivosť nie je obmedzený a ani nie je možné ho vylúčiť, prípadne obmedziť. Ako príklad je možné uviesť nemocnice nadregionálneho významu, ktoré poskytujú ambulantnú a ústavno-preventívnu starostlivosť. Dennodenne navštívi takéto zariadenie množstvo ľudí s cieľom získať potrebnú zdravotnú starostlivosť, pričom nie je možné vylúčiť prípadnú infekčnosť niektorých osôb pohybujúcich sa v priestoroch daného zariadenia.

Monitorovanie pohybu osôb pohybujúcich sa v rámci areálu zdravotníckeho zariadenia sa môže stať významnou pomôckou pri vyhľadávaní kontaktov potvrdených prípadov.

Je pravdou, že v súčasnosti existuje niekoľko technologicky aj aplikačne rôznych riešení. Najčastejšie sa spomína trasovania kontaktov cez mobilné aplikácie. Našou snahou nie je vyvíjať ďalšiu mobilnú aplikáciu. veríme, že niektoré riešenia sú dobré a majú svoje miesto v boji proti šíreniu ochorenia pandémie COVID-19. Je pravdou, že niektoré podmienky neumožňujú nasadzovať mobilné zariadenia na princípe GPS – napr. vnútorné priestory spomínaného zdravotníckeho zariadenia. Výber vhodného riešenia závisí od viacerých technických a cenových kritérií. Tiež nie každé zariadenia disponuje potrebnou personálnou infraštruktúrou, čo by znamenalo ďalšie zvýšenie nákladov. Preto považujeme za dôležité minimalizovať náklady na prevádzku systému trasovania osôb. Mohli by sme tiež uvažovať o automatizovanom systéme bez nutnosti kontaktu s osobou, ktorú chceme trasovať (monitorovať).

Problémom je, že je potrebné na vstupe (začiatok trasovania) prideliť osobe ID, to je možné realizovať napríklad pomocou snímania osoby napríklad kamerovým zariadením, alebo že osoba sa zaregistruje do systému cez tzv. token, ktorý bude musieť nosiť počas svojho pobytu v zdravotníckom zariadení pri sebe.

Samozrejme, že vznikajú ďalšie otázky, napríklad súhlas so spracovaním údajov a či je vôbec potrebné takýto súhlas poskytnúť ak osobe nepriradíme meno a priezvisko, či iný kontakt. Kontakt na osobu je potrebný, ak ju chceme informovať, napr. že sa stretla pozitívne testovanou osobou, že s ňu strávila dlhší čas (napr. v čakárni v blízkosti menšej ako 2 metre viac ako 15 minút) a pod. Otázkou tiež ostáva, či osoba, ktorá vstupuje do verejne prístupného zariadenia môže byť monitorovaná (samozrejme je vopred o tom informovaná) a či sa nejedná o zásah do ochrany osobných údajov (citlivých zdravotníckych údajov).

Môžeme tiež diskutovať o probléme identifikácie pomocou zdravotníckej kartičky, keďže je potrebná pri návšteve zdravotníckeho zariadenia. ďalej môžeme uvažovať o nasadení takéhoto systému len do časti zdravotníckeho zariadenia, napr. návšteva lôžkového oddelenia.

Predpokladáme, že v dôsledku používania systému trasovania osôb napr. v zdravotníckych zariadeniach, môžeme špecifikovať úžitky ako napríklad znižovanie nákladov súvisiacich s vyhľadávaním kontaktov, zvýšenie celkovej presnosti vyhľadávania kontaktov vo vybranom objekte (priemysel, obchody, zamestnanie), zníženie nákladov na realizáciu systémov ochrany štátnych a súkromných objektov, zvýšenie účinnosti navrhovaných systémov ochrany objektov, zníženie nákladov pri posudzovaní rizík, bezpečnostných správ, dokumentov a tiež zvýšenie pripravenosti riešiť podobné krízové situácie aj v budúcnosti.

ZÁVER

Príspevok má za cieľ informovať o možnostiach trasovania pohybu osôb s využitím dostupných technologických hardvérových a softvérových riešení. V príspevku sme stručne opísali súčasné technologické možnosti. Zároveň sme opísali princíp trasovania osôb a vytvorili prienik medzi hardvérovou zložkou a softvérovou na princípe simulácie trasovania osôb. Pre simuláciu sme zvolili metódu AntComputing a prostredie NetLogo. Na záver sme vytvorili ukážku práce v tomto prostredí.

Ďalším krokom bude navrhované technické riešenie a softvérové riešenie otestovať v laboratórnych podmienkach a následne po odladení implementovať v reálnom zdravotníckom zariadení. Testovanie v laboratórnych podmienkach bude sledovať cieľ simulovať rôzne scenáre na trasovaných osobách. Tomu bude taktiež predchádzať podrobná analýza požiadaviek na takýto bezpečnostný systém. Súčasťou toho bude aj návrh grafického rozhrania pre jednoduchšie testovanie s nástrojmi pre notifikáciu, zber nových dát či nastavenie klasifikačných kritérií.

POĎAKOVANIE

Tento článok bol pripravený v rámci podpory projektu APPV-20-0457 Monitorovanie a trasovanie pohybu a kontaktu osôb v zdravotníckych zariadeniach.

LITERATÚRA

[1] Geotab team. What is GPS?. Geotab Inc. 2020. https://www.geotab.com/blog/what-is-gps/
[2] MBUNGE, E, AKINNUWESI, B, FASHOTO, SG, METFULA, AS, MASHWAMA, P. A critical review of emerging technologies for tackling COVID-19 pandemic. Hum Behav & Emerg Tech. 2021. 3. 25– 39. https://doi.org/10.1002/hbe2.237
[3] FDA. Radio Frequency Identification (RFID). 2018. https://www.fda.gov/radiation-emitting-products/electromagnetic-compatibility-emc/radio-frequency-identification-rfid
[4] GERMA, T, LERASLE, F, OUADAH, N, CADENAT, V. Vision and RFID data fusion for tracking people in crowds by a mobile robot. Computer Vision and Image Understanding. 2010. 114/6, 641-651. https://doi.org/10.1016/j.cviu.2010.01.008.
[5] STN EN 62676 Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách.
[6] RAFAJOVÁ, M., VÁRYOVÁ L., Biometrické osobné údaje podľa GDPR (biometrický podpis, kamerový systém). 2019. Praha: Leges. 115s. ISBN 978-80-7502-433-6
[7] TREPTOW, A., CIELNIAK, G., DUCKETT, T. Real-time people tracking for mobile robots using thermal vision. Robotics and Autonomous Systems. 2006. 54. 729-739. 10.1016/j.robot.2006.04.013.
[8] Bluetooth SIG, Inc. Radio Spectrum. 2021. https://www.bluetooth.com/learn-about-bluetooth/key-attributes/range/
[9] iBeacon. What is ibeacon? A guide to beacons. 2021. http://www.ibeacon.com/what-is-ibeacon-a-guide-to-beacons/
[10] NIU. E., What Ever Happened to Apple iBeacons? 2021. The Motley Fool. https://www.fool.com/investing/2016/12/22/what-ever-happened-to-apple-ibeacons.aspx
[11] MAX, R., 12 Technologies to Track People. 2017. https://ronnymax.medium.com/12-technologies-to-track-people-f39d9473c1ae
[12] KUMAR, S., MARKS, T. K., JONES, M. Improving Person Tracking Using an Inexpensive Thermal Infrared Sensor, 2014. IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 217-224, doi: 10.1109/CVPRW.2014.41.
[13] FOD, A., HOWARD., A., MATARIC, M. J., Laser-Based Poeple Tracking. 2002. In Proc. of the IEEE International Conference on Robotics & Automation (ICRA). pp. 3024-3029. doi: 10.1.1.16.1183
[14] MAX, R. 19 Technologies of People Tracking. 2021. https://behavioranalyticsretail.com/technologies-tracking-people/
[15] OOSTERLINCK, D. et. al., Bluetooth tracking of humans in an indoor environment: An application to shopping mall visits. 2017. Applied Geography. 78, 55-65, doi: 10.1016/j.apgeog.2016.11.005.

[16] WILENSKY, U. NetLogo. 1999. http://ccl.northwestern.edu/netlogo/

MANAŽÉRSTVO RIZÍK OBJEKTU „A N“

Ing. Alexander Végsö[*)]

ABSTRAKT

Článok opisuje referenčný objekt „A N“ ako obchodnú prevádzku z hľadiska jej funkcionality, polohy, umiestnenia na pozemku, pôdorysu. Následne identifikuje a hodnotí riziká pre bezpečnosť predmetného objektu. Register rizík vo vzťahu k hodnotám zo záveru článku môže slúžiť ako podklad pre vypracovanie bezpečnostného projektu a bezpečnostnej politiky podnikateľského subjektu, ktorý pôsobí v danom objekte. Uplatnením princípu komplexnosti - zameranie auditu na všetky možné kategórie rizík - vonkajšie, vnútorné, sa autor snaží o ich reálne vyhodnotenie a klasifikáciu. Pre referenčný podnikateľský subjekt je objektová bezpečnosť významná, nakoľko podmieňuje bezpečnosť informačných technológií, ktoré subjekt prevádzkuje a v oblasti ktorých podniká.

Kľúčové slová:
Technická dokumentácia, perimeter objektu, plášť objektu, priestor objektu, analýza rizík, dostatočnosť použitých opatrení, prevádzkový poriadok objektu.

ABSTRACT

The article describes the reference object "A N" as a business operation in terms of its functionality, location, location on the land, floor plan. It then identifies and assesses the risks to the security of the object in question. The register of risks in relation to the values from the end of the article can serve as a basis for the development of a security project and security policy of a business entity operating in the building. By applying the principle of complexity - the focus of the audit on all possible categories of risks - external, internal, the author seeks their real evaluation and classification. Object security is important for a reference business entity, as it conditions the security of information technologies that the entity operates and in the area in which it operates.

Key words:
Technical documentation, building perimeter, building envelope, building space, risk analysis, sufficiency of used measures, operating rules of the building;

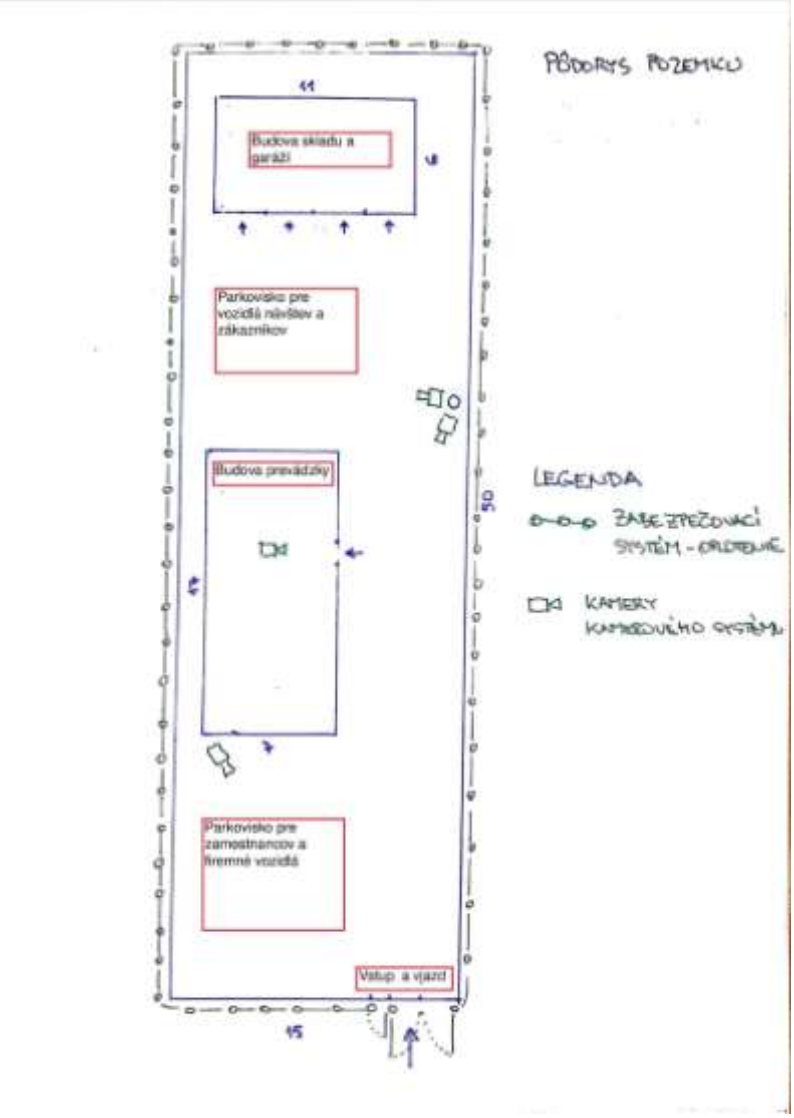
[*)] Ing. Bc. Alexander Végsö, Partizánska cesta 112, 974 01, Banská Bystrica,
+421 905 810 234, alexander.vegso@akcent.sk

1 TECHNICKÁ DOKUMENTÁCIA OCHRANY OBJEKTU

1.1 PERIMETER OBJEKTU

Referenčný objekt „A N“ sa nachádza v katastrálnom území Banská Bystrica na parcele č. 383 v záhradkárskej oblasti v intraviláne. Pozemok o rozlohe 15 m x 50 m. je oplotený klasickým drôteným oplotením bez bezpečnostnej triedy (bariéra s nízkou pasívnou bezpečnosťou), výšky 120 cm, veľkosť oka 50x50 mm a priemerom drôtu 2,2 mm, pevné oceľové stĺpy na ktorých je pletivo upevnené napínacím drôtom sú od seba vzdialené 2 m. Oplotenie je bez vrcholových a podhrabových zábran. Ku pozemku vedie asfaltová miestna komunikácia. Vstup na pozemok je cez otočnú bránku konštruovanú z oceľových profilov výšky 2 m a vjazd cez otočnú dvojkrídlovú bránu konštruovanú z oceľových profilov výšky 2 m. Vstupná bránka a vstupná brána majú namontované bezpečnostné zámky FAB a sú riadené v režime systému generálneho kľúča. Predná časť parcely je situovaná na juh, nachádza sa na nej parkovisko vyhradené pre zamestnancov spoločnosti a firemné vozidlá. Stredná časť parcely je zastavaná samostatne stojacou, dvojpodlažnou, nepodpivničenou budovou prevádzky. Nasleduje parkovisko pre vozidlá návštev a zákazníkov. Zadná časť parcely, situovaná na sever, susedí so železničnou traťou Banská Bystrica – Žilina, nachádza sa na nej samostatne stojacia, nepodpivničená, jednopodlažná budova skladu a garáží.. Pozemok je pripojený na inžinierske siete: elektrina, voda, kanalizácia.

Obrázok č. 1: Satelitný snímok polohy objektu.



Obrázok č. 2: Pôdorys pozemku so stavbami.

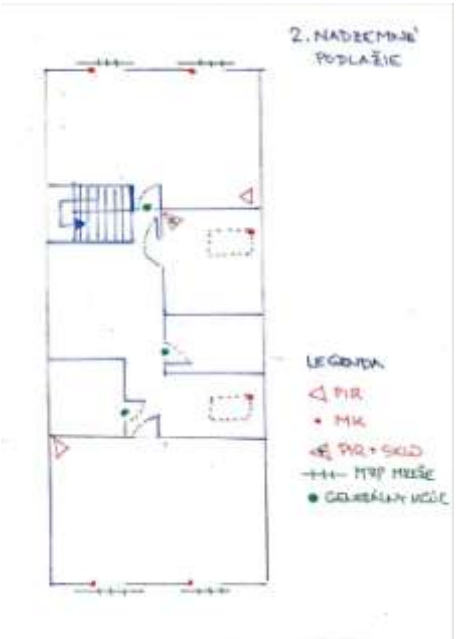
1.2 Plášť objektu

1.2.1 Plášť - budova prevádzky

Samostatne stojaca, nepodpivničená budova prevádzky, má pôdorys tvaru obdĺžnika s rozmermi 7 m x 11 m. Obvodový plášť budovy prevádzky je murovaný, kde nosnú vrstvu tvorí murivo na báze pórobetónových tvárnic YTONG, hrúbky300 mm (trieda reakcie na oheň A1, REI 120/D1, uvádzaná výrobcom), tepelnoizolačnú vrstvu tvorí izolácia z fasádneho polystyrénu hrúbky 200 mm. Vnútorné nosné a nenosné steny sú murované, z murovaného materiálu na báze pórobetónových tvárnic YTONG , hrúbky 250 a 100 mm (trieda reakcie na oheň A1, REI 120/D1). Stropná konštrukcia na d 1. NP je železobetónový strop (REI 120/D1). Strešná konštrukcia je sedlová, hambálková za rasteného dreva(trieda reakcie na oheň D-s2,

d0). Strešnú krytinu tvorí pozinkovaný plech, doplnený o proti zosuvu snehu namontované zábrany po obidvoch stranách strechy. Tepelnoizolačnú vrstvu strechy tvorí tepelná izolácia na báze minerálnej vlny, hrúbky 300 mm + 100 mm (trieda reakcie na oheň A1 – uvádzaná výrobcom), z interiérovej strany sú stropná konštrukcia a trámy opláštené sadrokartónovými doskami trieda reakcie na oheň A2-s1, d0 – uvádzaná výrobcom. Vnútorné povrchy stien tvorí minerálna omietka, v priestoroch kúpeľní a toaliet je keramický obklad. Podlahy kancelárií sú pokryté kobercami a podlahy priestorov technického oddelenia, skladu a serverovne objektovou (komerčnou) podlahovou krytinou B4b – PVC s kompaktnou nosnou vrstvou a nášľapnou vrstvou 0,8 mm.
Otvorové výplne okná na objekte sú štandardné pastové okná, zasklené izolačným troj sklom a dve strešné, drevené okná situované na východ, zasklené troj-sklom.
Vo všetkých oknách sú namontované drôtové magnetické kontakty poplachového systému. Vstupné dvere, situované na východ, sú plastové, bezpečnostné, dvojkrídlové, zasklené dvoj sklom a sú v nich namontované drôtové magnetické kontakty poplachového systému. Vstupné dvere a interiérové dvere kancelárie vedenia majú namontované bezpečnostné zámky FAB a sú riadené v režime systému generálneho kľúča. Pred vstupnými dverami zvonku aj zvnútra, sa nachádza čítačka RFID prístupových médií systému kontroly vstupu prepojená z elektromechanickým závorníkom vstupných dverí a systémom kontroly vstupu a dochádzkovým systémom. Pred vstupnými dverami zvonku sa nachádza audio komunikátor, slúžiaci pre overenie oprávnenia vstupu cez IP telefóniu objektu.
Okrem strešných okien a vstupných dverí sú pred všetky stavebné výplne - okná z vonkajšej strany napevno pod omietku namontované oceľové, zvárané mreže kruhového prierezu s priemerom 2 cm. Pred druhé vstupné dvere technického úseku sú namontované otváracie oceľové, zvárané mreže kruhového prierezu s priemerom 2 cm.

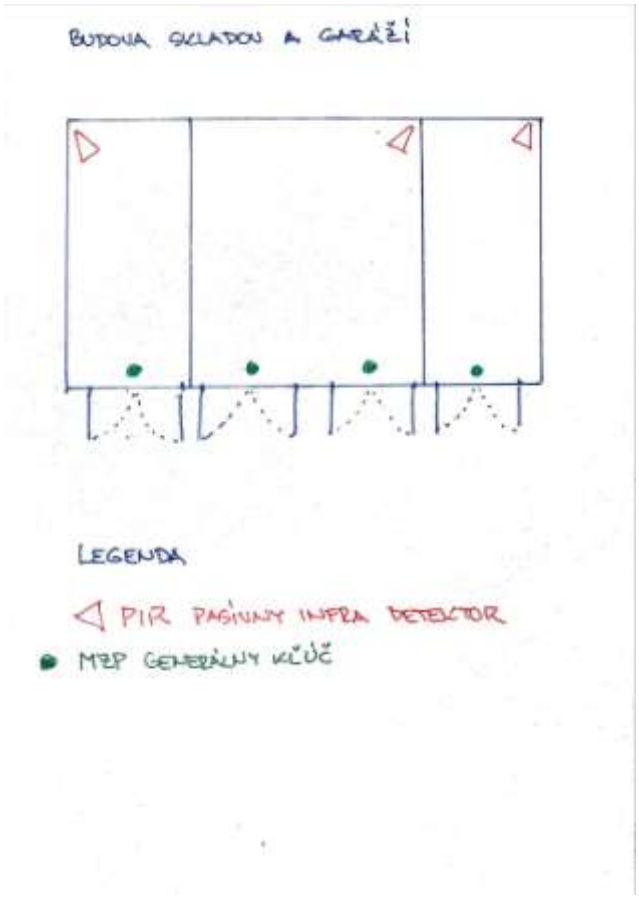
Obrázok č. 3: Pôdorys prvého nadzemného podlažia budovy prevádzky



Obrázok č. 4: Pôdorys druhého nadzemného podlažia budovy prevádzky

1.2.2 Plášť - budova skladu a garáží

Samostatne stojaca nepodpivničená jednopodlažná budova skladu a garáží je tvorená oceľovou konštrukciou ukotvenou na betónovej platni rozmerov 6 m x 11 m. Oceľová konštrukcia je opláštená vlnitým pozinkovaným plechom, rovnako ako strecha tvaru A. Opláštenie je realizované bez zateplenia. Vnútorné priečky tvorí taktiež vlnitý pozinkovaný plech. Jedinými otvorovými výplňami sú štyri dvoj krídlové plechové brány, na ktorých sú namontované bezpečnostné zámky FAB a sú riadené v režime systému generálneho kľúča.



