Univerza v Mariboru
Fakulteta za varnostne vede

Matej Cimerman

SISTEM TEHNIČNEGA VAROVANJA- PRIMER POSTAVITVE SISTEMA ZA FIZIČNE OSEBE

Diplomsko delo
visokošolskega študijskega programa Varnost in policijsko delo

Ljubljana, september 2021

Univerza v Mariboru

Fakulteta za varnostne vede

SISTEM TEHNIČNEGA VAROVANJA- PRIMER POSTAVITVE SISTEMA ZA FIZIČNE OSEBE

Diplomsko delo

Študent: Matej Cimerman

Študijski program: Visokošolski študijski program Varnost in policijsko delo

Mentor: Doc. dr. Srečko F. Krope

Zahvala

Za pomoč pri izdelavi diplomskega dela se zahvaljujem mentorju doc. dr. Srečko F. Kropetu.

Zahvaljujem se tudi Mojci Cimerman za svetovanje pri pisanju diplomskega dela.

Sistem tehničnega varovanja - primer postavitve sistema za fizične osebe

Ključne besede: Wi-Fi, usmerjevalnik, mobilni telefon, aplikacija

Povzetek

V diplomskem delu smo predstavili tehnično opremo, ki smo jo uporabili, postopek konfiguriranja naprav ter uporabili program DEXi. Podrobno smo opisali katero opremo smo uporabili sami, kje smo jo kupili in koliko smo zanjo odšteli. Razložili smo kaj pomenijo pojmi, ki smo jih uporabili in kje jih uporabiti.

Pri uporabi tehnične opreme smo ugotovili, kako se ta odziva in koliko je uporabna v praksi. Ugotovili smo, da je oprema funkcionalna do določene mere, saj je oprema v nizkocenovnem razredu. Slabosti smo ugotovili predvsem pri občutljivosti kamer, saj so zaznavale premik listja, dreves in senc, česar po besedah proizvajalca ne bi smele. Stopnjo občutljivosti kamere za zaznavanje se lahko nastavi na nizko raven in v tem primeru bi morala kamera zaznati samo premike večjih objektov ali ljudi. Slaba vidljivost kamere je tudi v nočnem pogledu, saj se v popolni temi skoraj nič ne vidi. Slabost je tudi ta, da ni možno vse opreme dodati v eno aplikacijo in od tam vsega konfigurirati, saj določeni izdelki ne podpirajo te možnosti. S pomočjo programa DEXi smo ugotovili, da je naš sistem tehničnega varovanja priporočljiv v vseh kategorijah.

Povezljivost kamer deluje dobro, prav tako obveščanje uporabnika na mobilni telefon. Z tehničnim sistemom smo relativno zadovoljni. Smo pa tudi bolj sproščeni z vidika varnosti.

Example of setting up a technical security system for private individuals

Keywords: Wi-Fi, router, mobile phone, application

Abstract

In this paper work, we presented the technical equipment we used, the process of configuring devices and used the DEXi program. We described in detail which equipment we used ourselves, where we bought it and how much we paid for it. We explained what terms we used, what they meant and where to use them.

When using technical equipment, we found out how it responds and how useful it is in practice. We found that the equipment is functional to some extent as the equipment is in the low cost class. We mainly found weaknesses in the sensitivity of the cameras, as they detected the movement of leaves, trees and shadows, which, according to the manufacturer, should not have happened. The sensitivity level of the detection camera can be set to low in which case the camera should only detect the movements of larger objects or people. The camera's poor visibility is also in the night view, as almost nothing can be seen in complete darkness. Another disadvantage is that it is not possible to add all the equipment to one application and configure everything from there, as certain products do not support this option. With the help of DEXi program, we found that our technical security system is recommended in all categories.

Camera connectivity works well, as does informing the user on the mobile phone. We are relatively satisfied with the technical system. But we are also more relaxed in terms of security.

Kazalo vsebine

Kazalo tabel

Kazalo slik

Uporabljeni simboli in kratice

Wi-Fi brezžična tehnologija (Wireless network)

LAN lokalno omrežje (Local Area network)

WLAN brezžično krajevno omrežje (Wireless local area network)

WAN široko pasovno omrežje (Wide Area Network)

IP Internet protokol (Internet Protocol)

USB univerzalno serijsko vodilo (Universal Serial Bus)

1 UVOD

Tehnično varovanje z video nadzornim sistemom je danes zelo popularno in razširjeno, vendar se fizične osebe zanj odločajo redkeje, saj predstavlja ne nujen strošek. Za sistem tehničnega varovanja se zaradi vidika varnosti odloči skoraj vsako podjetje kot so bencinski servisi, prodajalne, trgovine, banke in pošte. Podjetjem tehnično varovanje postavljajo profesionalne ekipe. Postavitev sistema za tehnično varovanje je lahko zelo obširen z več kamerami, senzorji in alarmi ali samo s kamero ali dvema za nadzorovanje območja. Od tega koliko kamer, njihove ločljivosti, kvalitete kamer in povezljivosti je odvisna tudi cena. Postavitev video nadzornega sistema s strani podjetja predstavlja mnogo večji strošek kot v primeru če ga postavimo sami. O varovanju in oddaljenem nadzoru doma lahko, preberemo članek v reviji Monitor, ki pa za laika ni tako enostaven (naslov članka v reviji Monitor se glasi) »Prihajajo negotovi časi. Kako izdelamo enostaven varnostni sistem s kamero? Koliko stane? Katero programsko opremo lahko uporabimo? Kako omogočiti dostop do žive slike iz stanovanja preko spleta?«(Vavpotič, S. P., 2020). Ravno zaradi pomankanja literature, ki opisuje enostaven postopek postavitve tehničnega sistema, smo se odločili, da sami raziščemo to področje in ga opišemo.

Problem oziroma vprašanje se pojavi, ko želimo zavarovati naš dom s tehnično varnostnim sistemom, vendar nismo pripravljeni plačati veliko denarja. Investicija namreč ni nujno potrebna, vendar se počutimo bolj varne če tehnično varnostni sistem imamo.

Uporaba pametnih naprav kot so pametni telefoni, tablice, računalniki, avtomatsko nastavljivi usmerjevalniki in Wi-Fi omrežja je danes namreč zelo razširjena, tako da lahko relativno enostavno sami postavimo sistem tehničnega varovanja. Pri raziskovanju nismo nikjer našli, kako bi z enostavnimi navodili postavili lasten sistem tehničnega varovanja za fizične osebe. Literature, člankov je veliko vendar le ti niso napisani za laike, zaradi tega se ljudje odločajo za postavitve s strani podjetij.

Sistem tehničnega varovanja je priporočljiv in uporaben z vidika varnosti. Saj se vlomilci redkeje odločajo za vlome v objekte, ki so zavarovani z video nadzornimi sistemi, kar so pokazale raziskave v tujini. Celovita študija petletne statistike, ki so jo izvedli raziskovalci na

Univerzi za kazensko pravosodje Univerze Rutgers (SCJ) v Newarku, je pokazala, da stanovanjski protivlomni sistemi zmanjšujejo kriminal. Medtem ko so druge študije pokazale da se večina vlomilcev izogiba alarmnim sistemom, je to prva študija, ki se osredotoča na alarmne sisteme, hkrati pa znanstveno izključuje druge dejavnike, ki bi lahko vplivali na stopnjo kriminala (Lee, 2009).

V primeru, da pride do vloma še vedno imamo možnost, da je vlomilca posnela nadzorna video kamera in lahko video posnetek posredujemo policiji, ki primer raziskuje.

»Kljub manjši dejavnosti organiziranih kriminalnih skupin, ki izvajajo vlome in rope, je policija zaznala tuje organizirane skupine, ki so v Sloveniji izvajale premoženjska kazniva dejanja – od vlomov v stanovanja do vlomov v poslovne prostore« (Policija, 2020, str. 27).

Kaznivih dejanj zoper premoženje in sicer velikih tatvin je bilo leta 2020 na območju Slovenije 9039 in vse od leta 2016 upada (Policija, 2020).

Varovanje delimo na tri glavna področja, ki so »fizično varovanje (varovanje oseb, ljudi in premoženja…), tehnično varovanje (sistemi in oprema tehničnega varovanja – kamere, senzorji…) in kombinacijo fizičnega in tehničnega varovanja, ki je tudi najbolj učinkovita« (Koščak, 2017).

Avtomatiziran video nadzor je pomembno raziskovalno področje tudi v komercialnem sektorju. Tehnologija je dosegla stopnjo, ko je montaža kamer za snemanje video posnetkov poceni, ampak najti razpoložljive človeške vire, da bi sedeli in gledali posnetke je drago. Nadzorne kamere so že razširjene v komercialnih ustanovah, pri čemer se izhod kamere snema na trdi disk, ki se občasno prepišejo ali shranijo v video arhivu. Ko se zgodi zločin, na primer je vlomljeno v stanovanje, hišo ali trgovino, se lahko preiskovalci vrnejo po dogodku, da bi videli kaj se je zgodilo, vendar je takrat že prepozno. Potreben je 24 urni nadzor in analiza videa da opozori varnostnika ali lastnika, da je vlom v teku ali opozori na sumljivega posameznika, ki si ogleduje potencialen objekt za vlom in so možnosti za izogib kaznivega dejanja še odprte (Burt, Collins, Duggins, Enomoto, Fuyiyoshi, Hasegawa, Kanade, Lipton, Tolliver, Tsin, 2020).

V primeru, da želimo privarčevati nekaj denarja, se postavitve tehničnega sistema lotimo sami, vendar se pojavi vprašanje kje začeti. Zaradi tega smo se odločili da bomo primer postavitve sistema preizkusili sami. Postopek bomo predstavili in opisali kar se da

razumljivo in enostavno primerno za uporabo ljudi z malo znanja, ki bi želeli postaviti sistem tehničnega varovanja. Uporabili smo kavzalno-eksperimentalno metodo.

Pri izdelavi diplomskega dela smo dobili odgovora na hipotezi, ki smo si ju zastavili za namen pisanja diplomskega dela:

1. Sistem tehničnega varovanja z opremo nižjega cenovnega razreda, postavljen v lastni režiji je učinkovit način zaščite premoženja pred morebitnimi vlomilci.
2. Objekti varovani z video nadzorom niso tarča vlomilcev.

Raziskovali smo določen primer postavitve sistema tehničnega varovanja in pri tem uporabili tehnično opremo in aplikacije.

Uporabili smo računalniški program DEXi, ki je program za odločanje z več atributi. Namenjen je razvoju kakovostnih modelov odločanja z več atributi in oceni možnosti različnih končnih rezultatov. To je uporabno za podporo kompleksnim nalogam odločanja, kjer je treba iz nabora možnosti izbrati določeno možnost, da bi zadovoljili cilje odločevalca. Model z več atributi je hierarhična struktura, ki predstavlja razgradnjo problema odločanja na podprobleme, ki so manjši, manj zapleteni in jih je mogoče lažje rešiti kot celoten problem. Modeli, ki jih je razvil DEXi, so kakovostni in običajno vsebujejo kakovostne (diskretne) lastnosti. Zaradi tega je DEXi še posebej primeren za rešitev nalog razvrščanja pri odločanju, kjer je treba možnosti umestiti v omejeno število vnaprej določenih kategorij (Bohanec, 2021).

Zaradi več spremenljivk kot so, cena sistema tehničnega varovanja, dobavljivost opreme, zahtevnost uporabe sistema, zahtevnost postavitve sistema in vpliva na našo varnost in ali je naš sistem vredno postaviti ali ne smo preverili s programom Dexi.

2 OPREDELITEV POJMOV

2.1 Usmerjevalnik (router)

Usmerjevalniki so naprave, ki sprejemajo in oddajajo podatke. Na njih se lahko povežemo žično preko kabla ali brezžično preko Wi-Fi povezave. Za brezžično povezavo potrebujemo ime povezave in če je nastavljeno geslo za dostop potrebujemo tudi tega. V primeru odprtega dostopa se nanj lahko poveže kdorkoli. Usmerjevalnik služi tudi kot zaščita, ki jo imenujemo požarni zid (firewall) in je most med svetovnim spletom in krajevnim omrežjem (Divjak, 2019; FRI, 2007).

Usmerjevalniki so skozi leta vse naprednejši, hitrejši in z boljšim dometom signala, saj imamo tudi vse več naprav, ki se povezujejo brezžično na usmerjevalnik ter postajajo dodatno breme. Pomembno je tudi kje postavimo usmerjevalnik, saj z oddaljenostjo od usmerjevalnika signal hitro pada posebej če so vmes stene in še bolj če so vmes stene s cevmi. Ko kupujemo usmerjevalnik se varčevanje ne izplača, saj če bomo imeli povezanih več naprav in bomo želeli močan signal in stabilno povezavo bomo izbirali vsaj v srednjem cenovnem razredu. (Forstnerič, 2020).