Obrázok č. 5: Pôdorys budovy skladu a garáží

1.3 Priestor objektu

1.3.1 Priestor – budova prevádzky

Na prvom nadzemnom podlaží budovy prevádzky sa nachádza vpravo od vstupu miesto prvého kontaktu, pracovisko sekretariátu a logistiky, ďalej zasadacia a prezentačná miestnosť. Oproti vstupu sa nachádza sklad pre upratovací servis a odpadové hospodárstvo. Smerom doľava nasledujú pánske a dámske toalety a príručný sklad. Oproti toaliet sa nachádza miestnosť serverovne. Ďalej smerom doľava sa

nachádza miestnosť technikov, servisná miestnosť a príručný sklad náradia. Medzi toaletami a zasadacou miestnosťou je schodisko na druhé nadzemné podlažie . Po vystúpení schodiskom vľavo sa nachádza kancelária vedenia, oproti schodisku miestnosť jedálne. Vedľa jedálne sa nachádza miestnosť registratúrneho strediska, oproti neho kuchynka. Vedľa kuchynky sa nachádza toaleta pre vedenie. Nasleduje miestnosť pracoviska vývoja a podpory informačného systému.

Všetky miestnosti budovy prevádzky sú strážené PIR (pasívny infra detektor pohybu) detektormi a miestnosť zasadačky, serverovne a jedálne kombinovaným detektorom PIR a rozbitia skla. Miestnosť serverovne stráži aj detektor dymu a teploty. Ústredňa poplachového systému sa nachádza v serverovni a má vlastný záložný zdroj napätia na 48 hodín, v prípade prerušenia dodávky 230 V. Poplachový systém je pripojený pomocou GPRS vysielača na PPC/PCO poplachové prijímacie centrum / pult centralizovanej ochrany súkromnej bezpečnostnej služby.
Vstup do budovy z vnútra monitoruje dome IP kamera, ktorá je súčasťou kamerového systému objektu. Záznamové zariadenie NVR kamerového systému sa nachádza v serverovni, má vlastný záložný zdroj UPS a je pripojené na internet, následne tak aj na pracovisko PPC/PCO súkromnej bezpečnostnej služby.

1.3.2 Priestor – budova skladu a garáží

V budove skladu a garáží sú tri miestnosti: prvá zľava je garáž s plechovými dvojkrídlovými dverami, druhá zľava je dvoj garáž s dvoma dvojkrídlovými plechovými dverami a tretia miestnosť je sklad s plechovými dvojkrídlovými dverami. Iné stavebné otvory sa na budove nenachádzajú.

Analýza rizík

Pod pojmom riziko, v zmysle STN ISO 31000:201, rozumieme účinok neistoty na zámery. Pričom účinok, chápeme ako výsledok istého pôsobenia, pozitívnej alebo negatívnej odchýlky od očakávania, ktorá môže pozitívne alebo negatívne ovplyvňovať zámery, ciele. Pojem neistota predstavuje stav, aj keď čiastočného nedostatku informácií, ktoré sa týkajú chápania alebo vedomostí o udalosti, jej následkoch alebo možnostiach. Tento stav vedie k neprimeranému, či neúplnému poznaniu alebo porozumeniu udalosti, jej následkov alebo pravdepodobnosti. Preto je žiadúce redukovať, manažovať neistotu, ako je to možné. Rozlišujúcim faktorom medzi rizikom a neistotou je, že riziko sa berie ako merateľná vlastnosť a má miesto v kalkulácii pravdepodobnosti, zatiaľ čo neistota takúto vlastnosť nemá. V tejto kapitole sa budeme zaoberať analýzou rizík bezpečnosti objektu, a to identifikáciou rizík vonkajších a vnútorných, hodnotením rizík z hľadiska pravdepodobnosti a následkov a nakoniec zostavením registra rizík vo vzťahu k hodnotám.

2.1 Identifikácia rizík

Identifikácia rizík je najdôležitejším procesom pre efektívne (znamená to tak, že sa na bezpečnosť nevydáva viac, ani menej prostriedkov, než je suma hodnôt neriadených rizík) manažovanie rizík. Jeho podstata je v neustálom odhaľovaní možných negatívnych udalostí a javov daného bezpečnostného prostredia. Riziká vo všeobecnosti delíme na vonkajšie a vnútorné.

2.1.1 Vonkajšie riziká

Vonkajšie riziká zahŕňajú tie, ktorých zdroje sa nachádzajú mimo objektu a pôsobia z vonku chráneného objektu.

2.1.1.1 Živelné pohromy a katastrofy

Poškodenie rozsiahlym požiarom, poškodenie spôsobené úderom blesku, poškodenie vodou spôsobené prívalovými dažďami, poškodenie spôsobené zemetrasením, poškodenie spôsobené zosuvom pôdy.

2.1.1.2 Havárie stacionárnych alebo mobilných zdrojov

Požiar automobilu na parkoviskách a v garážach objektu, únik nebezpečných látok z automobilu na parkoviskách a v garážach objektu, porucha vodovodnej prípojky, pád vzdušného elektrického vedenia v blízkosti objektu, požiar trafostanice vysokého napätia v blízkosti objektu.

2.1.1.3 Kriminálne činy

Krádež alebo poškodenie motorového vozidla z parkoviska alebo garáže objektu, krádež hnuteľného majetku z pozemku objektu, krádež majetku vlámaním, poškodenie nehnuteľného majetku, lúpež, kyber-kriminalita.

2.1.2 Vnútorné riziká

Zdroj vnútorných rizík sa nachádza vnútri objektu alebo jeho súčasti.

2.1.2.1 Technologické a technické zariadenia

Požiar spôsobený poruchou vnútorného elektrického zariadenia, zaplavenie spôsobené prasknutím vodovodného potrubia, znehodnotenie a strata dát.

2.1.2.2 Bezpečnosť a ochrana zdravia pri práci

Pracovný úraz spôsobený zasiahnutím elektrickým prúdom, choroba z povolania spôsobená nadmerným sledovaním monitorov pracovných staníc personálnych počítačov, choroba z povolania spôsobená sedavým spôsobom výkonu práce, pracovný úraz spôsobený haváriou na služobnom vozidle, pracovný úraz spôsobený pádom z výšky.

2.1.2.3 Kriminálne skutky

Krádež majetku, krádež know-how, kyberkriminalita, poškodenie majetku úmyselné, poškodenie majetku nedbanlivostné.

2.2 Register rizík

Dôslednou a objektívnou analýzou, najmä zodpovedaním otázok „ČO sa môže stať?“, „PREČO sa to môže stať?“, predmetného bezpečnostného prostredia, v našom prípade objekt „A N“, vypracujeme register bezpečnostných rizík, ktoré produkuje bezpečnostné prostredie.

Tabuľka 1 *Register rizík*

Oblasť rizika	**Druh rizika**	**Forma prejavu**	**Príčiny, zdroje ,**
Vonkajšie riziká	Poškodenie rozsiahlym požiarom	Požiar	Havária
	Poškodenie spôsobené úderom blesku	Požiar, poškodenie elektroniky	Živelné pohromy a katastrofy
	Poškodenie vodou spôsobené prívalovými dažďami	Zaplavenie	Živelné pohromy a katastrofy
	Poškodenie spôsobené zemetrasením	Zrútenie, poškodenie statiky budov	Živelné pohromy a katastrofy
	Poškodenie spôsobené zosuvom pôdy	Zrútenie, poškodenie statiky budov	Živelné pohromy a katastrofy
	Požiar automobilu na parkoviskách a v garážach objektu	Požiar	Havária, technická porucha
	Únik nebezpečných látok z automobilu na parkoviskách a v garážach objektu	Ekologická havária	Havária, technická porucha

	Porucha vodovodnej prípojky	Zatopenie, zastavenie dodávky vody	Živelné pohromy a katastrofy
	Pád vzdušného elektrického vedenia v blízkosti objektu	Požiar, zasiahnutie elektrickým prúdom	Živelné pohromy a katastrofy, havária, technická porucha
	Požiar trafostanice vysokého napätia v blízkosti objektu	Požiar, zasiahnutie elektrickým prúdom	Živelné pohromy a katastrofy, havária, technická porucha
	Krádež alebo poškodenie motorového vozidla z parkoviska alebo garáže objektu	Vlámanie	Náhodný páchateľ
			Organizovaná skupina
			Konkurencia
		Sabotáž	Konkurencia
	Krádež hnuteľného majetku z pozemku objektu	Vlámanie	Náhodný páchateľ
			Organizovaná skupina
			Konkurencia
		Sabotáž	Konkurencia
	Krádež majetku vlámaním	Vlámanie	Náhodný páchateľ
			Organizovaná skupina
			Konkurencia
		Sabotáž	Konkurencia
	Poškodenie nehnuteľného majetku	Vlámanie	Náhodný páchateľ
			Organizovaná skupina
			Konkurencia
		Sabotáž	Konkurencia
	Lúpež	Lúpežné prepadnutie	Náhodný páchateľ
			Organizovaná skupina
	Kyberkriminalita	Hackerský útok	Páchateľ alebo páchatelia kybernetickej trestnej činnosti
		Malware	
		Škodlivý kód	
		Neoprávnený prístup do počítačového systému, programu, údaja	
Vnútorné riziká	Požiar spôsobený poruchou vnútorného elektrického zariadenia	Požiar	Skrat, technická porucha

	Zaplavenie spôsobené prasknutím vodovodného potrubia	Zaplavenie	Havária, technická porucha,
	Znehodnotenie a strata dát	Nedostupnosť dát	Zamestnanci
	Pracovný úraz spôsobený zasiahnutím elektrickým prúdom	Ujma na zdraví, prerušenie alebo zníženie pracovnej výkonnosti	Zamestnanci
	Choroba z povolania spôsobená nadmerným sledovaním monitorov pracovných staníc personálnych počítačov	Ujma na zdraví, prerušenie alebo zníženie pracovnej výkonnosti	Zamestnanci
	Choroba z povolania spôsobená sedavým spôsobom výkonu práce	Ujma na zdraví, prerušenie alebo zníženie pracovnej výkonnosti	Zamestnanci
	Pracovný úraz spôsobený haváriou na služobnom vozidle	Ujma na zdraví, prerušenie alebo zníženie pracovnej výkonnosti	Zamestnanci
	Pracovný úraz spôsobený pádom z výšky	Ujma na zdraví, prerušenie alebo zníženie pracovnej výkonnosti	Zamestnanci
	Krádež majetku	Manko v inventúre skladu a majetku	Zamestnanci
			Outsourcovaní dodávatelia

	Krádež know-how	Prezradenie obchodného tajomstva	Zamestnanci
			Outsourcovaní dodávatelia
	Kyberkriminalita	Prezradenie obchodného tajomstva, krádež, poškodenie, dát	Správca siete
			Zamestnaci
			Rodinný príslušníci zamestnancov
			Outsourcovaní dodávatelia
	Poškodenie majetku úmyselné	Zníženie hodnoty majetku	Zamestnaci
	Poškodenie majetku nedbanlivostné	Zníženie hodnoty majetku	Zamestnaci
			Rodinný príslušníci zamestnancov
			Outsourcovaní dodávatelia

2.3 Hodnotenie rizík

Cieľom hodnotenia identifikovaných rizík je priradiť každému riziku číselnú hodnotu, alebo slovné hodnotenie. Platí rovnosť, že **R**iziko je funkciou **P**ravdepodobnosti výskytu rizika a **D**ôsledku rizika **R** =**P** x **D**.
Na účely hodnotenia rizík sa využívajú nasledujúce skupiny metód:
Kvantitatívne metódy – využívajú numerické ohodnotenie rizík vyjadrením ich pravdepodobnosti, početnosti, vierohodnosti, dôsledkov a pod. dajú sa hlavne použiť v prípadoch ak je dostatok relevantných údajov, ktoré sa dajú ohodnotiť štatisticky.
Kvalitatívne metódy – využívajú slovné vyjadrenia v prípadoch ak ide jednoduché situácie, alebo ak chýbajú alebo ak sú ťažko dostupné číselné hodnoty (údaje) pre kvantitatívne ohodnotenia rizík.
Polo kvantitatívne metódy – využívajú kvalitatívne popísanie stupnice, ktoré majú pridelené číselné hodnoty. Kombináciou týchto charakteristík sa určí hodnota rizík.

V našom prípade budeme hodnotiť riziko kvalitatívnou metódou pomocou uvedenej tabuľky.

Tabuľka 2 *Hodnotenie veľkosti rizika funkciou pravdepodobnosti a dôsledkov*

Pravdepodobnosť výskytu udalosti	**D**ôsledky výskytu rizika				
	VM Veľmi malé, Nevýznamné: **Nijaký úraz, minimálne, zanedbateľné škody, veľmi malé finančné straty**	**M** Malé: **Ľahké poškodenia zdravia, malé škody, malé finančné straty**	**S** Stredné: **Vážnejšie poškodenia zdravia, rozsiahlejšie škody na majetku, poškodenia objektov, väčšie finančné straty**	**V** Veľké: **Ťažké poškodenia zdravia, veľké škody na majetku, rozsiahle poškodenia objektov, veľké finančné straty**	**VV** Veľmi veľké: **Usmrtenie osôb, veľmi veľké škody na majetku, zničenie objektov, veľmi veľké finančné straty**
Takmer istá	**V (veľké)**	**V**	**VV (veľmi veľké)**	**VV**	**VV**
Asi nastane	**NM (nie malé)**	**V**	**V**	**VV**	**VV**
Možno nastane	**M (malé)**	**NM**	**V**	**VV**	**VV**
Asi nenastane	**M**	**M**	**NM**	**V**	**VV**
Sotva nastane	**M**	**M**	**NM**	**V**	**V**

Tabuľka 3 *Hodnotenie rizík*

Oblasť rizika	**Druh rizika**	**Pravdepodobnosť výskytu udalosti**	**Dôsledky výskytu rizika**	**Veľkosť rizika**
Vonkajšie riziká	Poškodenie rozsiahlym požiarom	Asi nenastane	VV	**VV**
	Poškodenie spôsobené úderom blesku	Sotva nastane	M	**V**
	Poškodenie vodou spôsobené prívalovými dažďami	Sotva nastane	S	**NM**
	Poškodenie spôsobené zemetrasením	Sotva nastane	S	**NM**
	Poškodenie spôsobené zosuvom pôdy	Sotva nastane	S	**NM**
	Požiar automobilu na parkoviskách a v garážach objektu	Asi nenastane	V	**V**
	Únik nebezpečných látok z automobilu na parkoviskách a v garážach objektu	Asi nenastane	M	**M**
	Porucha vodovodnej prípojky	Možno nastane	Malé	**NM**
	Pád vzdušného elektrického vedenia v blízkosti objektu	Asi nenastane	Veľmi malé	**M**
	Požiar trafostanice vysokého napätia v blízkosti objektu	Asi nenastane	Veľmi malé	**M**
	Krádež alebo poškodenie motorového vozidla z parkoviska alebo garáže objektu - Vlámanie	Asi nenastane	Stredné	**NM**

	Krádež alebo poškodenie motorového vozidla z parkoviska alebo garáže objektu - Sabotáž	Sotva nastane	Stredné	**NM**
	Krádež hnuteľného majetku z pozemku objektu – Vlámanie	Asi nenastane	Veľmi malé	**M**
	Krádež hnuteľného majetku z pozemku objektu - Sabotáž	Asi nenastane	Veľmi malé	**M**
	Krádež majetku vlámaním	Sotva nastane	Veľmi malé	**M**
	Krádež majetku vlámaním - sabotáž	Sotva nastane	Veľmi malé	**M**
	Poškodenie nehnuteľného majetku - vlámanie	Asi nenastane	Malé	**M**
	Poškodenie nehnuteľného majetku - sabotáž	Asi nenastane	Malé	**M**
	Lúpež Lúpežné prepadnutie	Asi nenastane	Malé	**M**
	Kyberkriminalita Hackerský útok	Možno nastane	Veľké	**VV**
	Kyberkriminalita Malware	Možno nastane	Veľké	**VV**
	Kyberkriminalita Škodlivý kód	Možno nastane	Veľké	**VV**
	Kyberkriminalita Neoprávnený prístup do počítačového systému, programu, údaja	Možno nastane	Veľké	**VV**
Vnútorné riziká	Požiar spôsobený poruchou vnútorného elektrického zariadenia	Asi nenastane	Veľké	**V**

	Zaplavenie spôsobené prasknutím vodovodného potrubia	Asi nenastane	Stredné	**NM**
	Znehodnotenie a strata dát	Možno nastane	Veľké	**VV**
	Pracovný úraz spôsobený zasiahnutím elektrickým prúdom	Asi nenastane	Veľké	**V**
	Choroba z povolania spôsobená nadmerným sledovaním monitorov pracovných staníc personálnych počítačov	Možno nastane	Stredné	**V**
	Choroba z povolania spôsobená sedavým spôsobom výkonu práce	Možno nastane	Stredné	**V**
	Pracovný úraz spôsobený haváriou na služobnom vozidle	Možno nastane	Veľmi veľká	**VV**
	Pracovný úraz spôsobený pádom z výšky	Možno nastane	Veľmi veľká	**VV**
	Krádež majetku zamestnanci	Sotva nastane	Stredné	**NM**
	Krádež majetku - Outsourcovaní dodávatelia	Sotva nastane	Stredné	**NM**
	Krádež know-how Zamestnanci	Asi nenastane	Veľké	**V**
	Krádež know-how Outsourcovaní dodávatelia	Asi nenastane	Veľké	**V**
	Kyberkriminalita správca siete	Asi nenastane	Veľké	**V**

	Kyberkriminalita Zamestnaci	Asi nenastane	Veľké	**V**
	Kyberkriminalita Rodinný príslušníci zamestnancov	Sotva nastane	Veľké	**V**
	Kyberkriminalita Outsourcovaní dodávatelia	Sotva nastane	Veľké	**V**
	Poškodenie majetku úmyselné zamestnanci	Sotva nastane	Veľké	**V**
	Poškodenie majetku nedbanlivostné zamestnanci	Asi nenastane	Veľké	**V**
	Poškodenie majetku nedbanlivostné Rodinný príslušníci zamestnancov	Sotva nastane	Stredné	**NM**
	Poškodenie majetku nedbanlivostné Outsourcovaní dodávatelia	Asi nenastane	Stredné	**NM**

Preukázanie dostatočnosti použitých opatrení v súlade so závermi vyplývajúcimi z analýzy rizík

Bezpečnostnú politiku ochrany objektu bude tvoriť syntéza bezpečnostných opatrení navrhnutých viacvrstvovo, spôsobom perimeter, plášť, priestor, predmet, osoba, informácia.

3.1 Perimeter

„Perimetrická“ ochrana, viď *obrázok č. 2 je* kombináciou zabezpečovacieho systému - oplotenie pozemku a bezpečnostného zámku vstupnej bránky a brány v režime generálneho kľúča, spolu s kamerovým systémom pripojeným na PPC/PCO súkromnej bezpečnostnej služby.

3.2 Plášť

„Plášťová“ ochrana objektu budovy prevádzky viď *obrázok č. 3, 4* je tvorená zabezpečovacím systémom – vonkajším omrežovaním okien a druhých vstupných dverí, bezpečnostnými vstupnými dverami so zámkom FAB v režime systému generálneho kľúča. Ďalej nasleduje systém kontroly vstupu a dochádzky vstupných dverí, prepojený s audio vrátnikom cez IP telefóniu. Ochranu plášťa budovy tvorí aj

časť poplachového systému pripojeného na PPC/PCO SBS, formou magnetických kontaktov vo dverách a oknách budovy. „Plášťovú ochranu budovy skladu a garáží viď *obrázok č. 5* tvoria bezpečnostné zámky v režime systému generálneho kľúča a stavebné prevedenie - plechové opláštenie.

3.3 Priestor

Priestorovú ochranu objektu budovy prevádzky viď *obrázok č.3, 4* tvorí kamerový systém – kamera snímajúca hlavný vstup z vnútra, ďalej poplachový systém súborom „PIR“ detektorov vo všetkých miestnostiach, „PIR plus SKLO“ kombinovaných detektorov v miestnosti serverovne, zasadačky, jedálne a detektoru dymu a teploty v miestnosti serverovne. Poplachový systém je pripojený GPRS vysielačom technológie NAM multiSIM na PPC/PCO SBS. Kamerový systém je pripojený vytvorením užívateľského konta na PPC/PCO SBS ako verifikačná súčasť systému, pre overenie a dokumentovanie poplachových správ z poplachového systému a preventívny monitoring stavu.
Priestorovú ochranu budovy skladu a garáží tvoria „PIR“ detektory v každej miestnosti budovy.

3.4 Predmet

Predmetovú ochranu tvorí certifikovaný trezor (z pochopiteľných dôvodov nezakreslený na obrázkoch) a príručné kovové uzamykateľné trezory – pokladnice“ v mieste prvého kontaktu a výdaja tovaru.

3.5 Osoba

Ochrana osôb je zabezpečená formou zadania bezpečnostného kódu na PPC/PCO SBS cez „RIZ“ – klávesnici poplachového systému, nakoľko postačuje ako iniciácia prípadného poplachu v stave tiesne a nie je potrebné do systému priraďovať „hold-up device“, takzvané panik tlačidlo. Ďalej ochranu osôb zabezpečujú dve plne vybavené lekárničky po jednej na každom podlaží budovy prevádzky a systém školení v oblasti bezpečnosti a ochrany pri práci a ochrany pred požiarmi, zabezpečovaný outsourcovanou zmluvnou spoločnosťou.