Usmerjevalnik, naprava za domače omrežje, je del omrežne strojne opreme, ki omogoča komunikacijo med vašim lokalnim domačim omrežjem, kot so vaši osebni računalniki in druge povezane naprave in internetom. Usmerjevalnik je prva varnostna linija pred vdorom v omrežje. Če omogočite najvišjo raven varnosti na usmerjevalniku, kot je požarni zid, in je najboljši način za zaščito vašega računalniškega sistema in informacij pred napadi. Večina usmerjevalnikov se poveže z drugimi omrežnimi napravami samo z omrežnimi kabli in ne zahteva gonilnikov za delovanje v sistemu Windows ali drugih operacijskih sistemih. Vendar pa usmerjevalniki, ki se povežejo z računalnikom z omrežnim kablom, običajno zahtevajo pravilno delovanje gonilnikov. Večino usmerjevalnikov izdelujejo podjetja, kot so Linksys, 3Com, Belkin, D-Link, Motorola, TRENDnet in Cisco, vendar obstaja še veliko drugih. Usmerjevalniki so različnih oblik in velikosti. Usmerjevalniki povezujejo modem, na primer optični, kabelski z drugimi napravami, da omogočijo komunikacijo med temi napravami in internetom. Večina usmerjevalnikov, vključno z brezžičnimi, ima običajno več omrežnih

vrat za istočasno povezovanje številnih naprav z internetom. Usmerjevalnik se običajno prek omrežnega kabla fizično poveže z modemom prek interneta ali vrat WAN in nato fizično, spet prek omrežnega kabla, na kartico omrežnega vmesnika v vseh žičnih omrežnih napravah, ki jih imate. Brezžični usmerjevalnik se lahko z različnimi brezžičnimi standardi poveže z napravami, ki podpirajo tudi določen standard. Naslov IP, dodeljen WAN ali internetni povezavi, je javni naslov IP. Naslov IP, dodeljen lokalni omrežni povezavi, je zasebni naslov IP. Zasebni naslov IP, ki je dodeljen usmerjevalniku, je običajno privzeti prehod za različne naprave v omrežju. Brezžični usmerjevalniki in žični usmerjevalniki z več povezavami delujejo tudi kot preprosta omrežna stikala, ki napravam omogočajo medsebojno komunikacijo. Na primer, več računalnikov, povezanih z usmerjevalnikom, je mogoče konfigurirati za izmenjavo datotek in tiskalnikov med seboj. Usmerjevalniki so kot majhni računalniki za obravnavo dohodnih in odhodnih podatkov. Na usmerjevalnik je mogoče naložiti različno programsko opremo, podobno kot operacijski sistem v računalniku. Pred nakupom usmerjevalnika je potrebno razmisliti o številnih stvareh, na primer o tem, kako hiter mora biti, da podpira hitrost in naprave interneta, ter o njegovi moči, da lahko vse naprave dobijo dostop do interneta. Na primer, pri nakupu usmerjevalnika Wi-Fi, ki bo služil številnim napravam, kot so igralne konzole, računalniki, tablični računalniki in telefoni. V primeru manjše hiše, bo najverjetneje zadostoval en usmerjevalnik, medtem ko bi bili večji domovi ali podjetja z več sobami bolje opremljeni z mrežnim omrežjem z ojačevalcem Wi-Fi (Fisher, 2021).

2.2 Brezžično omrežje (Wi-Fi)

Brezžični telefoni so brezžične naprave, prav tako daljinski upravljalniki televizije, radijski sprejemniki in sistemi GPS. Druge brezžične naprave vključujejo telefone, tablične računalnike, brezžične usmerjevalnike in večino naprav, ki za prenos informacij ne uporabljajo žic. Brezžični polnilci so druga vrsta brezžičnih naprav. Čeprav se prek brezžičnega polnilnika ne pošiljajo nobeni podatki, je v interakciji z drugo napravo (na primer telefonom) brez uporabe žic. Pod pojem brezžični sodijo tudi omrežne tehnologije, ki povezujejo več računalnikov in naprav brez žic, na primer brezžično lokalno omrežje

(WLAN). Pogosto se te naprave imenujejo z vseobsegajočim izrazom Wi-Fi, ki je zaščiten z blagovno znamko Wi-Fi Alliance. Brezžično omrežje, poznano pod kratico Wi-Fi, je bilo ustanovljeno leta 1999 s strani šest podjetij in prenaša podatke po zraku namesto po žicah. Omogoča povezavo med različnimi napravami kot so računalniki, mobilni telefoni, tablice, kamere in tiskalniki, ter omogoča dostop do spleta. Za delovanje Wi-Fi potrebujemo oddajnik, ki oddaja Wi-Fi signal in sprejemnik. Primer takšne naprave je usmerjevalnik. Brezžično omrežje je enostavno za uporabo in ga ima večina naprav že tovarniško vgrajenega. Uporabno je za dostop do spleta, saj ne potrebujemo kablov za povezavo, povezava namreč poteka brezžično. Je najpogosteje uporabljena brezžična komunikacijska tehnologija. Narašča z več kot 4 milijardami naprav letno in 16 milijardami naprav v uporabi. Tehnologija Wi-Fi, ki temelji na brezžičnem omrežju, se nenehno izboljšuje in prinaša večje hitrosti, nižje zakasnitve in boljše uporabniške izkušnje z različnimi vrstami naprav (Uy, 2021; Wi-Fi Alliance, 2021).

Wi-Fi ponuja eno od več tehnologij brezžičnega omrežja, ki računalnikom in drugim napravam omogoča, da se povežejo med seboj v lokalnem omrežju in v internet brez žic in kablov. Z Bluetoothom je Wi-Fi dejansko standard za brezžična omrežja. Največja prednost Wi-Fi je prenosljivost, ki jo ponuja ljudem, ki uporabljajo prenosne računalnike in ročne naprave, kot so pametni telefoni in dlančniki, ter lahko preklapljajo iz enega omrežja v drugo brez skrbi glede žic, nove naprave pa se lahko pridružijo omrežju brez izrecnega dovoljenja skrbnika omrežja, če naprava vsebuje pravilne poverilnice za geslo. Wi-Fi ima eno resno omejitev. Ker gre za tehnologijo LAN, Wi-Fi ponuja omejen doseg povezave, običajno 18 metrov ali manj, odvisno od ovir med napravo in usmerjevalnikom. Antena Wi-Fi pošilja valove povsod okoli sebe v krogli. Signali Wi-Fi izgubljajo intenzivnost, ko se oddaljujejo od antene, zato se kakovost povezave zmanjšuje, ko sta računalnik ali naprava oddaljena od vira. Aplikacije za upravljanje povezave Wi-Fi v računalnikih in drugih napravah pogosto označujejo stopnje za ocenjevanje moči povezave: odlično, dobro ali slabo. Ker se signali Wi-Fi priklopijo na usmerjevalnik, lahko vsak usmerjevalnik priključite v domače omrežje. Večina sodobnih modemov vključuje vgrajen usmerjevalnik. Za starejša okolja, ki ponujajo samo ožičene povezave, priključitev usmerjevalnika v povezavo in nato zagon čarovnika za nastavitev usmerjevalnika običajno deluje v redu. Naprava mora

vključevati potrebne radijske postaje za uporabo povezav Wi-Fi. Vsak sodoben prenosni računalnik in pametni telefon podpirata Wi-Fi, nekatere vrste namiznih računalnikov pa morda ne, vendar so tudi te naprave razširljive prek sprejemnikov USB (Unuth, 2020).