3.6 Informácia

Ochranu informácií – dát zabezpečuje licencovaný antivírusový program, licencovaný firewall, automatizované zálohovanie dát, záložné zdroje napätia UPS, organizačné a režimové opatrenia pre prístup a používanie pracovných staníc a mobilných zariadení, implementácia GDPR a výber dodávateľov prednostne s certifikáciou ISO/IEC 27000.

Stručný prevádzkový poriadok ochrany objektu

Prevádzkový poriadok obsahuje vybrané režimové opatrenia platné pre objekt "A N" Do objektu sa vstupuje vstupnou bránou odomknutím bezpečnostného zámku, následne do budovy prevádzky sa vstupuje hlavným vstupom odomknutím bezpečnostného zámku, v prípade že oprávnená osoba vstupuje ako prvá, inak sa použije pridelené prístupové médium na vonkajšej čítačke „Príchod", ktoré otvorí závorníkom vstupné dvere. Ak oprávnená osoba vstupuje v daný deň ako prvá, zadá na RIZ – klávesnici poplachového systému, PIN kód, skôr ako uplynie príchodový čas 15 sekúnd, ktorý vypne stráženie budovy prevádzky a budovy skladu a garáží, poplachovým systémom.
Pri odchode z objektu, ak osoba, ktorá odchádza nie je posledná v objekte, postačuje identifikácia prístupovým médiom na čítačke „Odchod" z vnútra pri vstupných dverách. Ak odchádzajúca osoba je posledná v objekte, skontroluje uzatvorenie okien a vstupných dverí, inak nie je možné aktivovať – zapnúť poplachový systém. Následne zadá PIN kód uzatvorí a uzamkne vstupné dvere skôr ako uplynie odchodový čas 15 sekúnd. V prípade chybného zadania kódu alebo inej udalosti, ktorá indikuje poplach, oprávnená osoba msí do 90 sekúnd zavolať na číslo PPC/PCO SBS a potvrdiť „Falošný poplach" aj nahlásením bezpečnostného hesla. Ak je heslo vyslovené oprávnenou osobou v správnom formáte, poplach je zrušený a zásahová skupina SBS nejde na preverenie poplachu, inak pokračuje proces preverenia poplachovej správy výjazdom zásahovej skupiny SBS.
Počas víkendov a sviatkov a mimo pracovnej doby 18:00 – 06:00 je oprávnená osoba pri vstupe do objektu prevádzky alebo budovy skladu a garáží, po vypnutí poplachového systému PIN kódom, identifikovať sa na PPC/PCO heslom, inak je realizovaný výjazd zásahovej skupiny SBS na preverenie stavu.

V prípade preverovania poplachovej udalosti vzniknutej na objekte, sú stanovené a na PPC/PCO nadefinované, tri kontaktné osoby, ktoré obsluha pultu centralizovanej ochrany kontaktuje v danom poradí, aby sa ak je to možné, zúčastnili na preverení poplachovej správa z objektu. Ak je účasť kontaktnej osoby nemožná alebo nežiadúca, má zásahová skupina pridelený prístupový PIN kód do ústredne poplachového systému a taktiež generálny kľúč.

Jedenkrát do mesiaca v nepravidelných intervaloch vykonáva zásahová skupina výjazdom monitorovanie objektu a tak preventívne demonštruje, že objekt je strážený súkromnou bezpečnostnou službou.

Záver

Vypracované podklady budú použité aj na technickú dokumentáciu objektu, ktorá obsahuje identifikáciu a rozmiestnenie prvkov „ZS" zabezpečovacích systémov, (oplotenie, mreže, zámky , bezpečnostné dvere a okná...), prvkov „PS" poplachového systému (ÚPS ústredňa poplachového systému, RIZ riadiace a identifikačné zariadenie

– klávesnica, PIR detektory, MK magnetické kontakty...), prvkov „KS“ kamerového systému (K kamera, NVR záznamové zariadenie...), prvkov „SKV“ systému kontroly vstupu. Ďalej budú tieto podklady, najmä register rizík a následné hodnotenie rizík kvalitatívnou metódou použité ako základ pre komplexnú bezpečnostnú politiku predmetného objektu „A N“, ako aj implementáciu GDPR – ochrany osobných údajov a audit ISO/IEC 27000.

SOULAD ODBORNÝCH ZNALOSTÍ A ZPÔSOBILOSTÍ ABSOLVENTA PROGRAMU BEZPEČNOSTNÍ TECHNOLOGIE, SYSTÉMY A MANAGEMENT S POŽADAVKY NA „BEZPEČNOSTNÍ OBORY

Martin Hromada[11]

ABSTRAKT

Dlouhodobým záměrem UTB v rámci rozvoje studijního programu Bezpečnostní technologie, systémy a management je vytvoření znalostního a kompetenčního základu absolventa, reflektujícího aktuální trendy v bezpečnostních vědách, oborech a trendech. Logickým krokem je proto tvorba předmětného programu v souladu s "Požadavky na studijní programy vysokých škol z oblasti vzdělávání „Bezpečnostní obory". Text článku bude proto prezentovat relevantní soubor předmětů i s počtem hodin, jako reflexi stanovených požadavků.

Klíčové slova: Bezpečnostní obory, Bezpečnostní technologie, systémy a management, Národní kvalifikační rámec terciálního vzdělávání,

ABSTRACT

TBU's long-term intention within the development of the Security Technologies, Systems and Management study program is to create a graduate's knowledge and competence base, reflecting current trends in security sciences, specialization and trends. The logical step is therefore the creation of the subject program in accordance with the "Requirements for study programs of universities in the specialization of education" Security specialization ". The text of the article will therefore present a relevant set of subjects with the number of hours, as a reflection of the requirements.

Key words: Security specialization, Security technologies, systems and management, National qualification framework of tertiary education,

[11] doc. Ing. Martin Hromada, Ph.D., Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, Ústav bezpečnostního inženýrství, Nad Stráněmi 4511, Zlín, 76005, ČR, +420608454732, hromada@utb.cz

ÚVOD

Magisterský studijní program Bezpečnostní technologie, systémy a management je akademicky zaměřený studijní program, který klade důraz na multidisciplinární propojení znalostí technického, manažerského a právního charakteru. V rámci tohoto studijního programu jsou vychováváni odborníci pro technické, manažerské, projekční a jiné funkce v soukromých bezpečnostních službách zabývajících se ochranou majetku a osob s důrazem na aplikace moderních informačních technologií. Mezioborové studium s převahou technických předmětů dává absolventům možnost uplatnit se v oblastech mechanického a elektronického zabezpečení objektů, dále v oblastech informačně-technologických a právně-bezpečnostních. Vzhledem k zahrnutí problematiky krizového řízení je uplatnění absolventů možné i ve státní správě.

Předkládaný studijní program a včetně profilu absolventa je plně v souladu s Dlouhodobým záměrem UTB, který si vytyčil jako jeden z cílů implementaci Národního kvalifikačního rámce terciárního vzdělávání[3].

1. SOULAD MAGISTERSKÉHO STUDIJNÍHO PROGRAMU BEZPEČNOSTNÍ TECHNOLOGIE, SYSTÉMY A MANAGEMENT S POŽADAVKY MINISTERSTVA VNITRA NA BEZPEČNOSTNÍ MINIMUM

Dle dokumentu vydaného Ministerstvem vnitra s názvem „Požadavky na studijní programy vysokých škol z oblasti vzdělávání „Bezpečnostní obory“ se zaměřením na ochranu obyvatelstva a krizové řízení“[66], je bezpečnostní minimum naplněno uvedenými předměty studijního programu Bezpečnostní technologie, systémy a management, viz Tabulka 1.

Tabulka 1: Soulad magisterského studijního programu Bezpečnostní technologie, systémy a management s požadavky Ministerstva vnitra na bezpečnostní minimum.[1]

Předmětový blok	Min. vyuč. hodin	Relevantní předmět (s počtem hodin) studijního programu Bezpečnostní technologie, systémy a management
Krizové řízení	60	Technologie krizového řízení (14h) (Systém KŘ v ČR, Orgány KŘ a vzájemné vazby, Havarijní a krizové plánování, Bezpečnostní rady a krizové štáby, Prevence závažných havárií, Finanční zabezpečení krizových opatření, Krizové řízení v bankovním a finančním sektoru) Informační podpora bezpečnostních systémů (12h) (Kybernetická bezpečnost, Informační systémy a technologie pro podporu KŘ) Management bezpečnostního inženýrství (8h) (Analýza rizik, Bezpečnostní politika státu, Financování obnovy území) Teorie bezpečnosti (10h) (Legislativa a základní pojmy, Civilní nouzová připravenost EU a NATO) Pokročilé bezpečnostní technologie (8h) (Povodňová ochrana) Bezpečnost veřejných akcí (10h) (Krizové řízení ve

		zdravotnictví)
Hospodářská opatření pro krizové stavy	40	Teorie bezpečnosti (10h) (Legislativa a základní pojmy) Management bezpečnostního inženýrství (10h) (Informační podpora HOPKS, Plánování věcných zdrojů k zajištění bezpečnosti ČR, Vyžadování věcných zdrojů za krizové situace) Ochrana obyvatelstva (20h) (Místo a úlaha HOPKS v bezpečnostním systému ČR, Systém nouzového hospodářství, Systém hospodářské mobilizace, Použití státních hmotných rezerv, Výstavba a údržba nezbytné infrastruktury, Systém regulačních opatření) Technologie krizového řízení (12h) (Působnost orgánů krizového řízení v systému HOPKS)
Obrana státu	40	Management bezpečnostního inženýrství (10h) (Povinnosti státních orgánů a orgánů územních samosprávných celků při zajišťování obrany ČR, Dílčí plány obrany, Příprava občanů k obraně státu, Operační příprava státního území) Elektronické zabezpečovací a přístupové systémy (16h) (Role ozbrojených sil ČR v bezpečnostním systému ČR, Použití armády ČR při nevojenských krizových situacích) Bezpečnostní futurologie (16h) (Právní předpisy, strategické a koncepční dokumenty a základní pojmy, Zapojení ČR do mezinárodních organizací (OSN, NATO, EU, OBSE, …), Kolektivní obrana NATO, Národní systém reakce na krize pro potřeby řízení obrany státu, Řešení krizových situací vojenského charakteru, Právní aspekty válečných konfliktů)
Ochrana obyvatelstva	20	Ochrana obyvatelstva (8h) (Varování, vyrozumění a způsob poskytování tísňových informací, Evakuace, ukrytí, Individuální a kolektivní ochrana obyvatelstva, Preventivně výchovná činnost, Ochrana obyvatelsta při stavu ohrožení státu a za válečného stavu) Bezpečnost veřejných akcí (10h) (Dekontaminace, Příprava obyvatelstva k sebeochraně) Technologie budov (10h) (Stavby dotčené požadavky civilní ochrany)
Integrovaný záchranný systém	20	Informační podpora bezpečnostních systémů (12h) (Složky IZS, jejich koordinace a úrovně řízení, Dokumentace a komunikace v IZS) Technologie krizového řízení (4h) (Využití IZS při mezinárodní spolupráci) Ochrana obyvatelstva (8h) (Legislativa, Požární ochrana, Psychosociálni pomoc)
Vnitřní bezpečnost a veřejný pořádek	20	Teorie bezpečnosti (6h) (Legislativa, Základní pojmy trestního práva, Kriminalistika)

		Elektronické zabezpečovací a přístupové systémy (8h) (Místní záležitosti veřejného pořádku) Bezpečnost veřejných akcí (10h) (Hybridní hrozby, Útoky na tzv. „měkké cíle“)
Zdravotnictví	20	Základy první pomoci (5h) (Úkoly a činnost zdravotnické složky v místě zásahu, Pandemické plány a typové plány) Ochrana obyvatelstva (8h) (Legislativa a základní pojmy, Mezinárodní zdravotnické předpisy a jejich implementace v ČR) Technologie krizového řízení (12h) (Civilní nouzová připravenost EU a NATO v oblasti zdravotnictví, Zabezpečení resortu zdravotnictví za vojenských krizových stavů, Vysoce specializovaná centra a jejich úkoly, Úloha neziskových organizací)
Kritická infrastruktura	20	Systém bezpečnosti a veřejná správa (8h) (Ochrana kritické infrastruktury na úrovni EU) Management bezpečnostního inženýrství (6h) (Působnost orgánů v oblasti kritické infrastruktury) Teorie bezpečnosti (8h) (Proces určování prvků kritické infrastruktury) Informační podpora bezpečnostních systémů (6h) (Povinnosti subjektu kritické infrastruktury)
Celkem	240	

2. SOULAD STUDIJNÍHO PROGRAMU BEZPEČNOSTNÍ TECHNOLOGIE, SYSTÉMY A MANAGEMENT SE ZÁKLADNÍM TEMATICKÝMI OKRUHY PRO OBLAST VZDĚLÁVÁNÍ „BEZPEČNOSTNÍ OBORY“

Následující tabulka uvádí základní tematické okruhy, které jsou u předkládaného studijního programu Bezpečnostní technologie, systémy a management v plném nebo částečném souladu s Nařízením Vlády č. 275/2016 Sb., o oblastech vzdělávání ve vysokém školství [4].

Tabulka 2: Soulad studijního programu Bezpečnostní technologie, systémy a management se základním tematickými okruhy pro oblast vzdělávání Bezpečnostní obory (hodnota 5 odpovídá 100% souladu s tematickým okruhem, hodnota 0 vyjadřuje 0% soulad s tematickým okruhem) [1]

Základní tematické okruhy	5	4	3	2	1	0
Bezpečnostní politika státu				X		
Metodologie posuzování rizik				X		
Hospodářská opatření pro krizové stavy					X	
Bezpečnostní hrozby vojenského a nevojenského charakteru,			X			
Vedení operací vojenského a nevojenského charakteru,					X	
Řízení bezpečnosti ve veřejném a soukromém sektoru,	X					
Krizové řízení,		X				
Právní systém České republiky v oblasti bezpečnosti,				X		
Ochrana kritické infrastruktury,		X				
Ochrana obyvatelstva,				X		
Kybernetická bezpečnost,		X				
Aplikovaná informatika pro bezpečnostní sbory,	X					
Informační a komunikační systémy pro podporu krizového řízení,		X				
Ochrana ekonomiky,						X
Vnitřní bezpečnost a veřejný pořádek,		X				
Civilní nouzová připravenost EU a NATO,						X
Prevence závažných havárií,			X			
Integrovaný záchranný systém,			X			
Požární ochrana,				X		
Preventivně výchovná činnost v oblasti obrany a ochrany obyvatelstva,					X	
Kriminalistika a forenzní disciplíny.		X				

3. SOULAD STUDIJNÍHO PROGRAMU BEZPEČNOSTNÍ TECHNOLOGIE, SYSTÉMY A MANAGEMENT S RELEVANTNÍMI PROFESEMI PRO OBLAST VZDĚLÁVÁNÍ BEZPEČNOSTNÍ OBORY

Následující tabulka uvádí relevantní charakteristické profese, které jsou u předkládaného studijního programu Bezpečnostní technologie, systémy a management v plném nebo částečném souladu s Nařízením Vlády č. 275/2016 Sb., o oblastech vzdělávání ve vysokém školství [4].

Tabulka 3: Soulad studijního programu Bezpečnostní technologie, systémy a management s relevantními profesemi pro oblast vzdělávání Bezpečnostní obory (hodnota 5 odpovídá 100% souladu s relevantními profesemi, hodnota 0 vyjadřuje 0% soulad s relevantní profesí) [1]

Relevantní charakteristické profese	Bezpečnostní technologie, systémy a management,	
	Specializace: Bezpečnostní technologie	Specializace: Bezpečnostní management
Osoba odborně způsobilá pro hodnocení vlastností zdrojů ionizujícího záření řízením a vykonáváním zkoušek	0	0
Osoba odborně způsobilá pro nakládání se zdroji ionizujícího záření	0	0
Osoba odborně způsobilá pro požární ochranu a technicko- organizační činnosti v oblasti požární ochrany	1	1
Autorizovaný inženýr	1	1
Autorizovaný technik	3	1
Osoba odborně způsobilá k zajišťování úkolů v prevenci rizik v oblasti bezpečnosti a ochrany zdraví při práci	3	4
Osoba odborně způsobilá pro zpracovávání hodnocení rizika,	5	5
Osoba odborně způsobilá pro nakládání s vysoce nebezpečnými látkami zneužitelnými k porušování zákazu chemických zbraní	2	2
Osoba odborně způsobilá pro poskytování technických služeb k ochraně majetku a osob	5	5
Osoba odborně způsobilá pro ostrahu majetku a osob	5	5
Bezpečnostní technik	4	4
Osoba odborně způsobilá pro nákup a prodej, půjčování, vývoj, výrobu, opravy, úpravy, uschovávání, skladování, přepravu, znehodnocování a ničení bezpečnostního materiálu	1	1
Osoba odborně způsobilá pro hodnocení rizik ukládání odpadů nebezpečných vlastností	3	3

Koordinátor bezpečnosti a ochrany zdraví na staveništi	1	2
Profesionální hasič	0	0
Osoba odborně způsobilá pro zajišťování úkolů v prevenci rizik v oblasti bezpečnosti a ochrany zdraví při práci	1	3

ZÁVER

Závěrem lze konstatovat, že studijní program „Bezpečnostní technologie, systémy a management“ je z hlediska vzdělávacího zaměření v souladu s Dlouhodobým záměrem vzdělávací a vědecké, výzkumné, vývojové a inovační, umělecké a další tvůrčí činnosti Univerzity Tomáše Bati ve Zlíně na období 2016–2020 (dále jen „Dlouhodobý záměr UTB ve Zlíně“) a její součástí „Plánem realizace Strategického záměru vzdělávací a tvůrčí činnosti Univerzity Tomáše Bati ve Zlíně pro rok 2018“ a také s „Dlouhodobým záměrem vzdělávací a vědecké, výzkumné, vývojové a inovační a další tvůrčí činnosti Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně na období 2016–2020“ (dále jen „Dlouhodobý záměr FAI“) a její součástí Plánem realizace Strategického záměru vzdělávací a tvůrčí činnosti Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně pro rok 2018. Zaměření a orientace předloženého studijního programu je také v souladu se „Statutem Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně“[7], v němž jsou v článcích 2 a 3 vymezeny vědní disciplíny zaměřené na informační technologie, bezpečnostní technologie, řídicí a automatizační techniku a robotické systémy. Předkládaný návrh studijního programu navazuje na dlouhodobou vědeckou, výzkumnou a vývojovou práci akademických pracovníků Fakulty aplikované informatiky a v souladu se strategií Univerzity Tomáše. Jak již bylo konstatováno, zmiňovaný program je v souladu s dokumentem vydaného Ministerstvem vnitra s názvem „Požadavky na studijní programy vysokých škol z oblasti vzdělávání „Bezpečnostní obory“ se zaměřením na ochranu obyvatelstva a krizové řízení“ [6]. Předmětný soulad je prezentovaný tabulkami 1 až 3.

LITERATÚRA

[1] UTB ve Zlíně, Fakulta aplikované informatiky, *Žádost o akreditaci magisterského studijního programu „Bezpečnostní technologie, systémy a management“,* Zlín, 2019.

[2] UTB ve Zlíně, *Dlouhodobý záměr vzdělávací a vědecké, výzkumné, vývojové a inovační, umělecké a další tvůrčí činnosti Univerzity Tomáše Bati ve Zlíně na období 2016–2020,* Zlín, 2015.

[3] ČR, *Národní kvalifikační rámec terciárního vzdělávání,* Ministerstvo školství, mládeže a tělovýchovy ČR, Praha, ISBN978-80-254-8569-9

[4] ČR, Nařízením Vlády č. 275/2016 Sb., o oblastech vzdělávání ve vysokém školství. 2016.

[5] UTB ve Zlíně, Fakulta aplikované informatiky, *Dlouhodobý záměr vzdělávací a vědecké, výzkumné, vývojové a inovační a další tvůrčí činnosti Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně na období 2016–2020*, Zlín, 2015

[6] *MV ČR, Metodika pro tvorbu studijních programů vysokých škol v oblasti bezpečnosti České republiky v působnosti Ministerstva vnitra,* Praha, *2020.*

[7] *UTB ve Zlíně, Fakulta aplikované informatiky, Statut Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně. Zlín, 2018*

ROZBOR KAMEROVÝCH SYSTÉMOV SLÚŽIACICH NA OCHRANU OBJEKTU

Zuzana Sochuľáková[12], Ján Šiňák[13]

ABSTRAKT

V úvode článku sa nachádza bližšia špecifikácia kamerových systémov, ich funkcia, základné delenie a správne používanie z pohľadu GDPR. Jadro článku tvorí podrobný popis jednotlivých druhov kamier a porovnanie parametrov v analógových, IP kamerách a hybridných kamerových systémoch. V závere sú zhrnuté výsledky z porovnávania a bližšie odporúčania na zavedenie jednotlivých kamerových systémov. Z článku sa dá zistiť kedy je vhodná inštalácia analógových kamier a kedy je potrebné použiť IP kamery. Záver obsahuje aj rozdiely medzi interiérovými a exteriérovými kamerami a odporúčania, kedy treba exteriérové kamery použiť v interiéri.

Kľúčové slová: kamerové systémy, IP kamery, analógové kamery, hybridné kamery, ochrana objektu

ABSTRACT

The introduction of the article contains a more detailed specification of camera systems, their function, basic division and proper use from the point of view of GDPR. The core of the article is a detailed description of individual types of cameras and a comparison of parameters in analog, IP cameras and hybrid camera systems. In the end, the results of the comparison and more detailed recommendations for the implementation of individual camera systems are summarized. From the article it is possible to find out when the installation of analog cameras is suitable and when it is necessary to use IP cameras. The conclusion also contains the differences between indoor and outdoor cameras and recommendations on when outdoor cameras should be used indoors.