2.3 Internet Protokol (IP)

Internetni protokol (IP) se nanaša na niz pravil, ki urejajo način prenosa podatkovnih paketov po omrežju. Internet protokol je niz specifikacij, ki standardizirajo delovanje stvari v napravah, povezanih z internetom. Ko je internetni protokol postavljen v kontekst omrežne komunikacije, opisuje, kako se podatkovni paketi premikajo po omrežju. Protokol zagotavlja, da vse naprave v omrežju (ali v svetu, ko gre za internet), pa naj bodo še tako različni, govorijo isti "jezik". Protokol IP standardizira način, kako naprave po internetu ali katerem koli omrežju IP posredujejo ali usmerjajo svoje pakete glede na njihove naslove IP. Poleg naslavljanja je usmerjanje ena glavnih funkcij protokola IP. Usmerjanje je sestavljeno iz posredovanja paketov IP od izvornih do ciljnih strojev po omrežju na podlagi njihovih naslovov IP. Ta prenos običajno poteka prek usmerjevalnika. Usmerjevalnik uporablja ciljni naslov IP za določitev naslednjega cilja prek vrste usmerjevalnikov. Naslovi IP so za mnoge uporabnike računalnikov morda najbolj zanimiv in skrivnosten del IP. Naslov IP je edinstven nabor številk, ki identificira stroj v omrežju, ne glede na to, ali gre za računalnik, strežnik, elektronsko napravo, usmerjevalnik, telefon ali drugo napravo. Naslov IP je bistven za usmerjanje in posredovanje paketov IP od vira do cilja. Brez naslovov IP internet ne bi vedel, kam poslati e-pošto in druge podatke. Najpogostejša vrsta naslova IP je naslov iPv4 (za različico 4 tehnologije IP). Njegovo 32-bitno naslavljanje ponuja približno 4,3 milijarde naslovov IP, vendar je s širjenjem mobilnih naprav in drugih naprav povezanih na internet bilo potrebno več naslovov IP. Uvedena je bila nova vrsta naslova IP, iPv6, ki s svojim 128-bitnim naslavljanjem zagotavlja toliko naslovov, da teoretično nikoli več ne bomo potrebovali novih.

2.4 Senzor za okna in vrata

Senzorji oken so potrebni za celovite sisteme za zaščito doma. Senzorji oken delujejo tako da, stikalo in magnet pritrjena na okenski okvir in podokno in dokler okno ostane zaprto, magnet ohrani stik stikala nedotaknjen. Pri odprtju okna se magnet potegne stran od stikala, se odpre vezje, ki pošlje signal na nadzorno ploščo, da oglasi alarm. Tehnologija senzorjev za okna je razmeroma preprosta in so zanesljive varnostne naprave, ki se lahko preprosto namestijo. Ločimo žične in brezžične senzorje oken. Večina senzorjev za okna, tako kot senzorji za vrata, je sestavljena iz magnetov in trstičnih stikal. Trstična stikala se običajno uporabljajo v vsakodnevnih gospodinjskih predmetih. Trstično stikalo z majhnim vezjem v notranjosti sedi na okvirju okna, magnet pa se pritrdi na steklo, tik ob stikalu. Magnet drži kovinske kontakte stikala skupaj in ko je okno zaprto električni tok teče v neprekinjeni zanki. Pri odprtju okna se ta dva dela ločita in električni tok preneha teči ter vezje se izklopi. Senzor nato signalizira varnostno nadzorno ploščo in sproži alarm. Senzorji vrat so bistvena sestavina domačega varnostnega sistema. Sporočijo, ko nekdo vstopi v naš dom. Te naprave so sestavljene iz dveh delov, ki tvorijo vezje, ko sta med seboj vzporedna. Pri odprtju vrat, se oba dela ločita in prekineta vezje, zaradi česar nadzorna plošča sproži alarm. Ker so senzorji vrat enostavni za namestitev, je te koristne pripomočke enostavno jemati kot nekaj samoumevnega. Čeprav obstaja več različnih vrst in stilov senzorjev za vrata, večina uporablja trstično stikalo in magnet, da ugotovi, kdaj so vrata odprta ali zaprta. Trstična stikala se uporabljajo v neštetih napravah, od zvoncev do prenosnih računalnikov in se opirajo na niz električnih priključkov. Stikalo je zaprto, ko sta oba dela blizu drug drugega in lahko teče električni tok. Ko se stikalo odpre, se oba dela ločita, kar povzroči ustavitev električnega toka in izklop tokokroga. En kos je pritrjen na okvir vrat, drugi pa vzporedno s prvim kosom na samih vratih. Oba dela ustvarita zaprt krog, ko so vrata zaprta. Ko se vrata odprejo, se magnet in stikalo ločita in prekineta vezje. Ko se vezje prekine, senzor signalizira osrednjo nadzorno ploščo. Glede na varnostni sistem se lahko prilagodi vrsto opozorila, ki ga prejmemo ob odpiranju vrat. Izberemo lahko, da se ob odpiranju vrat oglasi zvočni alarm, ali pa raje, da se alarm sproži tiho, medtem ko opozori varnostno podjetje in nas obvesti o možni kršitvi. Noben senzor vrat ne traja večno. Senzor se lahko poškoduje, stikalo se lahko obrabi in brezžičnim senzorjem sčasoma zmanjka baterij. Če senzor vrat sproži lažne alarme ali ne deluje pravilno, ga je potrebno nemudoma zamenjati (Tholen, 2021).