[12] Ing. Zuzana Sochuľáková, Vysoká škola bezpečnostného manažérstva v Košiciach, Košťová 1, 04001, Slovensko, +421918472050, zuzana.sochulakova@vsbm.sk

[13] Ing. Ján Šiňák, MBA, Vysoká škola bezpečnostného manažérstva v Košiciach, Košťová 1, 01001, Slovensko, +4915141300373, sinak@centrum.sk

Key words: camera systems, IP cameras, analog cameras, hybrid cameras, object protection

ÚVOD

Kamerové systémy sú systémy, ktoré slúžia predovšetkým ako prevencia pred páchaním kriminálnej činnosti a monitorovanie daného objektu s možnosťou archivácie záznamov pre neskoršiu rekonštrukciu. Hlavnou úlohou kamerových systémov je zabezpečiť nepretržité monitorovanie a zaznamenávanie situácie v stráženom priestore v príslušnom monitorovacom centre a z pohľadu kriminality majú dôležitú úlohu pri identifikovaní páchateľa, prostredníctvom kamerového záznamu, prípadne môžu odradiť potencionálneho zlodeja od jeho protiprávneho konania. Kamerové systémy sa taktiež využívajú na monitorovanie verejných priestorov, objektov, stavieb, lokalít, vo firmách za účelom kontroly pracoviska, ale aj z dôvodu vzdialeného dohľadu nad výrobnými procesmi. V neposlednom rade majú kamerové systémy využitie aj v cestnej premávke, za účelom sledovania dopravných situácií.

Kamerové systémy umožňujú sledovanie stráženého priestoru v reálnom čase, zabezpečujú nepretržitý záznam obrazu a následne prezeranie záznamov a taktiež dokážu verifikovať príčinu požiaru.

Dôležitou skutočnosťou je fakt, že prostredníctvom prevádzkovania kamerových systémov sa zasahuje do práv aj iných osôb a preto je potrebné aby boli kamerové systémy nainštalované v súlade so zákonom. Usmernenie pre prevádzkovateľov kamerových systémov bližšie pojednáva Usmernenie 3/2019 o spracúvaní osobných údajov prostredníctvom kamerových zariadení. [1].

4. OCHRANA OBJEKTU

Kriminalita je v súčasnej dobe stále rozširujúcim sa a narastajúcim problémom, ktorým sa celý svet zaoberá. Objavujú sa neustále nové hrozby, na ktoré je treba pohotovo reagovať a preto otázka bezpečnosti majetku, osôb a iných chránených záujmov vystupuje čoraz viac do popredia. Obava o bezpečnosť sa zvyšuje aj v prípade, keď prostredie v ktorom žijeme nie je dostatočne chránené. V dobe plnej vandalizmu, násilia, krádeží je dôležité zaoberať sa zabezpečením súkromného majetku.

Bezpečnosť je stav, v ktorom je zachovaný mier a bezpečnosť štátu, jeho demokratický poriadok a zvrchovanosť, územná celistvosť a nedotknuteľnosť hraníc štátu, základné práva a slobody a v ktorom sú chránené životy a zdravie osôb, majetok a životné prostredie. [2]

Vo všeobecnosti je pojem bezpečnosť definovaný ako stav, bez reálnej hrozby nebezpečenstva, v ktorom sú minimalizované alebo odstránené riziká a z nich

vyplývajúce ohrozenia. Bezpečnosť predstavuje súhrn bezpečnostných opatrení na zaručenie bezpečnosti objektov.

Objekt predstavuje osobu, skupinu osôb, budovy, stavby alebo umelecké predmety.

Vo všeobecnosti môžeme objekty rozdeliť do 3 skupín:

- *Osoba ako objekt – osoba, skupiny osôb*
- *Objekt statický – stavby, areál s materiálom*
- *Objekt mobilný – umelecké predmety* [3]

Pod pojmom ochrana objektu sa predstavuje celok opatrení, ktoré sú potrebné na zníženie, alebo celkové odvrátenie nebezpečenstva, ktoré hrozí chránenému objektu. Prostredníctvom dostupných metód, je základným cieľom ochrany zamedziť, alebo z časti odstrániť rizikové vplyvy ohrozujúce chránený záujem. Dá sa tak povedať, že základným prvkom ochrany je prevencia. [3]

4.1. GDPR A KAMEROVÉ SYSTÉMY

Uhol pohľadu na monitorovanie z hľadiska ochrany osobných údajov závisí od účelu monitorovania. Najčastejšie ide o monitorovanie zamestnancov za účelom bezpečnosti a ochrany zdravia pri práci alebo monitorovanie objektu za účelom vyššieho zabezpečenia ochrany majetku proti krádežiam alebo vandalizmom.

Monitorovanie zamestnancov na pracovisku

Zamestnávateľ má právo kontrolovať pracovnú činnosť svojich zamestnancov za účelom bezpečnosti a ochrany zdravia pri práci, prípadne za účelom kontroly dodržiavania stanovených pravidiel zamestnávateľa. Zamestnávateľ však musí rešpektovať právo na ochranu súkromia zamestnanca a nesmie kamerový systém inštalovať v priestoroch, kde by toto súkromie bolo narušené (Napríklad šatne, toalety, oddychové miestnosti a podobne) [11]

Monitorovanie za účelom ochrany majetku

Prevádzkovateľ si musí splniť informačnú povinnosť voči dotknutým osobám a to zverejnením informácií pri vstupe do budovy alebo na webe spoločnosti. Monitorovaný priestor musí byť označený viditeľným piktogramom – napríklad na vchodových dverách. Prevádzkovateľ musí poučiť oprávnené osoby, ktoré môžu manipulovať so záznamom alebo sledovať záznam a zamedzí prístup k záznamu nepovolaným osobám. Po splnení účelu, na ktorý bol záznam uchovávaný, alebo po uplynutí doby, ktorú si prevádzkovateľ interne určil, záznam zlikviduje. [11]

5. DRUHY KAMEROVÝCH SYSTÉMOV

Kamerové systémy sú v súčasnosti veľmi žiadanými ochrannými prostriedkami. Využívajú sa na monitorovanie objektu a následného uchovávania obrazového a zvukového záznamu. Kamerové systémy chránia bezpečnosť osôb, zvyšujú

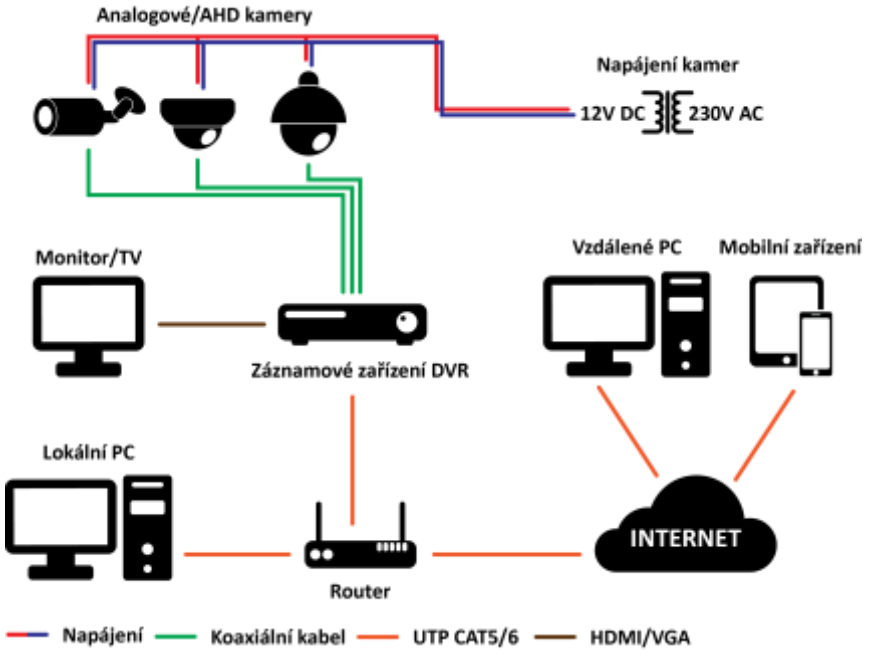
efektivitu práce zamestnancov, chránia pred krádežami a vlámaniami a v neposlednom rade dokážu spustiť alarm v prípade vlámania.
Kamerové systémy rozdeľujeme do 4 základných skupín:

- *Analógové kamerové systémy*
- *IP kamerové systémy*
- *Hybridné kamerové systémy [4]*

5.1. ANALÓGOVÉ KAMEROVÉ SYSTÉMY

Analógové systémy predstavujú najstaršiu a najrozšírenejšiu technológiu kamerových systémov. Hlavnými znakmi analógových kamerových systémov sú predovšetkým nízke obstarávacie náklady a jednoduchá inštalácia. Táto technológia a môže zaradiť medzi spoľahlivú, ktorá zvládne prenos analógového signálu po koaxiálnom kábli až do 500 metrov. Analógové kamerové systémy sa v súčasnosti skladajú z analógových kamier, prenosných prostriedkov, záznamových zariadení a zobrazovacích zariadení Medzi výhody analógových kamerových systémov patria jednoznačne nízke obstarávacie náklady, jednoduchá infraštruktúra, nízke nároky na kapacitu úložiska záznamu, prenos signálu až do 500 metrov a v neposlednom rade je to obraz v HD rozlíšení, čo sa hlavne odzrkadľuje na kvalite obrazu pri zlých svetelných podmienkach. K nevýhodám patrí nízke rozlíšenie obrazu a snímaciu frekvenciu, obmedzenú vzdialenosť prenosu signálu, absenciu audio prenosu a iných pokročilých funkcií video analýzy, nízku úroveň zabezpečenia signálu a teda aj samotný analógový signál. [5,6]

Uplatnenie analógových kamerových systémov je predovšetkým v aplikáciách, kde sa nepožaduje vysoká kvalita záznamu, konkrétne môžeme hovoriť o monitoringu rozsiahlych areálov, detekciu vniknutia nepovolaných osôb do stráženého priestoru, alebo snímanie davu na kultúrnych, športových alebo iných podujatiach. [6]



Obr.. 1 Schéma zapojenia analógových kamerových systémov [6].

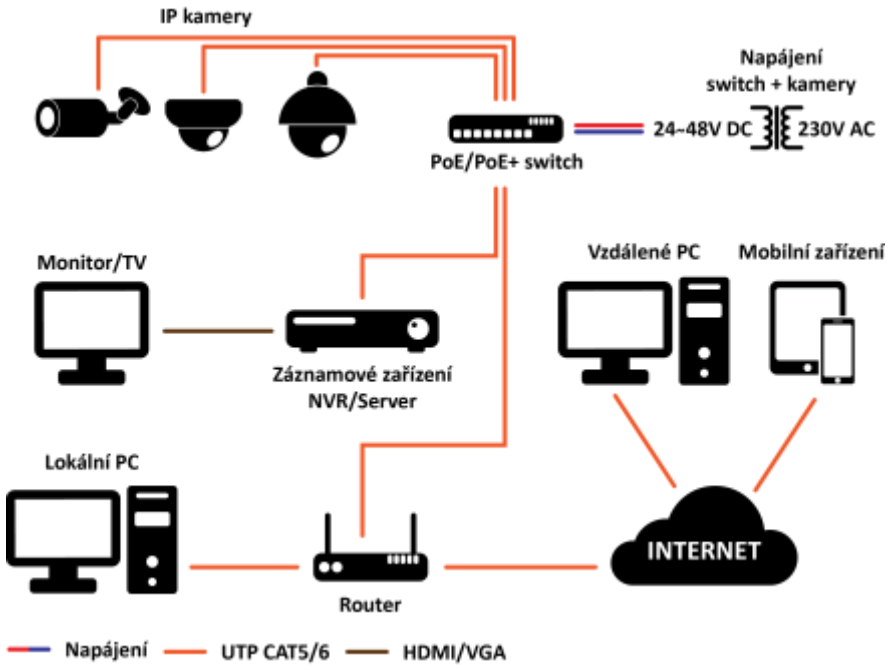
5.2. IP KAMERY

IP kamerové systémy sa od ostatných kamerových systémov líšia predovšetkým spracovaním vstupného signálu z kamier. Iné kamerové systémy využívajú predovšetkým nespracovaný analógový signál, IP kamery obsahujú vstavané obvody, ktoré zaisťujú digitalizáciu a komprimáciu vstupného signálu a následne jeho prenos do dátovej siete. IP kamery sa vyznačujú vysokým rozlíšením Megapixelov a pokročilými funkciami video analýzy. Hlavnou funkciou je napríklad inteligentná detekcia pohybu alebo možnosť čítania ŠPZ na vozidlách a mnoho iného. Ďalšou významnou črtou je „Technológia progresívneho skenovania obrazov“, čo v preklade znamená, že zabraňuje rozmazávaniu obrazu pri rýchlo pohybujúcich sa predmetoch alebo ľuďoch. K pozretiu záznamu videa z IP kamier stačí bežný počítač, ktorý ma špeciálny software alebo sieťový rekordér, označovaný ako NVR.

Výhodou IP kamerových systémov je jednoznačne vysoké rozlíšenie a kvalita obrazu, vyššia snímkovacia frekvencia (fps) ako u iných kamier, progresívne skenovanie obrazu, pokročilé funkcie video analýzy, obojsmerný audio prenos, vyššia úroveň zabezpečenia a využívanie dátovej kabeláže – napájanie, ovládania, komunikácia.

K nevýhodám patrí určite citlivosť, ktorá je nižšia ako napríklad u analógových kamier, má vysoké nároky na dátovú sieť a dátové úložisko, cena je taktiež vyššia ako u iných kamerových systémov a pre pozretie video záznamu je nutnosť použiť sieťové záznamové zariadenie alebo počítač. [6]

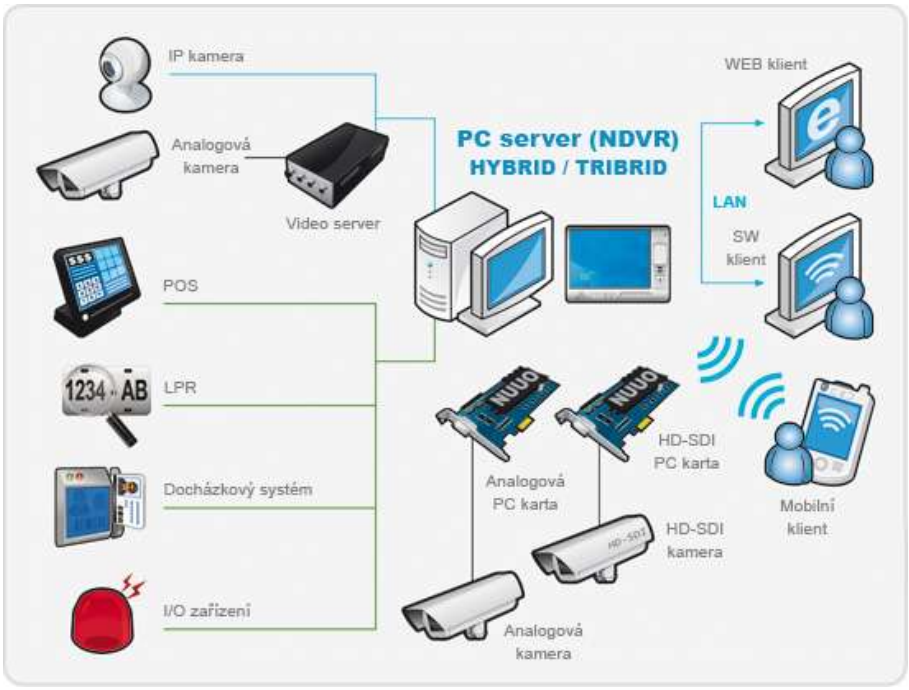
Využívanie IP kamerových systémov je potrebné najmä v prípadoch, kedy je dôležité vysoké rozlíšenie video záznamu, predovšetkým za účelom identifikácie osôb, kontroly vstupov a výstupov do areálov a podobne.



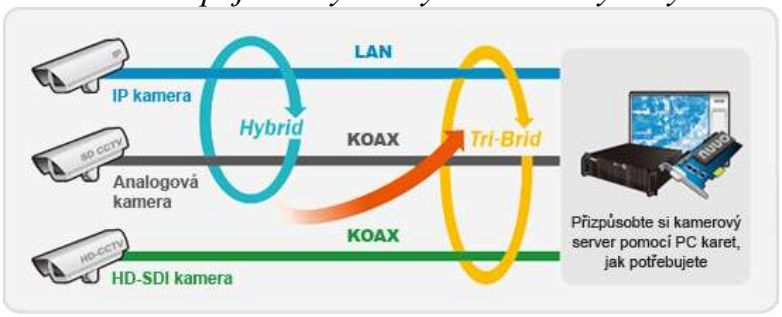
Obr.. 2 Schéma zapojenia IP kamier [6].

5.3. HYBRIDNÉ KAMEROVÉ SYSTÉMY

Hybridné kamerové systémy predstavujú kombináciu analógových kamerových systémov a IP kamier. Hlavnou úlohou hybridných kamier je, že sa dajú kombinovať už nainštalované analógové systémy s možnosťou rozšíriť kamerový systém zavedením IP kamery.



Obr.. 3 Schéma zapojenia hybridných kamerových systémov [7].



Obr.. 4 Schéma fungovania hybridných kamerových systémov [7].

6. POROVNANIE ANALÓGOVÝCH KAMIER A IP KAMIER

VLASTNOSŤ	ANALÓGOVÉ KAMERY	IP KAMERY
Rozlíšenie kamier	0,4MPx	1,3MPx ;2MPx ;5MPx a viac
Snímková frekvencia	25 FPS	6-60 FPS
Inteligentná	Nie	Áno

analýza		
Možnosť sledovať cez internet	Áno	Áno
Nároky na diskovú kapacitu	Nižšia Jedna kamera pri plnej snímkovej frekvencii spotrebuje cca 20GB denne	Vyššia Jedna kamera pri rozlíšení 2MPx a plnej snímkovej frekvencii spotrebuje cca 100GB denne
Kabeláž	Pomocou koaxiálneho káblu. Každá kamera musí byť napojená samostatne + 1 prívod na napájanie.	Štandardný UTP/FTP kábel. Pomocou 1 kábla sa môže pripojiť niekoľko kamier naraz.
Prístup a funkcionalita	Ide o uzavretý televízny okruh, čo znamená nemožnosť vzdialenej konfigurácie kamier cez internet, resp. je možná konfigurácia len na obmedzené funkcie	Možnosť vzdialenej konfigurácie a sledovanie live prenosu cez webový prehliadač
Flexibilita systému	Každá kamera potrebuje vlastný kábel + kábel na napájanie, čím je rozšírenie celého systému veľmi limitované.	Jednoduché pridávanie ďalších kamier. Pripojenie na už existujúci UTP/FTP kábel.
Cena	Nižšia	Vyššia

Tabuľka 1.Porovnanie vlastností analógových kamier a IP kamier [9].

Porovnanie kvality obrazu

Rozlíšenie obrazu určuje koľkými obrazovými bodmi je tvorený výsledný obraz, najčastejšie sa udáva v MPix (Mega – pixel). Vyššie rozlíšenie umožňuje ostrejší obraz, na ktorom dokážeme zachytiť viac detailov.

D1 je označenie pre kamery, ktoré majú rozlíšenie do 1 MPix, patria sem všetky analógové kamery a niektoré IP kamery. Tieto kamery sa využívajú najčastejšie len ako prehľadové kamery, kde nie sú potrebné detaily. HD je skratka pre vysoké rozlíšenie, ktoré obsahuje 1280x720 pixelov. Full HD je momentálne najpoužívanejšie rozlíšenie u IP kamier, toto rozlíšenie obsahuje 1920x1080 pixelov. Kamery s týmto rozlíšením sa využívajú na monitorovanie priestoru, kde je nutné sledovať detaily a to aj detaily pomocou digitálneho priblíženia.

Na obrázku sa dajú vidieť tri rôzne rozlíšenia kamier a to D1, HD a Full HD. Hlavný a viditeľný rozdiel je predovšetkým v kvalite, ostrosti a veľkosti obrazu. Pri rozlíšení D1 sa dajú vidieť len základné črty, pri HD je obraz kvalitnejší a dokáže

ostrejšie zachytiť niektoré detaily a Full HD obraz dokáže celkom ostro zachytiť celý obraz vrátane najmenších číslic na tabuľke.

Dôležitým faktorom pri výbere kamerového systému nie je len vysoké rozlíšenie ale je to predovšetkým aj počet kamier a ich následné umiestnenie tak, aby snímali čo najväčšiu plochu chráneného objektu.

Obr.. 5 Porovnanie kvality obrazu v rôznych rozlíšeniach [8].

U analógových kamerových systémoch je v súčasnosti dosiahnuté maximálne možné rozlíšenie obrazu a to 0,4 MPix. Naopak IP kamery dokážu rozlíšenie obrazu stále zvyšovať, IP kamera s najkvalitnejším obrazom má rozlíšenie okolo 10MPix, no väčšinou tieto kamery dosahujú rozlíšenie 1,3-2 MPix. [10]

Na obrázku je vidno porovnanie obrazu snímaného objektu pomocou dvoch rôznych kamerových systémov. Je viditeľné, že IP kamery majú kvalitnejší a ostrejší obraz, kde sa dajú zachytiť aj detaily.

Obr.6 Porovnanie kvality obrazu u analógových kamier a IP kamier [8].

ZÁVER

Využívanie kamerových systémov je v súčasnosti veľmi obľúbený bezpečnostný prvok. Pomocou kamerových systémov sa dá sledovať daný objekt s možnosťou uchovávania obrazových a zvukových záznamov. Medzi funkcie modernejších kamerových systémov patrí aj spustenie alarmu v prípade vlámania.
V článku sú porovnávané dva druhy kamerových systémov a to analógové kamerové systémy a IP kamery. Oba druhy kamerových systémov majú svoje výhody a nevýhody, ktoré boli bližšie popísane v jadre článku. Pri porovnávaní parametrov jednotlivých druhov, vznikol záver, že aj napriek tomu, že analógové kamery majú výrazne nižšie a menej kvalitné rozlíšenie obrazu, svojimi vlastnosťami sú vhodné do priestorov, kde nie je potrebné sledovať detaily a rovnako nie je potrebné vynaložiť vysoké finančné možnosti na kúpu tohto kamerového systému. Spravidla sa používajú predovšetkým len ako prehľadné kamery. IP kamery a hybridné kamery so svojou HD a Full HD kvalitou obrazu nájdu uplatnenie všade tam, kde je veľmi dôležité sledovanie detailov. Tieto kamery dokážu z rovnakej vzdialenosti zachytiť niekoľko násobne vyšší počet detailov ako analógové kamery a to vrátane detailov pomocou digitálneho priblíženia. Treba brať do úvahy aj fakt, že cena IP kamier alebo hybridných kamerových systémov je výrazne vyššia ako u analógových, zato samotná inštalácia daného systému je o niečo jednoduchšia, nakoľko pomocou jedného kábla sa IP kamier môže pripojiť viac na rozdiel od analógových, kde každá kamera potrebuje vlastný kábel + kábel na napájanie.
Pred samotnou inštaláciou kamerového systému je potrebné poznať priestor, ktorý chceme monitorovať, vybrať vhodne miesto umiestnenia a správny uhol, tak aby nám kamera pokryla celý požadovaný priestor. Pri výbere vhodného kamerového systému sa dajú vybrať buď interiérové alebo exteriérové kamery. Zásadný rozdiel medzi nimi je v tom, že interiérové kamery sa používajú len v interiéroch a sú porovnateľne menšie ako exteriérové kamery. Exteriérové kamery sa môžu používať aj v interiéroch aj v exteriéroch. V interiéroch sa externé kamery využívajú hlavne v prípade, že je potrebné monitorovať priestor, v ktorom je nadmerná vlhkosť, prach alebo teplota môže skĺznuť pod -10°C. Kamerové systémy určené do exteriérov sú odolné voči dažďu, mrazu, iným poveternostným podmienkam, taktiež voči prachu, ale aj proti poškodeniu hrubou silou. Pri výbere kamier do vonkajšieho prostredia si treba všímať udávaný stupeň ochrany krytom (IP kód). Tento IP kód by mal mať stupeň krytia minimálne IP65.

Je dôležité vybrať si správny kamerový systém do daného prostredia, aj napriek možno vyššej cene. Zabezpečí to tak kvalitné monitorovanie daného priestoru, primeranú odolnosť a dá sa tak vyhnúť vysokým poplatkom za následný servis, náklady za výmenu, prípadne problémovú reklamáciu.

LITERATÚRA

[1] JELINEK, A., Za Európsky výbor pre ochranu osobných údajov. Usmernenie 3/2019 o spracúvaní osobných údajov prostredníctvom kamerových zariadení

[2] Ústavný zákon č. 227/2002 Z.z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu

[3] SEDLAK, V., LOŠONCZI, P., KISS, I., Bezpečnostné informačné technológie, 2008, ISBN: 9788089282265

[4] MOREZ GROUP a.s., CCTV – Zabezpečovacie kamerové systémy, [Online] [Cit 24-3-2021], dostupné na internete: https://www.morez.sk/?cmd=produkty/cctv_zabezpecovacie_kamerove_systemy & =&

[5] SECURIA PRO, Analógový alebo digitálny (IP) systém – aké sú rozdiely?, [Online] [Cit 28-3-2021], dostupné na internete: https://www.securiapro.sk/clanok/porovnanie-kamerovych-systemov/

[6] Veria by design, Analógové kamerové systémy, [Online] [Cit 30-3-2021], dostupné na internete: http://www.veria.eu/portfolio-produktu/kamerove-systemy

[7] NUUO, Inteligentní řešení kamerového systému, NDVR HYBRIDNÍ a TRIBRIDNÍ systém, [Online] [Cit 30-3-2021], dostupné na internete: http://www.nuuo.cz/produkty_tribrid.php

[8] TSS GROUP, Prečo si vybrať HDCVI a aké sú výhody inštalácie? [Online] [Cit 01-4-2021], dostupné na internete: https://www.tssgroup.sk/aktuality/zaujimavosti/preco-si-vybrat-hdcvi-a-ake-su-vyhody-instalacie

[9] ELMECH, IP kamery vs. Analógové, [Online] [Cit 01-4-2021], dostupné na internete: https://elmech.sk/clanok/ip-kamery-vs-anal%C3%B3gov%C3%A9

[10] Media Leaders s.r.o., IP vs. analógové kamery a základné pojmy, [Online] [Cit 01-4-2021], dostupné na internete: https://www.bezpecnostnekamery.sk/clanky/ip-vs-analogove-kamery-a-zakladne-pojmy

ILAVSKA Marcela, *AKO GDPR NAHLIADA NA POUŽÍVANIE KAMEROVÝCH SYSTÉMOV,* [Online] [Cit 16-4-2021], dostupné na internete: https://www.isecure.sk/sk/aktuality/monitorovanie-kamerovym-systemom-z-pohladu-gdpr.html?fbclid=IwAR2uZt9zgvvRSVg5WlJbByV404boGLOqP_C_e0Jd1eRsNXMUzE4tvEnTXBA

PRÁVNE ASPEKTY MONITOROVANIA A TRASOVANIA POHYBU OSÔB MODERNÝMI TECHNOLÓGIAMI V ZDRAVOTNÍCKYCH ZARIADENIACH

Tomáš Loveček[14], Marián Magdolen[15], Bohuš Leitner[16]

ABSTRAKT

Rýchly technologický rozvoj a globalizácia so sebou priniesli nové výzvy v oblasti ochrany osobných údajov. Rozsah získavania a zdieľania a osobných údajov sa výrazne zväčšil. Moderné technológie umožňujú súkromným spoločnostiam a orgánom verejnej moci pri výkone ich činností využívať osobné údaje v doteraz bezprecedentnom rozsahu. Príkladom je aj monitorovanie a trasovanie osôb v priestoroch objektov zdravotníckych zariadení (napr. nemocnice, polikliniky, ambulancie) s využitím moderných technológií (napr. RFID, Bluetooth, resp. Ibeacon). Článok prepája svet moderných technológií a právne požiadavky na ochranu osôb, ktoré môžu byť týmito technológiami, za účelom ochrany ich života a zdravia, monitorované a trasované.

Kľúčové slová:
právne aspekty trasovania pohybu osôb, ochrana osobných údajov, GDPR, informačný systém, moderné technológie

ABSTRACT

Fast technological development and globalization have brought new challenges in the field of personal data protection. The scope of collection and sharing of personal data has increased significantly. Modern technologies enable private companies and public authorities to use personal data to an unprecedented extent in the performance of their activities. An example is the monitoring and tracing of people in the premises of medical facilities (eg hospitals, clinics) using modern technologies (eg RFID, Bluetooth, or Ibeacon). The article connects the world of modern technologies and the

[14] prof. Ing. Tomáš Loveček, PhD., Žilinská univerzita v Žilina, Fakulta bezpečnostného inžinierstva, Katedra bezpečnostného manažmentu, Univerzitná 8215/1, 010 26 Žilina, Slovakia, tomas.lovecek@uniza.sk

[15] Mgr. Marián Magdolen, PhD., Žilinská univerzita v Žilina, Fakulta bezpečnostného inžinierstva, Katedra bezpečnostného manažmentu, Univerzitná 8215/1, 010 26 Žilina, Slovakia, marian.magdolen@uniza.sk

[16] doc. Ing. Bohuš Leitner, PhD., Žilinská univerzita v Žilina, Fakulta bezpečnostného inžinierstva, Katedra požiarneho inžinierstva, Univerzitná 8215/1, 010 26 Žilina, Slovakia, bohus.leitner@uniza.sk

legal requirements for the protection of persons who may be monitored and traced by these technologies in order to protect their lives and health.

Key words:
legal aspects of monitoring the movement of persons, personal data protection, GDPR, information system, modern technologies

1 DEFINOVANIA PRÁVNEHO RÁMCA

Rýchly technologický rozvoj a globalizácia so sebou priniesli nové výzvy v oblasti ochrany osobných údajov. Rozsah získavania a zdieľania a osobných údajov sa výrazne zväčšil. Technológia umožňuje súkromným spoločnostiam a orgánom verejnej moci pri výkone ich činností využívať osobné údaje v doteraz bezprecedentnom rozsahu. (GDPR, Recital 6)

Pri využití technologických nástrojov, ktoré pre svoje fungovanie budú okrem všeobecných údajov využívať napríklad aj údaje, ktoré svojou povahou zasahujú do súkromia fyzických osôb alebo údaje, pomocou ktorých je možné fyzické osoby identifikovať priamo alebo nepriamo musíme takéto spracúvanie posudzovať s ohľadom na pravidlá spracúvania osobných údajov. Právny rámec pre pravidlá ochrany osobných údajov vytvára v Európskej únii Všeobecné nariadenie o ochrane údajov, Nariadenie Európskeho parlamentu a rady 2016/679 o ochrane ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“ alebo „GDPR“). Členské štáty môžu v určitých špecifických situáciách pravidlá GDPR ďalej konkretizovať a upravovať podľa národných požiadaviek. Vhodným zdrojom ako byť v kontakte s aktuálnym ponímaním ochrany osobných údajov je aj sledovanie metodických usmernení národných dozorových orgánov alebo Európskeho výboru pre ochranu údajov.

2 DEFINÍCIE

Podľa Krátkeho slovníka slovenského jazyka slovo **monitorovanie** znamená pozorovať a zaznamenávať, zatiaľ čo **trasovať** znamená vytyčovať trasu. Preto pod monitorovaním a trasovaním pohybu osôb, môžeme chápať pozorovanie a zaznamenávanie trasy, ktorú človek prešiel za určitý čas v danom priestore.

Podľa Článku 4 Nariadenia GDPR osobné údaje sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby. Pričom identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

Lokalizačné údaje sú všetky údaje spracúvané v elektronickej komunikačnej sieti alebo prostredníctvom elektronickej komunikačnej služby, ktoré udávajú geografickú polohu koncového zariadenia používateľa verejne dostupnej elektronickej komunikačnej služby, ako aj údaje z iných potenciálnych zdrojov týkajúce sa (Usmernenie 4/2020, Príloha):

a) zemepisnej šírky, zemepisnej dĺžky alebo nadmorskej výšky koncového zariadenia,
b) smeru pohybu používateľa alebo,
c) času zaznamenania informácií o polohe.

Spracúvanie osobných údajov je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.

Elektronická komunikačná sieť je sieť, ktorú tvoria prenosové systémy, ktoré môžu, ale nemusia byť založené na trvalej infraštruktúre alebo centralizovanej správe kapacity, prípadne prepájacie alebo smerovacie zariadenia a iné prostriedky, vrátane neaktívnych prvkov siete, ktoré umožňujú prenos signálov po vedení, rádiovými vlnami, optickými alebo inými elektromagnetickými prostriedkami vrátane družicových sietí, pevných sietí s prepájaním okruhov a s prepájaním paketov vrátane internetu, mobilných sietí, elektrických vedení určených na prenos a distribúciu elektriny v rozsahu, v ktorom sa používajú na prenos signálov, sietí používaných na rozhlasové a televízne vysielanie a sietí káblovej televízie bez ohľadu na druh prenášaných informácií. (Zákon č. 452/2021 Z.z., §2).

V prípade monitorovania a trasovania osôb v stavebne ohraničenom priestore (napr. stavebný objekt zdravotníckeho zariadenia) modernými technológiami (napr. RFID, Bluetooth, resp. Ibeacon), je možné hovoriť o spracúvaní osobných údajov v rámci PAN, resp. LAN sietí.

Podľa §7 zákona č. 578/2004 Z.z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov, **zdravotnícke zariadenie** je prevádzkový útvar zriadený na poskytovanie zdravotnej starostlivosti a služieb súvisiacich s poskytovaním zdravotnej starostlivosti. Medzi zdravotnícke zariadenie patrí napríklad ambulancia, poliklinika, nemocnica, liečebňa, laboratória, stacionár, atď.

PAN (**Personal Area Network**) je osobná počítačová sieť, ktorá je spravidla tvorená počítačmi umiestnenými v tesnej blízkosti alebo počítačom a iným

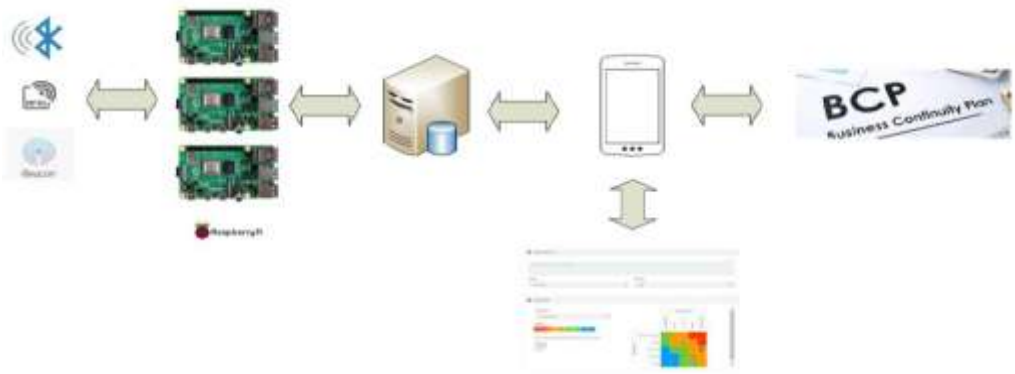
elektronickým zariadením (tlačiareň, PDA, mobilný telefón). Na prenos údajov najčastejšie používa bezdrôtové pripojenie.

LAN (**Local Area Network**) lokálna počítačová sieť je sieť, ktorá pracuje v režime neustáleho spojenia a na komunikáciu medzi počítačmi nepotrebuje nadväzovať spojenie (nepoužíva prostriedky pre diaľkový prenos údajov). (Encyklopédia poznania, 2013)

Z pohľadu spracúvania osobných údajov s využitím moderných technológií je potrebné prepojiť pojmy ako ako informačný systém, spracovateľská činnosť a spracovateľská operácia.

V Nariadení GDPR pojem **informačný systém** je definovaný ako akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe. V minulosti bol informačný systém definovaný zákonom č.122/2013 Z.z. (účinný od 15.04.2014 do 24.05.2018), ako systém, v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií, bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe (ďalej len „informačný systém“).

Informačný systém v sebe teda môže združovať viacero **spracovateľských činností**, resp. **spracovateľských operácií.** Tieto novozavedené pojmy v Nariadení GDPR bohužiaľ nemajú svoju definíciu, ktorá by jasne stanovila ich vzájomnú väzbu na informačný systém. V Nariadení GDPR je iba uvedená definícia pojmu spracúvanie, ako operácia alebo súbor operácií s osobnými údajmi. Tu možno bolo potrebné doplniť, že spracovateľská operácia je napríklad prenos, záznam alebo zobrazenie a súbor týchto operácií vytvára určitú spracovateľskú činnosť (napr. monitorovanie osôb). Potom informačný systém by bol funkčný celok, ktorý prostredníctvom technických prostriedkov, programových prostriedkov a ľudských zdrojov zabezpečoval túto spracovateľskú činnosť.



Obrázok 1: Bloková schéma informačného systému Cov-ID určeného na monitorovanie, trasovanie osôb a vyhodnotenia rizikovosti možného kontaktu

Podľa čl. 30 Nariadenia GDPR každý prevádzkovateľ a v príslušnom prípade zástupca prevádzkovateľa vedie záznamy o spracovateľských činnostiach, za ktoré je zodpovedný. Úrad na ochranu osobných údajov SR (ÚOOÚ SR) zverejnil na svojich webových stránkach vzor záznamu spracovateľských činností. Príklad spracovateľských činností súvisiacich s monitorovacími systémami je uvedený v tabuľke 1.

Tabuľka 1 Príklad spracovateľských činností prevádzkovateľa s využitím monitorovacích systémov

Účel spracúvania	**Právny základ**	**Dotknuté osoby**
Monitorovanie a kontrola zamestnancov (napr. prostredníctvom kamerového systému)	čl. 6 ods. 1 f) Nariadenia GDPR Oprávnený záujem prevádzkovateľa	- zamestnanci prevádzkovateľa - iné osoby, ktoré sa ocitnú (oprávnene alebo neoprávnene) v priestore monitorovanom kamerovým systémom
Monitorovanie verejných priestorov za účelom ochrany majetku, zdravia a odhaľovania kriminality.	čl. 6 ods. 1 f) Nariadenia GDPR Oprávnený záujem prevádzkovateľa	- zamestnanci prevádzkovateľa - klienti prevádzkovateľa - iné osoby, ktoré sa ocitnú (oprávnene alebo neoprávnene) v priestore monitorovanom kamerovým systémom
Monitorovanie priestorov banky prostredníctvom kamerového systému na účely na účely	čl. 6 ods. 1 c)	- zamestnanci prevádzkovateľa

odhaľovania trestných činov, na zisťovanie ich páchateľov a pátranie po nich, a to najmä na účely ochrany pred legalizáciou príjmov z trestnej činnosti a pred financovaním terorizmu, odhaľovania nezákonných finančných operácií, súdneho konania, trestného konania, konania o priestupkoch a dohľadu nad plnením zákonom ustanovených povinností bánk a pobočiek zahraničných bánk	Nariadenia GDPR Osobitný predpis – zákon č. 483/2001 Z.z. o bankách	- klienti prevádzkovateľa - iné osoby, ktoré sa ocitnú (oprávnene alebo neoprávnene) v priestore monitorovanom kamerovým systémom

3 PRÁVNE ASPEKTY SPRACÚVANIA OSOBNÝCH ÚDAJOV

Pri akomkoľvek spracúvaní osobných údajov je prevádzkovateľ povinný postupovať v súlade s povinnosťami definovanými vo všeobecnom nariadení o ochrane údajov. GDPR stanovuje šesť základných zásad, od ktorých je možné odvodiť väčšinu povinných krokov pre posúdenie legálnosti spracúvania. Tieto základné zásady vytvárajú logickú a komplexnú sieť otázok, ktoré musí každý prevádzkovateľ pred spracúvaním osobných údajov zodpovedať a súčasne nastavením budúceho spracúvania v súlade s týmito zásadami zosúladiť právne požiadavky s reálnou aplikáciou v praxi.

Na základe Článku 5 Nariadenia GDPR základnými zásadami sú:

a) zákonnosť, spravodlivosť a transparentnosť;
b) obmedzenie účelu;
c) minimalizácia údajov;
d) správnosť;
e) minimalizácia uchovávania;
f) integrita a dôvernosť.

V nasledujúcich podkapitolách si rozoberieme, aké otázky je si pri jednotlivých zásadách potrebné zodpovedať.

3.1 ZÁKONNOSŤ, SPRAVODLIVOSŤ, TRANSPARENTNOSŤ

Každé spracúvanie osobných údajov by malo byť zákonné a spravodlivé. Spracúvanie osobných údajov je zákonné v prípade, ak je založené na správnom právnom základe, pričom sleduje legitímny účel spracúvania. (Komentár, str. 118) Zákonnosť akéhokoľvek monitorovania, ktoré je vždy výrazným zásahom do súkromia jednotlivca, môže byť s ohľadom na účel spracúvania a typ prevádzkovateľa vykonaný len na základe jedného z určených právnych základov, stanovených v Článku 6 Nariadenia GDPR. Z posúdenia špecifického prepojenia právneho základu, prevádzkovateľa a účelu vyplynie kombinácia, ktorá je nevyhnutná pre dané spracúvanie. Príkladom vhodej kombinácie je napríklad spracúvanie osobných údajov orgánom verejnej správy na právnom základe plnenia úloh vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi (Článok 6, ods. 1 e) Nariadenia GDPR), pričom účelom by mala byť konkrétna povinnosť takéhoto orgánu stanovená

v osobitnom právnom predpise. Menej vhodným príkladom by mohlo byť napríklad monitorovanie zamestnancov na základe súhlasu, kedy by neboli dostatočné záruky a možnosť preukázania, že súhlas zamestnancov bol udelený bez nátlaku a so slobodou voľby odmietnuť dané spracúvanie (najmä s ohľadom na hierarchickú pozíciu medzi zamestnávateľom a zamestnancom).

Z pohľadu spravodlivosti je potrebné zabezpečiť spracúvanie tak, aby dotknutá osoba bola transparentne informovaná o spracúvaní osobných údajov, pričom osobitne by sa mali uviesť podmienky spracúvania najmä s ohľadom na prípadné profilovanie, obmedzenie automatizovaného spracúvania osobných údajov či možnosti uplatnenia všetkých práv dotknutej osoby.