3 PREDSTAVLJENA OPREMA KI SMO JO UPORABILI

3.1 Kamera DG-BM01

Kamera proizvajalca Digoo z resolucijo 1280*720, kamera ima nočni vid, možnost alarmov, mikrofon in zvočnik. Kamera ima možnost shranjevanja slik in videoposnetkov na spominsko kartico ali shranjevanje v oblaku. Kamero dodamo v aplikaciji YCC365 Plus in podpira možnost povezave preko računalnika z operacijskim sistemom Windows ter deluje preko Wi-Fi povezave. Kamero smo kupili preko spletne strani www.banggood.com in zanjo odšteli 17 Eur. V paketu smo dobili kamero Digoo DG-BM01 z navodili, osnovni nosilec za kamero, vijake za pritrditev in USB kabel. Kamera je plastična in je bele barve.

Slika 3-1 kamera DG-BM01

3.2 Kamera DG-K2

Kamera proizvajalca Digoo ima resolucijo 1920*1080, ima možnost nočni pogled, alarme, mikrofon in zvočnik. Kamera ima možnost shranjevanja slik in videoposnetkov na spominsko kartico ali shranjevanje v oblaku. Doda se v aplikaciji DigooLife in ne podpira možnosti povezave preko računalnika z operacijskim sistemom Windows in deluje z Wi-Fi povezavo. Kamero smo kupili na spletni strani www.banggood.com in zanjo odšteli 24 Eur.

V paketu smo dobili kamero Digoo DG-K2 z navodili, USB kabel, električni polnilec, osnovni nosilec za kamero in vijake za pritrditev. Kamera je plastična in je bele barve.

Slika 3-2 kamera DG-K2

3.3 Senzor za vrata in okna DG-ZXD21

Senzor za okna in vrata proizvajalca Digoo, deluje z Wi-Fi omrežjem in se poveže v aplikaciji DigooLife. Ima možnost alarmov, ne podpira možnosti povezave z računalnikom. Senzor smo kupili preko spletne strani www.banggood.com in zanj odšteli 12 Eur, kupili smo dva kompleta. V paketu smo dobili senzor Digoo DG-ZXD21 z navodili in lepilnim trakom za

pritrditev na poljubno mesto. Senzor je plastičen je bele barve in je sestavljen iz dveh delov glavne enote v katero se vstavijo baterije za delovanje ter dodatne enote.

Slika 3-3 senzor DG-ZXD21

3.4 Usmerjevalnik Calix T077G

Usmerjevalnik (router) proizvajalca Calix je dostavil ponudnik internetnih storitev Telemach Slovenija. Uporabimo lahko poljuben usmerjevalnik in privzete nastavitve, druge

spremembe niso potrebne. Uporabljamo Wi-Fi omrežje usmerjevalnika za povezavo med napravami.

Slika 3-4 usmerjevalnik Calix T077G

3.5 Ojačevalec signala Wi-Fi mesh

Uporabili smo ojačevalec Wi-Fi signala znamke AirTies, ki smo ga naročili pri ponudniku internetnih storitev Telemach. Za delovanje kamer ni nujno potreben, je pa priporočljivo imeti ojačevalec signala, če potrebujete boljšo pokritost signala Wi-Fi.

Slika 3-5 ojačevalec signala AirTies

4 POSTAVITEV SISTEMA TEHNIČNEGA VAROVANJA

4.1 Zakonodaja

Zakon, ki ureja področje snemanja je zapisan v Zakon o varstvu osebnih podatkov. Za fizične osebe velja izjema pri uporabi tega zakona in sicer 7. člen 1. odstavek ki govori »Ta zakon se ne uporablja za obdelavo osebnih podatkov, ki jo izvajajo posamezniki izključno za osebno uporabo, družinsko življenje ali za druge domače potrebe«(ZVOP-1, 2020).
Splošne določbe so zapisane v 74. členu, za videonadzor v večstanovanjskih stavbah pa je opredeljen v 76. členu.
Splošne kršitve določb tega zakona so zapisane v 91. členu in sicer za nas pride v poštev četrti odstavek, ter 95. člen četrti odstavek.
Kršitev določb o videonadzoru pri večstanovanjskih stavbah je definiran v 97. členu (ZVOP-1, 2020).

4.2 Omrežje

Poznamo različna omrežja kot so električna, telefonska, radijska, televizijska, satelitska in računalniška. Računalniško omrežje lahko imenujemo, kjer sta povezani vsaj dve enoti in si med seboj izmenjujeta podatke.
Razumevanje omrežja je temeljni del konfiguriranja zapletenih okolij na internetu. To ima posledice pri učinkovitem komuniciranju med strežniki, razvoju varnih omrežij in jih imeti organizirana (Ellingwood, 2021).
Omrežje ima lahko precej široko definicijo. Najenostavnejša definicija omrežja je da, vedno vključuje dva ali več računalnikov, ki sta fizično povezana s kabli ali preko povezave Wi-Fi. Ko so računalniki povezani, lahko le-ti delijo svoje vire, datoteke ali internetno povezavo, ne da bi se ob vsaki priložnosti ročno povezali. Ko gre za velikost, so omrežja veliko bolj zapletena. Družinski dom bi lahko imel na primer omrežje, sestavljeno iz dveh domačih računalnikov in povezave Wi-Fi, ki jo družina uporablja za različne dodatne naprave, kot so

pametni televizor, pametna tablica, pametni telefon in drugi. Lahko pa ima poslovna stavba obsežno omrežje s tisoči računalnikov, ki so fizično povezani z mrežnimi kabli. Nekatera omrežja se lahko celo razširijo na velika geografska območja. Verjetno je edino omrežje, s katerim se boste zavestno srečevali vsak dan, domače omrežje, imenovano tudi lokalno omrežje (LAN). Če imamo samo en računalnik in nimamo drugih naprav, s katerimi želimo dostopati do spleta ali deliti virov, domače omrežje ni potrebno. Vendar ima dan danes večina ljudi lastno nastavitev lokalnega omrežja (LAN) doma z več napravami ki so povezana. Pomembno je vedeti, ali je za naš dom najboljše žično ali brezžično omrežje oziroma kombinacija obojega, ter razumeti, kako pravilno nastaviti domače omrežje (Allen, 2021).

Primer omrežja je povezava med usmerjevalnikom in kamero. Poznamo strojno in programsko izmenjavo podatkov. V strojni izmenjavi podatkov sta povezani dve napravi, npr. usmerjevalnik in senzor, v programski izmenjavi podatkov pa dva programa npr. aplikacija na mobilnem telefonu in program na računalniku. Hitrejše kot je omrežje, hitreje poteka izmenjava podatkov. Poznamo brezžična omrežja npr. Wi-Fi in žična omrežja, ki so povezana z kablom. Hitrosti računalniških omrežij so različne in so odvisne od našega ponudnika internetnih storitev in izbranega paketa, ter od naše strojne opreme. Večja kot je oddaljenost od usmerjevalnika, ki oddaja Wi-Fi povezavo počasnejša bo hitrost omrežja. Da povečamo učinkovitost povezave se lahko odločimo za ojačevalce signala kot smo storili v našem primeru.