Transparentnosť spracúvania osobných údajov spočíva v otvorenej komunikácii s dotknutými osobami, prípadne aj s dozorovým orgánom. Minimálne informácie, ktoré musí získať dotknutá osoba pred spracúvaním osobných údajov stanovuje GDPR, ale prevádzkovateľ v záujme transparentnosti môže ísť aj nad rámec povinných údajov a zverejniť aj iné podklady pre preukázanie jeho legitímnych záujmov ako nástroja ochrany a dôvery v ochranu súkromia, ktoré dodržiava. Všetky informácie, ktoré smerujú k dotknutým osobám, by mali byť v ľahko dostupnej forme, formulované zrozumiteľne, jasne a jednoducho. Medzi takýmito podkladmi by mohli byť napríklad **testy proporcionality**, **posúdenie vplyvov na ochranu osobných údajov**, **analýza rizík**, jasne definované role zainteresovaných osôb v rozsahu ich práv a povinností, spôsob a možnosť preskúmania spracúvania, odkazy na aktuálny stav poznania najmä s ohľadom na aplikované bezpečnostné a anonymizačné opatrenia a podobne. Európsky výbor na ochranu osobných údajov napríklad pri využívaní aplikácii špecificky uvádza, že: „s cieľom zabezpečiť spravodlivosť a zodpovednosť algoritmov a všeobecnejšie ich súlad s právom, algoritmy musia byť kontrolovateľné a mali by byť pravidelne skúmané nezávislými odborníkmi. S cieľom čo najširšej kontroly by sa mal zverejniť zdrojový kód aplikácie.“ (Usmernenie 4/2020, Bod 37).

3.2 OBMEDZENIE ÚČELU

Definícia účelu spracúvania je kľúčová tak pre posúdenie zákonnosti ale aj pre komunikáciu s dotknutými osobami. Pre naplnenie povinnosti určiť účel spracúvania musí prevádzkovateľ špecifikovať konkrétny, jednoznačný dôvod spracúvania. Tento účel definuje prevádzkovateľ alebo vyplýva z osobitných právnych predpisov, pokiaľ je právnym základom spracúvanie na základe osobitného zákona alebo pri výkone verejnej moci. Z konkrétneho účelu, ktorý je jasný a zrozumiteľný by mali okrem záujmu a zámeru prevádzkovateľa vyplývať aj prínosy pre dotknutú osobu.

Obmedzenie účelu stanovuje zákaz využitia získaných osobných údajov na iné účely než ten, na ktorý boli získané. Hudecová píše, že „zásada obmedzenia účelu predstavuje jednu z kľúčových zásad spracúvania osobných údajov. Je úzko spojená so zásadou zákonnosti, spravodlivosti a transparentnosti, keďže poskytuje dotknutým osobám právnu istotu, že ich osobné údaje môžu byť spracúvané iba na konkrétne určený, výslovne uvedený a legitímny účel. Zároveň predstavuje nevyhnutný

predpoklad, pre aplikáciu zásady minimalizácie údajov a minimalizácie uchovávania, a to z dôvodu, že stanovený účel spracúvania osobných údajov ovplyvňuje rozsah spracúvaných osobných údajov nevyhnutných na dosiahnutie účelu spracúvania, ako aj dobu ich uchovávania“. (Komentár, str. 122)

Hoci Nariadenie GDPR v určitých prípadoch umožňuje zlúčenie účelov, resp. využitie osobných údajov na iný účel ako boli získané, ale k tomu by mal každý prevádzkovateľ pristupovať nanajvýš opatrne. „S cieľom zistiť, či je účel ďalšieho spracúvania v súlade s účelom, na ktorý boli osobné údaje pôvodne získané, by mal prevádzkovateľ po splnení všetkých požiadaviek zákonnosti pôvodného spracúvania zohľadniť okrem iného akékoľvek prepojenie medzi týmito účelmi a účelmi zamýšľaného ďalšieho spracúvania; kontext, v ktorom sa osobné údaje získali, najmä primerané očakávania dotknutých osôb vyplývajúce z ich vzťahu k prevádzkovateľovi, pokiaľ ide o ich ďalšie použitie; povahu osobných údajov; následky zamýšľaného ďalšieho spracúvania pre dotknuté osoby; a existenciu primeraných záruk v pôvodných aj zamýšľaných operáciách ďalšieho spracúvania.“ (Recitál 50, GDPR)

3.3 MINIMALIZÁCIA ÚDAJOV

Minimalizácia údajov predstavuje povinnosť prevádzkovateľa získavať a spracúvať iba také osobné údaje, ktoré sú „primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú“. (Článok 5, ods. 1 c) Prevádzkovateľ by mal vždy vykonať dôkladnú analýzu, ktoré osobné údaje potrebuje získavať a tieto obmedziť na striktné minimum. Najmä pri získavaní lokalizačných údajov prostredníctvom moderných technológií je nevyhnutné zisťovať, či sa týmto nezískavajú aj „nesúvisiace alebo nepotrebné informácie, napríklad občiansky stav, identifikátory komunikácie, položky v adresári zariadenia, správy, záznamy hovorov, lokalizačné údaje, identifikátory zariadenia atď“. (Usmernenie 4/2020, bod 40) V prípade trasovania pohybu v zdravotníckych zariadeniach vzniká aj riziko, že určením polohy osoby bude nepriamo zisťovaný aj jej zdravotný stav alebo aspoň jeho indikácie (napríklad prostredníctvom ambulancií, ktoré navštívil, ako dlho sa tam zdržal a pod.). Pri aplikácií zásady minimalizácie údajov je vhodné použiť nástroje pre posúdenie primeranosti a proporcionality.

S ohľadom na minimalizáciu ale aj bezpečnosť osobných údajov je potrebné aby prevádzkovateľ využil nástroje špecificky navrhnutej a štandardnej ochrany osobných údajov. Európsky výbor na ochranu osobných údajov „zdôrazňuje, že pokiaľ ide opoužívanie lokalizačných údajov, malo by sa vždy uprednostniť spracúvanie anonymizovaných údajov, a nie osobných údajov.“ (Usmernenie 4/2020, bod 14) Avšak pri anonymizácii treba byť opatrný, pretože najmä pri veľkých a podrobných súboroch údajov, kde sú údaje prepojené, je anonymizácia veľmi obtiažna. „V mnohých výskumoch sa skutočne potvrdilo, že lokalizačné údaje, ktoré sa považujú za anonymizované, také v skutočnosti nemusia byť. Stopy mobility jednotlivcov sú vo svojej podstate úzko prepojené a jedinečné. Za určitých okolností preto môžu ľahko podliehať pokusom o opätovnú identifikáciu.“ (De Montjoye et al., 2013; Pyrgelis et al., 2017)

Minimalizácia údajov by mala zohľadňovať aj prípadnú vzájomnú komunikáciu s dotknutými osobami a pokiaľ z účelu spracúvania vyplýva aj spätné odovzdávanie informácií (napríklad vo forme informovania osôb o blízkom kontakte s osobou nakazenou ochorením Covid 19 a pod.) je potrebné aj odosielané informácie podrobiť testu primeranosti, aby z nich napríklad neoprávnene nevyplynuli závery zasahujúce do súkromia inej osoby než tej, ktorá je informovaná (napríklad o identite nakazeného).

3.4 SPRÁVNOSŤ

Zásada správnosti predpokladá využitie iba správnych a podľa potreby aktualizovaných osobných údajov. Prevádzkovateľ je povinný prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia. Hoci GDPR nestanovuje čo je nesprávny údaj, prevádzkovateľ by mal „nastaviť interné postupy na overovanie správnosti získavaných, ako aj následne spracúvaných osobných údajov a podľa potreby aj postupy na zabezpečenie ich aktualizácie. Zložitosť uvedených interných procesov bude závisieť od viacerých okolností, najmä od povahy spracúvaných osobných údajov a účelu ich spracúvania, ako aj od skutočnosti, do akej miery môže spracúvanie ovplyvniť dotknutú osobu.“ (Komentár, str. 129) Zavedené interné postupy môžu byť zverejnené s ohľadom na zásadu transparentnosti.

Spoločne s overovaním správnosti údajov by mal byť nastavený aj proces možnosti/povinnosti opraviť údaje, najmä ak ich spracúvanie môže mať veľký vplyv na jednotlivcov. Toto by sa, samozrejme, malo vzťahovať iba na prípady, keď sa údaje spracúvajú spôsobom, ktorý takúto opravu technicky umožňuje, a v prípadoch, keď sa pravdepodobne vyskytnú uvedené nepriaznivé účinky (napríklad v prípade lokalizačných údajov v prípade ak zle zaznamenaná poloha bude mať vplyv na poskytnutie služby alebo priamy dôsledok pre dotknutú osobu).

3.5 MINIMALIZÁCIA UCHOVÁVANIA

Zásada minimalizácie uchovávania vyjadruje povinnosť prevádzkovateľa uchovávať osobné údaje vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na sledované účely. Nariadenie nestanovuje žiadnu konkrétnu minimálnu, ako ani maximálnu dobu uchovávania osobných údajov a túto si musí prevádzkovateľ nastaviť samostatne tak aby to vyhovovalo jednak účelu ale aj primeranosti a proporcionalite s ochranou súkromia dotknutých osôb. V prípade ak je to technicky a organizačne možné, mal by prevádzkovateľ pristúpiť k anonymizácii údajov a ďalej využívať iba agregované a anonymizované údaje. Nariadenie pripúšťa dlhšiu dobu uchovávania údajov na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely v súlade s článkom 89 ods. 1 za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných týmto nariadením na ochranu práv a slobôd dotknutých osôb.

V každom prípade by prevádzkovateľ mal spracúvanie obmedziť na striktné minimum (okrem prípadov, kedy dobu uchovávania stanovujú osobitné právne predpisy). Pre prípady overenia je vhodné stanovenú dobu pravidelne prehodnocovať, aktualizovať testy proporcionality a uchovávať záznamy o príkladoch, ktoré poukazujú na potrebu kratšej/dlhšej doby spracúvania.

3.6 INTEGRITA A DÔVERNOSŤ

Zásada zachovania bezpečnosti a ochrany osobných údajov vyjadrená najmä prostredníctvom zachovania ich integrity a dôvernosti dopĺňa všetky predchádzajúce zásady najmä zdôraznením takého spracúvania, ktoré „zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení.“ (Článok 5, ods. 1 f))

Opatrenia podporujúce integritu a dôvernosť vychádzajú už z podstaty minimalizácie údajov a ich uchovávania a nadväzujú na podmienky špecificky navrhnutej a štandardnej ochrany. Pri vyhodnocovaní primeranosti opatrení je potrebné implementovať najnovšie (state of the art) techniky, podmienky šifrovania a kryptografie, autentifikácie ale aj fyzického zabezpečenia objektov. Pri stanovovaní opatrení by mali prevádzkovatelia vykonať analýzu rizík, posúdenie vplyvu na ochranu osobných údajov, testy proporcionality pri použití najnovších technických noriem a usmernení dozorných orgánov.

4 ZÁVER

Tento článok nemal ambíciu posúdiť komplexné právne aspekty spracúvania osobných údajov ale načrtnúť problematiku, s ktorou sa bude musieť akýkoľvek prevádzkovateľ vysporiadať pri aplikácii moderných technológií pri monitorovaní a trasovaní osôb vo svojich priestoroch. V článku bol popísaný proces prepojenia spracúvania osobných údajov, akými sú aj lokalizačné údaje osôb pohybujúcich sa v zdravotníckych zariadeniach, v rámci informačných systémov využívajúcich moderné technické a programové prostriedky. Článok mal za ambíciu popísať možnosti a úskalia využitia týchto prostriedkov, ktorých využitie je legislatívne regulované Nariadením GDPR a pri akomkoľvek spracúvaní osobných údajov je prevádzkovateľ povinný postupovať v súlade s týmto nariadením o ochrane údajov. V článku je postupne rozanalyzovaných šesť základných zásad, od ktorých je možné odvodiť väčšinu povinných krokov pre posúdenie legálnosti spracúvania (zákonnosť/spravodlivosť/transparentnosť, obmedzenie účelu, minimalizácia údajov, správnosť, minimalizácia uchovávani a integrita/dôvernosť).

POĎAKOVANIE

Tento článok bol pripravený v rámci podpory projektu APPV-20-0457 Monitorovanie a trasovanie pohybu a kontaktu osôb v zdravotníckych zariadeniach.

LITERATÚRA

[1.] NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
[2.] Krátky slovník slovenského jazyka, 2003. dostupné na: https://www.juls.savba.sk/kssj_4.html
[3.] Usmernenia 4/2020 týkajúce sa lokalizačných údajov a iných nástrojov na sledovanie kontaktov v kontexte vypuknutia nákazy COVID-19
[4.] De Montjoye et al., 2013. „Unique in the Crowd: The privacy bounds of human mobility
[5.] Pyrgelis et al., 2017. „Knock Knock, Who's There? Membership Inference on Aggregate Location Data
[6.] Encyklopédia poznania, 2013, dostupné na: https://encyklopediapoznania.sk/clanok/405/pocitacove-siete-rozdelenie-podla-rozlohy-pan-lan-man-a-wan
[7.] Zákon č. 452/2021 Z. z. o elektronických komunikáciách
[8.] Zákon č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov
[9.] Zákon č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
Irena Hudecová, Anna Cyprichová, Ivan Makatura. 2018. Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov-GDPR - Veľký komentár. 978-80-8155-077-5

VÝZNAM ZNALOSTÍ FYZIKY PRO MATEMATIZACI BEZPEČNOSTNÍHO VZDĚLÁVÁNÍ

Jaroslav Tureček[*)]

ABSTRAKT

Pro matematizaci bezpečnostní výuky a bezpečnostní problematiky jsou často zapotřebí znalosti alespoň základních fyzikálních principů interakcí objekt – subjekt. Je zapotřebí mít základní ucelený vědecký přehled lidskými smysly nevnímatelných fyzikálních interakcí, které jsou díky bezpečnostním technologiím využitelné bezpečnostními orgány při přímém poznávání okolí bez fyzického kontaktu, případně jen s minimálním fyzickým kontaktem. Někdy se objevují i mezery v znalostech jednoduché mechaniky, jejíž znalosti jsou vhodné pro použití donucovacích prostředků s mechanickým účinkem apod.

Klíčová slova:
Bezpečnostní vzdělávání, matematizace, fyzikální interakce.

ABSTRACT

Knowledge of at least the basic physical principles of object-object interactions is often required for the mathematization of security teaching and security issues. It is necessary to have a basic comprehensive scientific overview of physical interactions that cannot be perceived by the human senses, which are, thanks to safety technologies, usable by security authorities in direct knowledge of the environment without physical contact, or only with minimal physical contact. Sometimes there are gaps in the knowledge of simple mechanics, whose knowledge is suitable for use of non-lethal weapons with the mechanical effect, etc.

Key words:
Safety education, mathematization, physical interactions.

ÚVOD

[*)] Jaroslav Tureček, doc. RNDr., Ph.D., Ambis. Vysoká škola., Katedra bezpečnosti a práva, e-mail: jaroslav.turecek@ambis.cz

Vyhledávání nástražných výbušných systémů (NVS) v budovách, areálech, na ulicích apod. je technicky velmi náročné a nikdy nebude možno poskytovat preventivní ochranu vždy a všude. Vyhledávání nástražných výbušných systémů u osob a jejich zavazadel se však dnes všeobecně považuje za možné a zároveň i nutné v případě vstupů[17] do důležitých a citlivých objektů, jako do letadel, důležitých vládních budov, do jaderných elektráren apod. Tedy vstupů do objektů kritické infrastruktury. Ochota financování, pokud to nenařizují předpisy, bývá často minimální. Pokud teroristé nebudou v dané situaci schopni zaútočit na dobře chráněný důležitý cíl, vyberou si sice jiný, méně chráněný. V rámci svých sil však nepřestanou zkoumat možnosti útoku na ten cíl důležitější, lépe chráněný. Hlavní tíha řešení problematiky spočívá na vývojových týmech a firmách vyrábějících detekční techniku. Naskytuje se tu otázka, jaká je spolehlivost těchto prohlídek a jaká by v současné době mohla být. Bezpečnostní manažery zajímají slabá místa detekce NVS při bezpečnostních prohlídkách osob a jejich zavazadel. A nejlepším způsobem, jak tyto slabiny zjistit, je pokusit se uvažovat jako terorista. Díky pokrokům v detekční technice se ale neustále zvyšuje podíl automatizace při bezpečnostních prohlídkách. V současné době se pro první stupeň bezpečnostních prohlídek zavazadel pořizují v nejlepším případě rentgeny s počítačovou tomografií (CT) a automatizovanou detekcí výbušnin. I před tou lze výbušninu technicky zamaskovat a hlavně mají z principu vysoký počet falešně pozitivních případů. Druhý stupeň se pak nechává na zkoumání rentgenového obrazu s vyznačenou podezřelou látkou operátorem. A zde je ještě horší slabina. Obraz NVS lze technicky maskovat před zobrazováním na rentgenovém obrazu. A též před detekcí stopových částic výbušnin, ať již přístrojovou nebo psy, lze NVS technicky maskovat. Potencionálního útočníka bude určitě zajímat možnost, jak zamaskovat jeho NVS tak, aby oklamal nejen personál bezpečnostní prohlídky, ale i automatickou detekci výbušniny přístrojem. Tedy jak technicky zamaskovat především výbušninu a rozbušku. Dá se předpokládat, že potencionální útočník nebude znát přesné parametry detekční techniky, zvláště pak konkrétní nastavení (např. citlivosti) na daném stanovišti bezpečnostní prohlídky, možná ani konkrétní sestavu přístrojů. Musí se ovšem počítat s tím, že mnohým útočníkům budou známy fyzikální principy detekčních přístrojů a jejich principiální nedostatky. Na některé nedostatky současné techniky je veřejnost nepřímo upozorňována při propagaci vývoje a zavádění techniky nové. Například výrok, že rentgenové systémy s počítačovou tomografií detekují i slabý plát výbušniny, upozorňuje, že u předcházejících typů rentgenů tomu asi tak nebude.

[17] Většinou nejslabšího místa ochrany.

1 FYZIKÁLNÍ INTERAKCE PŘÍMÉHO POZNÁVÁNÍ OBJEKT - SUBJEKT

Při přímém poznávání okolní bezpečnostní situace bezpečnostním orgánem dochází k oboustranné interakci mezi objektem a subjektem. Snahou přitom je co nejvíce omezit nutnost fyzického kontaktu. I značná část možností aktivního působení na objekt je omezena z důvodu ochrany zdraví a práv subjektu. Nutno poznamenat, že často bezdůvodně přehnaně.[18] Klasickým fyzickým kontaktem je vzájemný dotek dvou těles z pevných látek. Zvláštním, až sporným případem je proud kapaliny nebo plynu.

Přímé poznávání okolí **bez fyzického kontaktu** (případně s minimálním fyzickým kontaktem) je možné **třemi skupinami interakcí**:

- **Zářením** a to především elektromagnetickým zářením

- **akusticky** - jedná se sice o mechanický děj, který ale pro přenos energie využívá přirozeného prostředí mezi objektem a subjektem - nejčastěji vzduch, ale i pevné látky, vodu a jiné kapaliny a plyny.

- **přenosem** velmi malého-**stopového množství** částic, kdy je ovlivňování objektu minimální, zvláště pokud tyto částice putují od objektu k bezpečnostnímu orgánu. Nedá se však mluvit o záření, protože například u proudění par (plynů) se z hlediska mikroskopického jedná o neuspořádaný pohyb (viz kapitola „záření“).

Máme tedy tři základní druhy přenosu energie, informací, neboli podnětů mezi objektem a subjektem. Toto rozdělení nápadně připomíná tři ze smyslů člověka-zrak, sluch a čich. Jak ale uvidíme dále, zdaleka ne všechny konkrétní interakce budou názorné, tedy takové, aby se daly vysvětlit nějakou analogií z našim smyslům známého světa.

Při analýze a hodnocení jednotlivých interakcí si budeme muset vždy uvědomovat, jaká tělesa, látky vlastně chceme rozpoznat, detekovat. V naší bezpečnostní praxi to jsou především osoby, pozemní a říční dopravní technika, zbraně, výbušniny (nástražné výbušné systémy) a drogy. Dále si budeme muset uvědomit, na jakou vzdálenost, v jakém prostředí apod. chceme dotyčné předměty rozpoznat. Aby daný typ interakce, přenosu podnětu objekt-subjekt byl pro daný účel teoreticky využitelný, musí být splněny následující podmínky:

[18] Jako příklad můžeme uvést obavy ze zdravotních následků ozařování policejními radary pro měření rychlosti. Lidský mozek je přitom vystaven daleko silnějšímu elektromagnetickým záření při volání z mobilního telefonu.

- Musí se vskutku jednat o výraznější interakci se zkoumaným objektem. To znamená, že daný tok interakční energie nebo hmoty (což je ostatně též energie) musí buď ve zkoumaném objektu v dostatečné intenzitě vznikat, ať již z vnějšího podnětu nebo ne, anebo musí na něm nějakým výraznějším způsobem změnit své vlastnosti (absorpce, odraz, difrakce apod.).

- Daná interakce s vyhledávaným tělesem či látkou musí být dostatečně odlišná od okolního prostředí. Například člověk v bílé kombinéze i s kapucí za jasného slunečního svitu odráží pro lidské oko dokonalý dostatek světla, dochází tedy k velmi výrazné interakci. Přesto na sněhové pláni ho ve viditelném spektru velmi těžko vyhledáme. Termovizí snadno. V davu pestrobarevně oblečených lidí na náměstí bude situace zcela opačná.

- Interakce nesmí být příliš zeslabena či pozměněna vzdáleností a prostředím mezi objektem a subjektem. Prostředí mezi objektem a subjektem musí být pro dané interakční podněty objekt-subjekt dostatečně propustné.

Tyto podmínky musí být splněny pro daný, konkrétní typ interakce, který chceme použít. Nebylo by pracné teoreticky i experimentálně prokázat následující obecné zásady[19]:

- V naprosté většině případů platí, že nejlepší je, když je možno pro daný účel využívat několik odlišných typů interakce současně. Podstatně to zvýší pravděpodobnost detekce zájmového tělesa či látky a/nebo zmenší pravděpodobnost mylné detekce - „falešného poplachu“.
- Platí obecná pravidlo, že pokud lze nějakou značně monotónní část pozorování v bezpečnostní činnosti automatizovat, tak ji automatizujte. Nejenom, že to bude nakonec ekonomicky efektivnější, ale i spolehlivější. Nezapomeňte však přitom, že nejlépe každou pozitivní nebo spornou detekci by měl co nejdříve verifikovat bezpečnostní orgán-člověk.