Zaradi lažje prepoznave omrežja jih poimenujemo in zaradi večje varnosti lahko omrežja zaščitimo z geslom. Omrežja lahko tudi delimo z drugimi uporabniki in vsak ki je seznanjen z omrežjem in geslom se lahko nanj poveže. Kamere in senzorje lahko torej povežemo v omrežje in do njih lahko dostopajo osebe, ki smo jim dodelili dostop. Omrežja so omejena glede na hitrost podatkov, ki se lahko po njih pretakajo in do katerih lahko dostopamo. Tehnologija se tako hitro razvija, da imamo vsakih nekaj let zelo velike spremembe in novosti. Primer je mobilno omrežje LTE/4G Telekoma Slovenija, ki dosega visoke hitrosti in teoretično znaša do 150 Mb/s v smeri k uporabniku in do 50 Mb/s iz smeri uporabnika od leta 2013. V letu 2017 so pričeli z uporabo mobilnega omrežja 4G+ ki teoretično znaša hitrost do 300 Mbit/s v smeri do uporabnika in do 50 Mbit/s v smeri od uporabnika. Od leta

2020 se uporablja novo omrežje 5G Telekoma Slovenije s teoretično hitrostjo do 1500 Mb/s v smeri k uporabniku in do 300 Mb/s iz smeri uporabnika (Breščak, n. d.; FRI, 2007; Telekom Slovenije, 2021).

4.2.1 LAN omrežje

Lokalno ali krajevno omrežje LAN (Local Area network), je sistem ki lahko poveže med seboj več računalnikov, ki so v bližini in so povezani med seboj s kablom. Lan omrežje je bilo med prvimi uporabljeno na univerzah že v letih 1960 in običajno se uporabljajo v podjetjih in število povezanih računalnikov v teoriji ni omejeno. Prednosti so v hitrem odzivnem času, enostavni povezljivosti v omrežje, zanesljivem delovanju in varnosti. Ta računalniška omrežja so bila uporabljena za katalogiziranje knjižničnih zbirk, načrtovanje pouka, beleženje ocen študentov in skupno rabo virov opreme. Chase Manhattan Bank v New Yorku je bila prva komercialna uporaba te nove tehnologije. Do zgodnjih osemdesetih let je imelo veliko podjetij lokalno omrežje sestavljeno iz več sto računalnikov, ki so delili tiskalnike in datoteke za shranjevanje na enem mestu. Lokalna omrežja so na voljo v različnih velikostih. Skupina naprav, povezanih prek domače internetne povezave, je lokalno omrežje. Mala podjetja imajo lokalna omrežja, ki povezujejo tudi sto računalnikov s tiskalniki in shrambo datotek. Največja lokalna omrežja nadzoruje strežnik, ki shranjuje datoteke, deli podatke med napravami in jih usmerja v tiskalnike in skenerje. Lokalno omrežje se od drugih vrst računalniških omrežij na primer interneta razlikuje po tem, da so naprave povezane z lokalnim omrežjem, v isti zgradbi, kot so dom, šola ali pisarna. Ti računalniki, tiskalniki, optični bralniki in druge naprave se povežejo z usmerjevalnikom z mrežnim kablom ali preko brezžičnega usmerjevalnika in dostopne točke Wi-Fi. Obstajata dve vrsti lokalnega omrežja to sta odjemalska/strežniška in enakovredna. Odjemalska/strežniška omrežja so sestavljena iz več naprav (odjemalcev), povezanih z osrednjim strežnikom. Strežnik upravlja shranjevanje datotek, dostop do tiskalnika in omrežni promet. Odjemalec je lahko osebni računalnik, tablični računalnik ali druge naprave, ki izvajajo aplikacije. Odjemalci se s strežnikom povežejo bodisi s kabli bodisi prek brezžične povezave. Omrežja enakovrednih omrežij nimajo osrednjega strežnika in ne

zmorejo velikih obremenitev, kot je odjemalec/strežnik. V omrežju enakovrednega omrežja imata vsak osebni računalnik in naprava enako vlogo pri upravljanju omrežja. Naprave si prek žične ali brezžične povezave z usmerjevalnikom delijo vire in podatke. Večina domačih omrežij je enakovrednih. Domače lokalno omrežje je odličen način za vzpostavitev povezave med vsemi napravami v vašem domu, vključno z osebnimi računalniki, prenosnimi računalniki, tabličnimi računalniki, pametnimi telefoni, tiskalniki in igralnimi napravami. Ko so vaše naprave povezane z omrežjem Wi-Fi, lahko zasebno delite datoteke z družinskimi člani, brezžično tiskate iz katere koli naprave in dostopate do podatkov v drugih povezanih napravah. Domače lokalno omrežje je mogoče razširiti tudi na domače varnostne sisteme, pametne televizorje, kontrole domačega okolja in pametne kuhinjske naprave. Ko te sisteme dodate v lokalno omrežje, lahko vsak sistem upravljate s katere koli naprave in lokacije v vašem domu (Whitehead, 2020).

4.2.2 WLAN omrežje

Brezžično krajevno ali lokalno omrežje WLAN (Wireless local area network) omogoča brezžično omrežno komunikacijo na kratke razdalje z uporabo radijskih ali infrardečih signalov namesto tradicionalnih omrežnih kablov. Brezžično lokalno omrežje je mogoče zgraditi z uporabo katerega koli od več različnih protokolov brezžičnega omrežja, najpogosteje Wi-Fi ali Bluetooth. Varnost omrežja ostaja pomembno vprašanje za omrežja WLAN. Brezžičnim odjemalcem se običajno preveri njihova identiteta, to je proces imenovan preverjanje pristnosti, ko se le-ti pridružijo brezžični povezavi. Tehnologije, kot je WPA, dvigujejo raven varnosti v brezžičnih omrežjih, da bi se ujemale s tradicionalnimi žičnimi omrežji. Prednosti WLAN omrežja so, da podpirajo veliko število naprav. Sama postavitev WLAN je lažja kot polaganje kablov za žično povezavo in tudi dostop do WLAN je lažji kot dostop do žičnega omrežja. Zato so razširjeni na odprtih prostorih izven domov in podjetij. Slabosti WLAN omrežja so, da je enostavneje vdreti v povezavo in zato je pomembno šifriranje brezžične povezave. Možne so brezžične motnje, ki lahko ogrozijo hitrost in stabilnost brezžičnega omrežja. Za razširitev brezžičnega omrežja je potrebno več brezžičnih naprav kot so ojačevalci signala. WLAN lahko vsebuje le dve napravi ali mnogo