V následujícím poznáme, že to, co platí pro jeden typ interakce, může být pro jiný typ interakce jinak. I staré rčení „Je to, jako hledat jehlu v kupce sena“ ztrácí trochu na váze. Vždyť v oblasti elektromagnetického záření v užším smyslu, konkrétně pro detektory kovů, to je celkem snadný úkol, zvláště když jehly bývají z feromagnetických kovů.

Problematikou, vztahem (interakcí) člověka a techniky, se zabývá filosofie techniky[20]. Nasazování této techniky ale nastoluje především některé teoretické otázky poznávání

[19] I když se musí, tak trochu ironicky, připomenout, že každé pravidlo se musí pro konkrétní případ posoudit znovu, samostatně.

[20] Viz např. Duda E.: *Filozofia techniky*, STU, Bratislava, 1991, str. 14., a další viz seznam literatury.

okolního světa[21], v našem případě bezpečnostní situace, prostřednictvím této techniky. Subjektem v poznávacím procesu se stává vlastně člověk i s přístrojem. Přístroj sice převede okolní podněty do podoby vnímatelné lidskými smysly, především zrakem, ale horší už je to s vytvořením představy v lidské mysli. I v případě, že technika vnější podněty automaticky vyhodnocuje a zpracovává do jasné výstupní formy (např. výbušnina je/není přítomna), stejně bezpečnostní orgán musí mít představu o jejích principech. Tato část poznávacího procesu, interakce mezi objektem a subjektem, není nikdy jednosměrná. Subjekt-bezpečnostní pracovníkpolicista, v tomto případě i s technikou - aktivně do procesu zasahuje. Přitom zákonitosti většiny interakcí objekt-subjekt (policista s technikou) se nebudou zcela shodovat s jeho přirozenými, zažitými představami, jakou jeho vědomí získalo během poznávání okolního světa pouze lidskými smysly. Někdy budou naopak na první pohled těmto představám odporovat. Například pokud interakce objekt-subjekt bude zprostředkována neutronovým zářením, znemožní nám pozorování nádherně průhledné akvárium s křišťálově-průzračnou vodou nacházející se mezi objektem a subjektem. A naopak tlustá ocelová deska mezi nimi nemusí vadit.

Je jasné, že znalost alespoň základních principů poznávací interakce objekt-subjekt je nezbytná i pro bezpečnostní orgány. Ani „inteligence“ nejmodernějších technických prostředků není všemohoucí. Zde si dovolím citaci z oblasti vojenství: „Je nesmyslné, aby souhru inteligentních senzorů s inteligentními zbraněmi měl v rukou člověk s nízkou inteligencí“.[22] Anebo všeobecně známý a zažitý citát amerických specialistů: „Veškeré zbraně jsou inteligentní jen tak, jak inteligentní je člověk, který je obsluhuje.“ V něčem trochu nadnesené, v něčem si ale dovolím jít ještě dál. Některé věci ani prostě nejde naučit výkladem nebo přijít na ně úvahami. Tyto vědomosti je potřebné doplnit praktickými zkušenostmi. Přístroj na základě interakce se zkoumaným objektem, například s taškou s nástražným výbušným systémem, transformuje lidskými smysly nevnímatelné podněty do podoby vnímatelné-většinou obrazu na monitoru. Policista si pak díky svým smyslovým orgánům udělá vjem tohoto obrazu. Pokud ale nemá dostačující představu o tom, jak různě by mohl vypadat obraz nástražného výbušného systému na monitoru dotyčného přístroje, přítomnost zájmové položky si ani neuvědomí. A zpětně. Nástražný výbušný systém bude pokaždé nejspíš jiný, jinak technicky maskovaný a zabalený mezi jinými věcmi. A zde je rozhodující, že lidský mozek je schopen nedostižitelného, někdy až intuitivního uvažování. Obsluha se s přístrojem „sžívá“, subjektem v poznávací interakci se stává policista s přístrojem. Stejný názor zastává i prof. dr. Ivan Úlehla, DrSc.: „V této diskusi jsme přenesli podstatu otázky vztahu subjektu a objektu na vztah zkoumaného objektu a přístroje.“[23] Věc se ještě více komplikuje tím, že spoléhat se pouze na jeden druh interakce objekt-subjekt není ve většině případů dostačující. A záleží zase především na policistovi, jak dobrou kombinaci si vybere a jak dobře ji využije.

[21] Viz Úlehla I.: *Fyzika a teorie poznání*, Horizont, Praha, 1982.
[22] Kaucký S.: *RC 400*, In: ATM, č.1/2000, str. 8-9.
[23] Úlehla I.: *Fyzika a teorie poznání*, Horizont, Praha, 1982, str. 412.

Vyvstává tu potřeba teoreticky se zabývat možnostmi a omezeními jednotlivých druhů interakcí zkoumaný objekt - policejní přístroj.

2 VYUŽITÍ ZÁŘENÍ PŘI POLICEJNÍ KONTROLE OBJEKTŮ

Tato skupina interakcí, zvláště pak elektromagnetické záření, poskytuje nejvíce možností pro využití v bezpečností praxi. Ve většině případů umožňuje bezpečnostním orgánům získávat dvoudimensionální, někdy i třídimensionální obrazy kontrolovaných objektů či celé pozorované scény. Bezpečnostní síly využívají nejrůznější druhy záření pro pozorování v terénu v noci, za mlhy, deště, hustého sněžení, pro pozorování teroristů za zdmi, pro odhalování zbraní, výbušnin, nástražných výbušných systémů, drog, většího množství bankovek či jiného kontrabandu pod oblečením osob, v jejich zavazadlech, v dopravních prostředcích i v budovách či pro detekci odposlouchávacích zařízení. Další obrovská oblast bezpečnostního využití je detekce pohybu narušitelů a jiné jejich činnosti v hlídaných objektech. Též při pátrání po objektech pod zemí či pod vodní hladinou nachází záření uplatnění. Jednotlivé druhy záření však mají často velmi odlišné, někdy i zcela protichůdné vlastnosti, a tak není možno v této úvodní části srozumitelně uvést všechny možnosti využití u bezpečnostních sil. Ty jsou nejpodrobněji uvedeny na začátku každé kapitoly o daném druhu záření.

Záření je uspořádaný pohyb částic. Pokud pohybující se částice jsou částice látkové, které mají klidovou hmotnost různou od nuly, mluvíme o **záření částicovém** (korpuskulárním). Jedná se například o proud elektronů, iontů, neutronů apod. Pokud pohybující se částice jsou částice polní, které mají klidovou hmotnost rovnu nule, mluvíme o **záření vlnovém**. Jedná se především o elektromagnetické záření, ale i o záření gravitační. Nutno podotknout, že i záření vlnové má korpuskulární vlastnosti a naopak, i záření korpuskulární (částicové) má též vlnové vlastnosti, ale ty nejsou tak zřetelné, a proto se užívají výše uvedené názvy druhů záření. Nejvýznačnější společnou vlastností korpuskulárního i vlnového záření je, že oba druhy jsou provázeny šířením energie v prostoru. Než přistoupíme k rozboru poznávací interakce objekt-subjekt v bezpečnostní činnosti prostřednictvím jednotlivých druhů záření, vysvětlíme si krátce pojmy částice látkové a polní.

2.1 ZÁŘENÍ ČÁSTICOVÉ (KORPUSKULÁRNÍ)

Této skupiny interakcí využívají bezpečnostní síly především pro vyhledávání výbušnin v zavazadlech určených do nákladových prostorů letadel, ale i výbušnin, drog a jiného kontrabandu ukrytého v osobních, nákladních a obytných vozech apod. Nelze je využívat pro kontrolu osob.

Záření částicové je uspořádaným (většinou velice rychlým) pohybem korpuskulárních částic (částic s nenulovou klidovou hmotností). Podle druhů těchto částic rozeznáváme i druhy korpuskulárního záření. Těch existuje více - například proud iontů, rychlých elektronů (záření α), héliových jader (záření β), atomové nebo molekulové svazky (paprsky), neutronové záření apod.

Většina druhů korpuskulárního záření je pro přímé pozorování bezpečnostní situace v podstatě nevyužitelná v důsledku buď malé průchodnosti materiály a/nebo destrukce materiálu zkoumaných objektů. Například známé záření α má ve vzduchu dosah řádově pouze centimetry, archem papíru neprojde a proniká do pokožky do hloubky pouze desetiny, spíše setiny milimetru. Přitom toto záření je přímo ionizující a na lidský organismus je více destruktivní než vlnové záření γ - pokud se radionuklidy vydávající záření α dostanou přímo na pokožku, ne-li do organismu. Záření β je sice méně, ale též nebezpečné živým organismům. Pronikavost je sice o něco lepší, ale stále malá - záření β přes tenkou hliníkovou desku, plexisklo nebo dlaň neprojde.

Výjimkou je neutronové záření. To je sice velmi nebezpečné živým organismům[24], ale když přestane na zkoumané předměty působit, nejsou tyto předměty prakticky vůbec zdrojem žádného nebezpečného záření ani nejsou ničím kontaminovány. Ani požívání takto ozářených tekutin a potravin není vůbec zdravotně závadné. Rozdíly nejsou větší než rozdíly mezi potravinami z různých přírodních zdrojů. Neutronové záření přitom z bezpečnostního hlediska velice zajímavé tím, že zcela snadno proniká materiály s vysokým protonovým číslem a naopak je brzděno materiály s nízkým protonovým číslem a navíc u jader dusíku, který je obsažen prakticky ve všech průmyslových a vojenských výbušninách, aktivuje okamžité záření γ o velmi vysoké energii. Teoretické možnosti uplatnění předurčují využití neutronového záření pro bezpečnostní prohlídku automobilů, zavazadel a zásilek, zvláště pro vyhledávání výbušnin a drog. Proto se neutronovému záření v rámci bezpečnostní činnosti budeme věnovat podrobněji.

2.2 ZÁŘENÍ VLNOVÉ

Fyzikální pole (polní kvanta, záření vlnové) zprostředkovávají silové působení mezi částicemi korpuskulárními, které je závislé na různých vlastnostech korpuskulárních částic. Podle toho, na kterých vlastnostech částic závisí, rozeznáváme čtyři druhy interakcí (sil, silových polí) mezi částicemi [25]:

[24] V sedmdesátých letech byla Spojenými státy vyvíjena neutronová hlavice pro taktické řízené střely, určená pro zneškodňování především velkých uskupení tanků a jiné obrněné techniky - přesněji pro zneškodňování jejich lidských osádek. Neutronové záření zcela snadno proniká těžkými kovy, tedy i pancířem obrněných vozidel, a usmrcuje živé organismy. Silněji ozáření lidé by umírali zhruba do 10 minut za příznaků podobným některým bojovým otravným látkám. Přitom terén, budovy, komunikace apod. by zůstaly nepoškozeny a terén nezamořen! Jednalo by se však o zbraň pouze taktickou, nikoliv strategickou, protože neutrony jsou intenzivně brzděny prvky s nízkým protonovým číslem, tedy i v atmosféře. Zvyšovat dosah nad ≈ 1,5 km by už bylo značně neúčinné.

[25] Viz Horák, Z. - Krupka, F.: Fyzika (Příručka pro vysoké školy technického směru). Praha, SNTL, 1981. Str. 20 a 985-6.

1. a 2.: slabá a silná interakce - ty však nemůžou, vzhledem ke svému omezenému dosahu, přenášet informaci přímo mezi objektem a subjektem - bezpečnostním orgánem. Není jim tedy třeba věnovat samostatnou pozornost.
3. gravitační interakce - přitahuje dvě částice silou úměrnou jejich hmotnostem. Využitelnost pro pozorování bezpečnostními silami spočívá pouze v tom, že jsou příčinou zemské tíže hmotných těles, tedy přitahování těles k Zemi, která má obrovskou hmotnost. Přitahování dvou těles o hmotnosti mnohem menší, než je hmotnost Země, je zanedbatelné.
Měření tíhy těles přístroji zvyšuje přesnost rozlišení a lze často snadno automatizovat. Je to však interakce vnímatelná lidskými smysly a proto lidé obecně mívají o ní dobrou představu. Též příklady využití vážení při bezpečnostní kontrole objektů každý dobře zná (kontrola maximálního přípustného zatížení náprav nákladních automobilů, celní převažování nákladů, nášlapná-tlaková nástrahová čidla pro detekci osob či vozidel, hmotnostní kontrola prázdnosti osobních propustní s automatizovanými detektory kovů a par výbušnin apod.). Výjimkou je mikrogravimetrie neboli velice přesné měření místních anomálií gravitačního pole Země, jenž je možno ve výjimečných případech využít i pro bezpečnostní účely.

4. elektromagnetická interakce - je zprostředkována polními částicemi (kvanty) zvanými fotony a působí silově na všechny částice s elektrickým nábojem. Z hlediska přímého poznávání bezpečnostní situace je velmi podstatné, že elektromagnetické pole se uplatňuje i v makroskopickém měřítku a je zcela rozhodujícím druhem přenosu informace - energie mezi objektem a subjektem.
Elektromagnetické záření poskytuje zdaleka nejvíce možností pro využití v bezpečností praxi. Ve většině případů umožňuje bezpečnostním orgánům získávat dvoudimensionální, někdy i třídimensionální obrazy kontrolovaných objektů či celé pozorované scény. Bezpečnostní síly využívají nejrůznější druhy záření pro pozorování v terénu v noci, za mlhy, deště, hustého sněžení, pro pozorování teroristů za zdmi, pro odhalování zbraní, výbušnin, nástražných výbušných systémů, drog, většího množství bankovek či jiného kontrabandu pod oblečením osob, v jejich zavazadlech, v dopravních prostředcích i v budovách či pro detekci odposlouchávacích zařízení. Další obrovská oblast bezpečnostního využití je detekce pohybu narušitelů a jiné jejich činnosti v hlídaných objektech. Též při pátrání po objektech pod zemí či pod vodní hladinou nachází záření uplatnění. Jednotlivé druhy záření však mají stále často velmi odlišné, někdy i zcela protichůdné vlastnosti, a tak není možno v rámci rozsahu tohoto článku srozumitelně uvést všechny možnosti využití u bezpečnostních sil. Ty jsou nejpodrobněji uvedeny na začátku každé kapitoly o daném druhu záření.

Z výše uvedeného vyplývá, že pro přímé poznávání okolní bezpečnostní situace bezpečnostním orgánem bude zcela nejvýznamnějším druhem zářením záření elektromagnetické.

2.3 AKUSTIKA

Techniky založené na akustických interakcí se při bezpečnostní kontrole objektů využívá pro rozšíření možností poslechu aktivních zdrojů zvuku, jako například časovacích mechanismů nástražných výbušných systémů, narušitelů pohybujících se v hlídané místnosti, po hlídaném pozemku, překračujícího státní hranice, narušitelů manipulujících s hlídaným předmětem, používajícího nejrůznějšího nářadí pro narušení pláště hlídaného objektu. Též se využívají pro zlepšení odposlechu přes zdi apod., což už ale není předmětem této práce. Při záchranných akcích se tyto systémy hojně využívají pro vyhledávání žijících osob ve zřícených budovách, v závalech apod. Při celních prohlídkách se akustických interakcí využívá pro vyhledávání kontrabandu v pneumatikách a nejrůznějších nádržích apod. Pro policejní síly je to důležitá interakce pro vyhledávání různého kontrabandu a informačně důležitých předmětů na dně hlubokých vod. V bezpečnostní praxi se této interakce využívá též pro detekci narušitelů hlídaného vodního prostoru, jako motorových člunů, potápěčů s i bez podvodních skútrů.

Zvuk je uspořádaný kmitavý pohyb molekul přenášený působením sil mezi molekulami. Zvuk je tedy vlastně vlnění molekul a může se šířit pouze v látkách, ne ve vakuu. Na zvukové vlny můžeme pohlížet jako na střídavé (podélné) zhušťování a zřeďování vzduchu (nebo jiného prostředí, v němž se šíří). Rychlost šíření zvuku ve vzduchu závisí na tlaku, teplotě a vlhkosti. Rychlost zvuku je též velmi závislá na prostředí. Intenzita zvuku se šířením postupně zeslabuje - jednak šířením do více stran, dále absorpcí v přenášející látce a též odrazem na tělesech.

3 VYUŽITÍ PŘENOSU STOPOVÝCH ČÁSTIC PŘI BEZPEČNOSTNÍ KONTROLE OBJEKTŮ

Pod pojmem přenos stopových částic (či pouze přenos částic) budeme chápat chaotický, neuspořádaný pohyb (neuspořádaný z hlediska jednotlivých částic) korpuskulárních částic a/nebo přenos těchto částic na povrchu či v objemu jiné látky. Tyto částice by měly být charakteristické pro zkoumaný objekt z bezpečnostního hlediska. Budou to tedy molekuly, atomy a jejich ionty. Určitý objem přenášených částic může mít společnou, uspořádanou složku pohybu. Například proud plynu nebo přenos částeček naadsorbovaných na povrchu přenášeného papírku apod. V bezpečnostní praxi se pro detekci objektů využívá přenosu malého množství částic, které jsou z objektu uvolňovány ve formě:

A) plynů či spíše par látek pocházejících z objektu
B) pevných částeček, výjimečně kapiček pocházejících z objektu

Pro úplnost musíme uvést též případ, kdy jsou detekovány plyny (páry) uvolňované nikoliv z vlastního zájmového objektu, ale z předmětů a látek v okolním prostředí,

jejichž zvýšené uvolňování par bylo zapříčiněno předcházející činností zájmového objektu.[26]

ZÁVĚR

Pro matematizaci bezpečnostní výuky a bezpečnostní problematiky jsou často zapotřebí znalosti alespoň základních fyzikálních principů interakcí objekt – subjekt. V práci byly uvedeny všechny základní, lidskými smysly nevnímatelné interakce s minimálním fyzickým kontaktem objekt-subjekt, prostřednictvím kterých může bezpečnostní orgán zásadně rozšířit své možnosti zkoumání neznámých, předem neoznačených objektů při pozorování a kontrole blízké bezpečnostní situace.
Výuka základních znalostí fyzikálních principů interakcí by měla být zaměřena na interakce nevnímatelné lidskými smysly proto, že zkoumání interakcí vnímatelných lidskými smysly by bylo buďto příliš obecné, a pak triviální, s minimálním vědeckým přínosem a zbytečné, protože to téměř každý zná, nebo naopak příliš technicky detailní a pak nezapadající už do obecné teorie policejních věd, a navíc pro většinu policejních pracovníků opět zbytečné, neboť by to v praxi nevyužili.
Z práce je uveden důležitý poznatek, že přímé poznávání okolí bez fyzického kontaktu (případně s minimálním fyzickým kontaktem) je možné třemi skupinami interakcí:

- zářením a to především elektromagnetickým zářením
- akusticky - jedná se sice o mechanický děj, který ale pro přenos energie využívá přirozeného prostředí mezi objektem a subjektem - nejčastěji vzduch, ale i pevné látky, vodu a jiné kapaliny a plyny.
- přenosem velmi malého-stopového množství částic, kdy je ovlivňování objektu minimální, zvláště pokud tyto částice putují od objektu k bezpečnostnímu orgánu.

Aby daný typ interakce, přenosu podnětu objekt-subjekt byl pro daný účel teoreticky využitelný, musí být splněny následující podmínky: Musí se vskutku jednat o výraznější interakci se zkoumaným objektem, daná interakce s vyhledávaným tělesem či látkou musí být dostatečně odlišná od okolního prostředí a interakce nesmí být příliš zeslabena či pozměněna vzdáleností a prostředím mezi objektem a subjektem.
Dále by se měly držet následujících obecných zásad: Nejlepší je, když je možno pro daný účel využívat několik odlišných typů interakce současně, pokud lze nějakou značně monotónní část pozorování v bezpečnostní činnosti automatizovat, tak ji automatizovat, avšak nezapomenout přitom, že nejlépe každou pozitivní nebo spornou detekci by měl co nejdříve verifikovat bezpečnostní orgán-člověk.

[26] Typickým příkladem je policejní pes „na frekvenci“ v lese, tj. když sleduje stopy zanechané před nepříliš dlouhou dobou (maximálně ≈ 8 hodin) sledovanou osobou. Plyny a páry uvolněné sledovanou osobou dávno odvál vítr a množství částeček otřených z jeho obuvi při každém šlápnutí, které jsou zároveň charakteristické pro jeho obuv, je minimální. Policejní pes však využívá i páry uvolňované ve zvýšené míře z měkké zeminy, narušené v místě šlápnutí.