več le-teh. Z vse večjim številom naprav je upravljanje brezžičnih omrežij vse težje. Brezžična lokalna omrežja lahko vsebujejo številne vrste naprav med drugim mobilne telefone, prenosne in tablične računalnike, internetne avdio sisteme, igralne konzole ter druge gospodinjske aparate in naprave, ki podpirajo internet. Povezave WLAN delujejo z radijskimi oddajniki in sprejemniki vgrajenimi v odjemalske naprave. Brezžična omrežja ne zahtevajo kablov, vendar se za njihovo izdelavo običajno uporablja več naprav za posebne namene, ki imajo tudi lastne vgrajene sprejemne antene. Lokalna omrežja Wi-Fi so na primer lahko zgrajena v enem od dveh načinov: ad-hoc ali infrastrukturni. Omrežja WLAN v ad-hoc načinu so sestavljena iz neposrednih povezav med odjemalci brez vmesnih komponent strojne opreme. Ad-hoc lokalna omrežja se lahko v nekaterih situacijah uporabijo za vzpostavitev začasnih povezav, vendar le-te ne podpirajo več kot nekaj naprav in lahko predstavljajo varnostno tveganje. Infrastrukturni način Wi-Fi WLAN uporablja osrednjo napravo, imenovano brezžična dostopna točka (AP), na katero se povežejo vsi uporabniki. V domačih omrežjih brezžični širokopasovni usmerjevalniki opravljajo funkcije dostopne točke in omogočajo WLAN za domači dostop do interneta. Več dostopnih točk je mogoče povezati med seboj v eno večjo WLAN omrežje. Nekatera brezžična omrežja LAN razširjajo obstoječe žično omrežje. Ta vrsta omrežja WLAN je zgrajena tako, da na rob žičnega omrežja pritrdite dostopno točko in nastavite dostopno točko za delovanje v premostitvenem načinu. Odjemalci komunicirajo z dostopno točko prek brezžične povezave in lahko dostopajo do omrežja skozi dostopno točko (Mitchell, 2020).

4.2.3 WAN omrežje

Prostrano omrežje ali široko pasovno omrežje WAN (Wide Area Network) obsega veliko geografsko območje, na primer mesto, občino ali državo. Lahko je privatno za povezovanje podjetij ali pa javno za povezovanje manjših omrežij. Najlažje je razumeti WAN, če pomislite na internet, največji WAN na svetu. Internet je WAN, ker z uporabo ponudnikov internetnih storitev povezuje številna manjša lokalna omrežja. V manjšem obsegu ima lahko podjetje WAN, ki ga sestavljajo storitve v oblaku, njegov sedež in podružnice. WAN v tem primeru povezuje te dele poslovanja. Ne glede na to, kako je omrežje WAN združeno ali kako

oddaljena so omrežja, rezultat omogoča komunikacijo manjšim omrežjem iz različnih lokacij. Ker omrežja WAN po definiciji pokrivajo večjo razdaljo od omrežij LAN, je smiselno povezati različne dele omrežja WAN z uporabo navideznega zasebnega omrežja. Ta okvir ščiti komunikacijo med spletnimi mesti. Čeprav virtualna zasebna omrežja zagotavljajo razumno raven varnosti za poslovne namene, javna internetna povezava ne zagotavlja vedno predvidljivih ravni zmogljivosti, ki jih zagotavlja namenska povezava WAN. Zato se optični kabli včasih uporabljajo za olajšanje komunikacije med povezavami WAN. Mnoga podjetja so začela uporabljati zakupljena omrežja WAN sredi devetdesetih let, ko sta splet in internet porasla. Mrežne povezave na daljših razdaljah se lahko uporabijo tudi za izgradnjo namenskih širokopasovnih omrežij. Čeprav so dražji od internetnih virtualnih zasebnih omrežij, zasebni mrežni WAN ponujajo visoko zmogljivost. Omrežja WAN so dražja od domačih ali korporativnih intranetov. Omrežja WAN, ki prečkajo mednarodne in druge teritorialne meje, spadajo v različne pravne jurisdikcije. Med vladami se lahko pojavijo spori glede lastninskih pravic in omejitev uporabe omrežja. Globalna omrežja WAN za komunikacijo po celinah zahtevajo uporabo podvodnih omrežnih kablov. Podvodni kabli so predmet sabotaže in nenamernih potopov ladij in vremenskih razmer. V primerjavi s podzemnimi fiksnimi telefonskimi kabli, podvodni kabli držijo dlje vendar so njihova popravila dražja (Allen, 2021; Mitchell, 2021).

4.2.4 Mesh omrežje

Namesto, da se zanašamo na en usmerjevalnik, mrežno omrežje uporablja več usmerjevalnikov za enakomernejšo porazdelitev brezžičnega omrežja na večjem območju. Namenjeni so odstranjevanju mrtvih točk, na katere običajno naletimo v velikih domovih, z enim usmerjevalnikom Wi-Fi. Mesh omrežje temelji na nizu mesh usmerjevalnikov, povezanih skupaj. To ni nova tehnologija, mesh omrežja, vojska uporablja od osemdesetih let. Toda prvi mesh usmerjevalniki so postali splošno dostopni za domače in potrošniške kupce z modeli, kot sta Eero in Orbi, od leta 2016. Mesh usmerjevalnik ni ena sama naprava kot tradicionalni usmerjevalnik, v mesh sistemu sta lahko dva, tri ali celo več usmerjevalnikov. Eden od teh usmerjevalnikov je prehod, ki se poveže z internetom,