LITERATURA

[1] TUREČEK, J. Policejní technika jako předmět vysokoškolské výuky. In *Úloha policejně bezpečnostních disciplín v systému vysokoškolské přípravy policistů: mezinárodní konference.* Praha: Police history, 2006, s. 27-33. ISBN 80-86477-34-7

[2] TUREČEK, J. Pojem a druhy policejní techniky. In *Bezpečnostní teorie a praxe: Problémy konstituování a rozvoje policejních věd, teorie policejně bezpečnostní činnosti a transferu vědeckých poznatků do policejní praxe.* Praha: Policejní akademie ČR, 2003, zvláštní číslo – 1. díl, s. 131-138. ISBN 80-7251-148-3

[3] TUREČEK, J. Význam znalostí techniky u policie (Zdokonalování bezpečnostních prohlídek pomocí inertních výbušnin). In *Teoretická reflexe a identifikace společenských potřeb ve vazbě na aktuální problémy policejní praxe.* Praha: Policejní akademie ČR, 2003, 1. díl, s. 159-169. ISBN 80-7251-145-9

[4] STRAUS, J. TUREČEK, J. Význam přírodních a technických věd pro činnost policie. In: *Problémy rozvoje teorie policejně-bezpečnostní činnosti a policejních věd.* Sborník Policejní akademie ČR k problematice vědecko-výzkumného úkolu: *Bezpečnostní teorie a praxe*. Zvláštní číslo. Praha: Policejní akademie ČR, 2000, s. 361-366

[5] TUREČEK, J. Aplikace vybraných přírodních a technických věd pro činnost policie při kontrole objektů. Doktorandská disertační práce. Bratislava, 2000, 140 s.

POSOUZENÍ RIZIK V RÁMCI NÁVRHU POPLACHOVÝCH SYSTÉMŮ

Ing. Jan Valouch, Ph.D., Ing. Stanislav Kovář, Ph.D.
Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky,
Ústav bezpečnostního inženýrství

ABSTRAKT
Bezpečnostní posouzení objektu představuje nedílnou součást etapy návrhu poplachových systémů. Na jeho základě je možno stanovit stupeň zabezpečení a získat představu o složení a rozsahu navrhovaného systému. Cílem příspěvku je provést porovnání normativních doporučení na postup a strukturu posuzování rizik objektů v rámci návrhu poplachových zabezpečovacích a tísňových systémů, systémů kontroly vstupu a dohledových videosystémů.

Klíčová slova
Bezpečnostní posouzení, posouzení rizik, analýza rizik, projektování, systém kontroly vstupu, dohledový videosystém, poplachový zabezpečovací a tísňový systém.

ABSTRACT
The security assessment of the object is an integral part of the design phase of alarm systems. On the basis of it, it is possible to determine the level of security and get an idea of the composition and scope of the proposed system. The aim of the paper is to compare normative recommendations for the procedure and structure of risk assessment within the design of intrusion and hold-up alarm systems, access control systems and video surveillance systems.

Key words:
Security Assessment, risk assessment, risk analysis designing, electronic access control systems, video surveillance systems, intrusion and hold-up alarm systems.

1 ÚVOD

Bezpečnostní posouzení objektů je jednou z podstatných činností v rámci procesu zřizování poplachových systémů. Mělo by být provedeno v rámci předprojektových prací před zpracováním prvního návrhu systému (studie). Bezpečnostní posouzení je

možno definovat jako proces analýzy faktorů ovlivňujících návrh poplachových systémů, s cílem zejména:

- identifikovat a vyhodnotit faktory mající vliv na volbu komponentů a jejich umístění,
- stanovit požadovaný stupeň zabezpečení systému,
- odhadnout možné budoucí hrozby na referenční objekt,
- charakterizovat potencionálního narušitele,
- redukovat plané poplachy [1].

Při návrhu zabezpečení objektů jsou kromě mechanických zábranných systémů aplikovány:

- poplachové zabezpečovací a tísňové systémy (PZTS),
- elektronické systémy kontroly vstupů (ESKV),
- dohledové videosystémy (DV).

Technické normy řešící problematiku návrhu, projektování a instalace výše uvedených poplachových systémů zahrnují rovněž ustanovení o realizaci bezpečnostního posouzení.

- ČSN CLC/TS 50131-7. Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace [2],
- ČSN EN 62676-4. Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 4: Pokyny pro aplikace [3],
- ČSN EN 60839-11-2. Poplachové a elektronické bezpečnostní systémy – Část 11-2: Elektronické systémy kontroly vstupu – Pokyny pro aplikace [4].

Pokud zákazník v praxi netrvá smluvně na dodávce a montáži poplachového systému dle výše uvedených technických norem, může dojít k následujícím pochybením ze strany dodavatele:

- bezpečnostní posouzení není provedeno vůbec,
- bezpečnostní posouzení není provedeno kompletně,
- bezpečnostní posouzení není provedeno vhodnou osobou,
- bezpečnostní posouzení není provedeno s využitím odpovídajících metod [5].

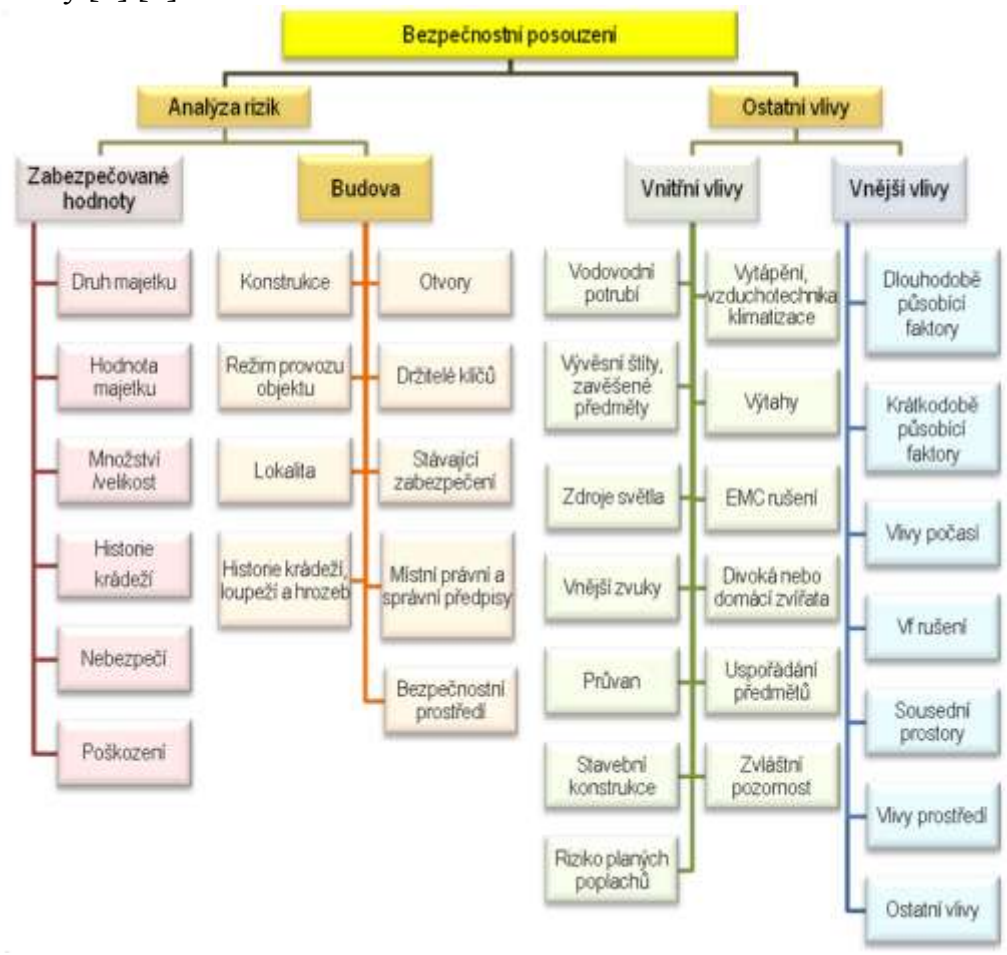
V současné době dodává (návrh, projekce, instalace) poplachové systémy (PZTS, ESKV i DV) zpravidla jeden dodavatel. V takovém případě je nanejvýš vhodné (v případě smluvního požadavku na realizaci systému dle stanovených technických norem řady ČSN EN 50131, ČSN EN 62676 a ČSN EN 60839 pak povinné) realizovat bezpečnostní posouzení objektu v takovém obsahu a formě, které budou naplňovat všechny relevantní normativní požadavky.

Následující podkapitoly prezentují základní normativní doporučení na bezpečnostní posouzení poplachových systémů a následně jejich komparaci.

Pozn. Pro označení procesu bezpečnostního posouzení jsou v relevantních technických normách (PZTS, ESKV, DV) používány i názvy posouzení rizik nebo analýza rizik.

2. BEZPEČNOSTNÍ POSOUZENÍ PZTS

Strukturu a obsah bezpečnostního posouzení PZTS upravuje norma ČSN CLC/TS 50131-7 [2] a technická normalizační informace TNI 334591-1 [7]. Bezpečnostní posouzení je zde založeno na vyhodnocení **čtyř základních oblastí zájmu**, které by měl projektant brát v úvahu při následném návrhu PZTS resp. při zpracování projektové dokumentace. Jedná se o **zabezpečované hodnoty, budovu, vnější a vnitřní vlivy.** Tyto oblasti je možné klasifikovat do dvou skupin- analýza rizik a ostatní vlivy [2] [9].



Obr. 1 Obsah bezpečnostního posouzení PZTS [2] [8], upravil Valouch 2021

Analýza rizik, obsahující posouzení zabezpečovaných hodnot a budovy, je zpracovávána **s cílem stanovení požadovaného stupně zabezpečení** (1 až 4) v souladu s ČSN EN 50131-1 ed.2. Na základě první části bezpečnostního posouzení je tedy nutno následně identifikovat potencionální hrozby a zvážit jejich rizika, identifikovat slabá místa objektu, kvantifikovat rizika s ohledem na následek škody a pravděpodobnost vzniku hrozby. Tuto identifikaci hrozeb a určení rizik již norma ČSN CLC/TS 50131-7 neřeší [9].
Druhá skupina oblastí zájmů bezpečnostního posouzení představuje posouzení ostatních vlivů (majících původ uvnitř/ vně střeženého objektu). Cílem posouzení ostatních vlivů je **vyhodnocení stávajících nebo budoucích podmínek uvnitř a vně střežených prostorů** z hlediska následného výběru a umístění komponent.

3. ANALÝZA RIZIK ELEKTRONICKÝCH SYSTÉMŮ KONTROLY VSTUPU

Strukturu a obsah bezpečnostního posouzení ESKV upravuje norma ČSN EN 60839-11-2 [4]. Proces bezpečnostního posouzení je zde označován jako **analýza rizik**, jejíž hlavním cílem je identifikovat rizika a vnímané hrozby za účelem stanovení vhodného stupně zabezpečení (1 až 4). Analýza rizik je první činností v rámci úvodní etapy zřizování ESKV - plánování systému. Norma popisuje analýzu rizik pouze ve formě schématu.

Obr. 2 Schéma analýzy rizik [4], upravil Valouch 2021

Aspekty identifikované v analýze rizik mají pomoci projektantovi při výběru ESKV, který zajistí kontrolu vstupu a integritu zabezpečení odpovídající hodnotě majetku vyžadujícího ochranu a souvisejícím rizikům [4]. Stupně zabezpečení se stanoví s ohledem na:

- hodnotu chráněného majetku,

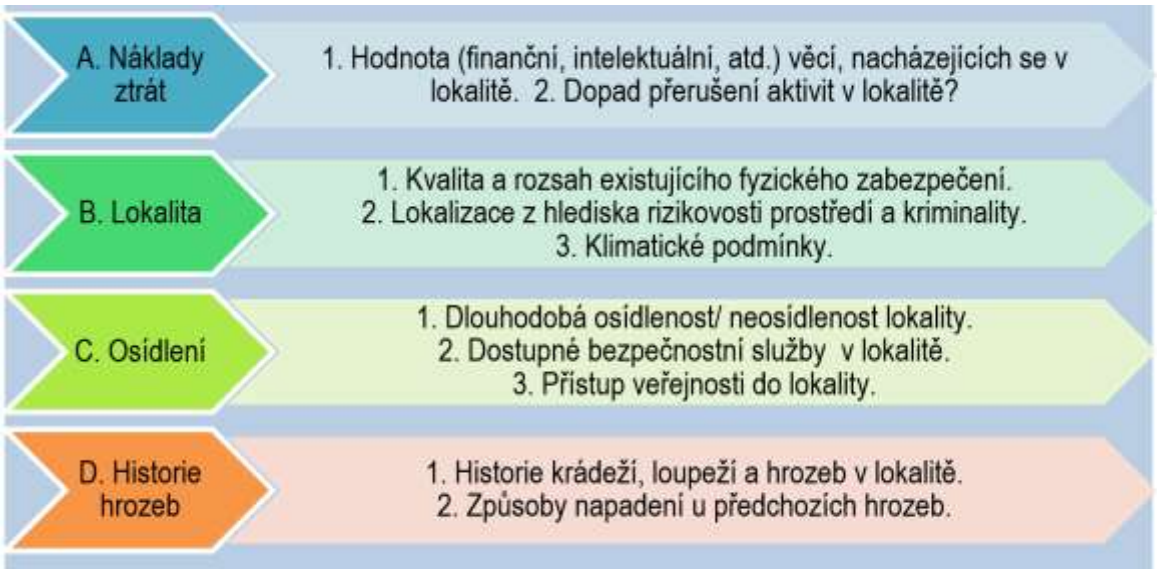
- odhodláním (znalosti/ schopnosti) potencionálního pachatele,
- způsoby útoku potencionálního pachatele, kteří se snaží ESKV obejít.

4. POSOUZENÍ RIZIK DOHLEDOVÝCH VIDEOSYSTÉMŮ

Strukturu a obsah bezpečnostního posouzení DV upravuje norma ČSN EN 62676-4. Proces bezpečnostního posouzení je zde označován jako **posouzení rizik**, který je definován jako systematický postup určování dopadů následků nebezpečí a hrozeb v závislosti na jejich pravděpodobnosti. Výsledek posouzení rizik zde poskytuje základ pro hodnocení rizik v procesu managementu rizik. Management rizik je chápán jako proces tvorby postupů a směrnic určených pro účinné zvládání možných událostí a jejich negativních následků [3].
Posouzení rizik je první činností implementace DV. Má být provedeno s cílem porozumění účelu DV a má zahrnovat:

- identifikaci a odhad hrozeb,
- identifikace nebezpečí,
- posouzení pravděpodobnosti hrozeb a nebezpečí,
- posouzení dopadu hrozeb a nebezpečí.

Struktura a obsah posouzení rizik je zde uvedena formou následujícího příkladu.



Obr. 3 Příklady struktury posouzení rizik DV [3], upravil Valouch 2021

Hrozby, nebezpečí a jejich dopad jsou zde chápány jako rizika pro objekty a organizace. DV má být navržen tak, aby zmírnil rizika, která z posouzení vyplynula. Výsledky hodnocení rizik mají být použity ke stanovení požadavků na DV a jeho komponenty (včetně stanovení stupňů zabezpečení 1 až 4) [3]. Norma se v rámci

realizace posouzení rizik odkazuje na technickou normu ISO 31000:2009, jejíž aktuální vydání ČSN ISO 31000 Management rizik – Směrnice: 2019, stanovuje pouze principy posuzování rizik (identifikace, analýza, hodnocení rizik).

4. KOMPARACE

Následující tabulka prezentuje komparaci normativních doporučení pro jednotlivé poplachové systémy.

Tab. 1 Základní charakteristika ustanovení technických norem pro bezpečnostní posouzení poplachových systémů

Charakteristika	PZTS	ESKV	DV
Název	Bezpečnostní posouzení	Analýza rizik	Posouzení rizik
Technická norma	ČSN CLC/TS 50131-7, TNI 334591-1	ČSN EN 60839-11-2	ČSN EN 62676-4
Dokument	Zápis (záznam) o bezpečnostním posouzení	Není upřesněno	Posouzení rizik
Zařazení	1. etapa Návrh systému	1. etapa Plánování systému	1. Posouzení rizik
Struktura	- zabezpečované hodnoty, - budova, - vnitřní vlivy, - vnější vlivy	- majetek - hrozba - riziko - co dělat (opatření)	- náklady ztrát - lokalita - osídlení - historie krádeží, loupeží a hrozeb
Obsah	- podrobně popsán v přílohách normy 50131-7 (B,C,D, E)	- uveden pouze v několika bodech formou schématu analýzy rizik	- uveden pouze v několika bodech formou odrážek
Metody	Předběžná analýza rizik PHA, expertní posouzení, strukturované metody analýzy rizik (ETA, FTA, HRA, FMEA).	Nejsou upřesněny	Pouze odkaz na základní principy v ČSN ISO 31000 Management rizik
Forma	Check list (příklad)	Není uvedena	Není uvedena
Používané pojmy	Riziko, hrozba, bezpečnostní prostředí	Hrozba, riziko, bezpečnostní opatření	Nebezpečí, hrozba, pravděpodobnost, management rizik.
Pozitiva	Jasná struktura, podrobný obsah.	Logická struktura a postup.	Naznačení logické struktury posouzení.
Nedostatky	Absence samostatné části pro vymezení hrozeb a rizik (stávajících i odhad budoucích).	- není stanoven podrobnější obsah analýzy rizik, metody ani forma.	- není stanoven podrobnější obsah posouzení rizik, metody ani forma.

Z komparace doporučení ke struktuře, obsahu a realizaci bezpečnostního posouzení publikovaných v technických normách pro aplikaci PZTS, ESKV a DV vyplývají následující závěry:

- používání nejednotné terminologie pro stejný proces (bezpečnostní posouzení, analýza rizik, posouzení rizik),
- obdobná struktura bezpečnostního posouzení (zabezpečované hodnoty, hrozby, vliv lokality), ale opět jiná terminologie a jiný obsah,
- nejlépe a nejpodrobněji je zpracován proces bezpečnostního posouzení PZTS (ČSN CLC/TS 50131-7, TNI 334591-1), který je přímo aplikovatelný v praxi,
- informace k bezpečnostnímu posouzení pro ESKV (ČSN EN 60839-11-2) a DV (ČSN EN 62676-4) jsou stručné, neúplné a v praxi přímo neaplikovatelné- bylo by nezbytné si nejdříve připravit podrobný obsah.

5. ZÁVĚR

Bezpečnostní posouzení objektů je jednou z podstatných činností v rámci procesu zřizování poplachových systémů. Mělo by být provedeno v rámci předprojektových prací před zpracováním prvního návrhu systému (studie). V praxi bývá tato činnost často opomíjena úplně, nebo realizována nedostatečně.
Článek analyzuje a porovnává doporučení technických norem k realizaci, struktuře a obsahu bezpečnostního posouzení pro PZTS, ESKV a DV. Nejlepší situace je v oblasti technických norem a technických normalizačních informací pro aplikaci PZTS (ČSN CLC/TS 50131-7, TNI 334591-1), jež stanovují postupy, struktury a obsah bezpečnostního posouzení, které je v praxi realizovatelné.
Pro realizaci bezpečnostního posouzení objektů je možné a velmi vhodné využít (samozřejmě v kombinaci s doporučeními ve výše analyzovaných oborových normách PZTS, SKV, DV) i doporučené postupy publikované v technických normách v oblasti **prevence kriminality** (řada ČSN P CEN/TS 14383 Prevence kriminality) a to např. pro objekty využívané jako obydlí, pro obchodní a administrativní budovy, čerpací stanice nebo zařízení veřejné dopravy). Tato doporučení jsou formulována především ve formě check listů a dotazníků [10] [11] [12].
Uvedenou kombinaci využívají autoři článku v praxi při praktických realizacích bezpečnostních posouzení technologických a obchodních objektů.

LITERATURA

[1] VALOUCH, Jan. Security Assessment of the Object in terms of Alarm system design. In the Science for Population Protection. Lázně Bohdaneč: MV- GŘHZS, Institut ochrany obyvatelstva. Vol. 4. p. 185 - 190. ISSN: 1803-568X.

[2] ČSN CLC/TS 50131-7. Poplachové systémy- Poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. 44 s.

[3] ČSN EN 62676-4. Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 4: Pokyny pro aplikace. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016. 64 s.

[4] ČSN EN 60839-11-2. Poplachové a elektronické bezpečnostní systémy - Část 11-2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016. 32 s.

[5] VALOUCH, Jan, Kovář Stanislav. Teorie a praxe zřizování poplachových zabezpečovacích a tísňových systémů. In Sborník mezinárodní konference Krizové řízení a řešení krizových situací. KONEČNÝ, Jiří (ed.). CrisCon 2021. Uherské Hradiště: Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení, 2021. ISBN 978-80-7678-028-6. s. 324- 336. 13 s.

[7] TNI 33 4591-1. Poplachové systémy-Poplachové zabezpečovací a tísňové systémy-Část 1: Návrh systému PZTS- Komentář k ČSN CLC/TS 50131-7:2011. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012. 16 s.

[8] ŠEVČÍK, Jiří, 2012. Bezpečnostní posouzení objektu. Security Magazin. Vyd. č. 105, 1/2012. Praha: Security Media, 2012, s. 8- 11. ISSN 1210-8273.

[9] VALOUCH, Jan. Projektování bezpečnostních systémů. [skriptum]. Zlín: UTB, 2012. ISBN 978-80-7454-230-5. 152 s.

[10] ČSN P CEN/TS 14383-3 Prevence kriminality – Plánování městské výstavby a navrhování budov - Část 3: Obydlí. Praha: ČNI, 2006. 52 s.

[11] ČSN P CEN/TS 14383-4 Prevence kriminality- Plánování městské výstavby a navrhování budov- Část 4: Obchodní a administrativní budovy. Praha: ČNI, 2007. 36 s.

[12] ČSN P CEN/TR 14383-5 Prevence kriminality- Plánování městské výstavby a navrhování budov- Část 5: Čerpací stanice. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. 52 s.

SECULIN 2021
Sborník 5. ročníku mezinárodního online workshopu SECULIN 2021, Zlín 11. listopadu 2021
Editor: doc. Ing. Martin Hromada, Ph.D.
Nebyla provedena jazyková korektura
Vydavatel: Univerzita Tomáše Bati ve Zlíně
Pořadí vydání: první
Rok vydání: 2022
ISBN 978-80-7678-067-5