običajno prek kabelskega modema. Toda vsak mesh usmerjevalnik v sistemu je vozlišče, ki se "pogovarja" med seboj in se obnaša kot primarni usmerjevalnik, ki lahko komunicira z vsemi napravami v dosegu. To omogoča, da sistem mesh usmerjevalnika zakrije velik dom z omrežjem Wi-Fi brez mrtvih točk. Ojačevalec Wi-Fi signala je običajno poceni pripomoček, ki ga priklopimo v del hiše s slabim signalom Wi-Fi, mesh pa vzame obstoječi Wi-Fi in ga ojača ter zapolni bližnje vrzeli v pokritosti. Ojačevalec lahko opravi delo, vendar ima pomanjkljivosti. Ojačevalec ima svoje ime signala, zato je potrebno pri selitvi iz enega dela hiše v drugega spremeniti omrežje Wi-Fi. Vse naprave, ki so odvisne od pravilnega delovanja v istem omrežju, lahko odpovejo, če so povezane v omrežje ojačevalca. Mesh omrežje je zelo drugačno. Vsi mesh usmerjevalniki so enaka vozlišča v našem primarnem omrežju Wi-Fi, zato uporabljajo isto ime signala in sodelujejo pri distribuciji omrežnega prometa za najboljšo možno zmogljivost. Pri nastavitvi mesh omrežja, moramo usmerjevalnike razporediti po celotnem domu tako, da so dovolj blizu drug drugemu, da lahko ostanejo v komunikaciji in izmenjujejo informacije, a vseeno dosežejo najbolj skrajne meje našega tlorisa. Običajno nam lahko pri tem pomaga programska oprema mesh usmerjevalnika. Če imamo tloris, ki je dovolj majhen ali kompakten, da ni mrtvih točk Wi-Fi, zadostuje tradicionalni usmerjevalnik. Mnogi proizvajalci mesh usmerjevalnikov na primer priporočajo svoj izdelek za domove, ki presegajo 600 kvadratnih metrov. Poleg tega bo skoraj vedno bolj priročen in učinkovitejši od ojačevalca Wi-Fi. Ena pomanjkljivost mesh omrežij pa je cena. Mesh usmerjevalni sistem je pogosto bistveno dražji od tradicionalnih usmerjevalnikov. Vendar jih je enostavno nastaviti, povsod v našem domu ponujajo dosleden Wi-Fi in jih je mogoče celo nadgraditi, saj v primeru da imamo mrtve točke, lahko dokupimo novo napravo za podaljšanje signala (Johnson, 2021).

4.2.5 Bluetooth omrežje

Bluetooth je brezžična komunikacijska tehnologija kratkega dosega, ki omogoča napravam, kot so mobilni telefoni, računalniki in zunanje naprave, brezžični prenos podatkov ali glasu na kratki razdalji. Namen Bluetootha je zamenjati kable, ki običajno povezujejo naprave, hkrati pa ohraniti varno komunikacijo med njimi. Ime "Bluetooth" je vzeto po danskem

kralju iz 10. stoletja po imenu Harald Bluetooth, ki naj bi združeval različne, medsebojno nasprotujoče si regionalne frakcije. Tako kot soimenjak tudi tehnologija Bluetooth združuje široko paleto naprav v številnih različnih panogah z enotnim komunikacijskim standardom. Bluetooth, razvit leta 1994, je bil namenjen brezžični zamenjavi kablov. Uporablja isto frekvenco 2,4 GHz kot nekatere druge brezžične tehnologije doma ali v pisarni, na primer brezžični telefoni in usmerjevalniki WiFi. Ustvarja brezžično omrežje polmera 10 metrov, imenovano osebno omrežje (PAN) ali pikonet, ki lahko poveže od dveh do osem naprav. To omrežje kratkega dosega omogoča, da stran, pošljemo tiskalniku v drugo sobo, ne da bi morali napeljati kabel. Bluetooth porabi manj energije in stane manj kot Wi-Fi. Zaradi manjše moči je tudi veliko manj nagnjen k motenju drugih brezžičnih naprav v istem radijskem pasu 2,4 GHz. Domet Bluetooth in hitrost prenosa so običajno nižji od Wi-Fi. Z razvojem tehnologije pa se je hitrost Bluetooth povečala. Specifikacija Bluetooth različica 4.0 je bila uradno sprejeta 6. julija 2010. Funkcije Bluetooth različice 4.0 vključujejo nizko porabo energije, nizke stroške in večji doseg. Značilnost izboljšave specifikacij Bluetooth 4.0 so njene nižje zahteve po porabi energije. Naprave, ki uporabljajo Bluetooth v4.0, so optimizirane za nizko delovanje baterije in lahko delujejo iz majhnih gumbastih baterij, kar odpira nove možnosti za brezžično tehnologijo. Namesto da bi se bali, da bo na primer pri vklopu Bluetootha izpraznjen akumulator našega mobilnega telefona, lahko pustimo mobilni telefon Bluetooth v4.0 ves čas priključen na našo drugo dodatno opremo Bluetooth. Mnoge mobilne naprave imajo vgrajene radijske postaje Bluetooth. Računalnike in nekatere druge naprave, ki nimajo vgrajenih radijskih sprejemnikov, lahko na primer omogočimo z uporabo Bluetooth ključa. Postopek povezovanja dveh naprav Bluetooth se imenuje "seznanjanje". Na splošno naprave oddajajo svojo prisotnost drug drugemu, uporabnik pa izbere napravo Bluetooth, s katero se želi povezati, ko se na njeni napravi prikaže njeno ime ali ID. Ker se naprave, ki podpirajo Bluetooth, množijo, je pomembno, da vemo, kdaj in s katero napravo se povezujemo, zato je morda treba vnesti kodo, ki pomaga zagotoviti, da se povezujemo s pravilno napravo. Ta postopek seznanjanja se lahko razlikuje glede na vpletene naprave. Na primer, povezava naprave Bluetooth z iPadom lahko vključuje različne korake od tistih za povezavo naprave Bluetooth z avtomobilom. Bluetooth ima nekaj pomanjkljivosti. Prvi je, da je to lahko poraba energije akumulatorja za

mobilne brezžične naprave, kot so pametni telefoni, čeprav je ta tehnologija napredovala, je ta problem manj pomemben, kot je bil nekoč. Tudi doseg signala je precej omejen, običajno se razteza le približno 9 metrov. Tako kot pri vseh brezžičnih tehnologijah lahko ovire, kot so stene, tla ali stropi, še dodatno zmanjšajo doseg signala. Postopek seznanjanja je lahko tudi težaven, pogosto odvisen od vpletenih naprav, proizvajalcev in drugih dejavnikov, ki lahko povzročijo frustracije pri poskusu povezovanja. Bluetooth velja za razumno varno brezžično tehnologijo, če se uporablja previdno. Povezave so šifrirane, kar preprečuje naključno prisluškovanje drugih naprav v bližini. Naprave Bluetooth pogosto premikajo radijske frekvence tudi v paru, kar preprečuje enostavni vdor. Naprave ponujajo tudi različne nastavitve, ki uporabniku omogočajo omejevanje povezav Bluetooth. Varnost "zaupanja" napravi Bluetooth na ravni naprave omejuje povezave samo na to posebno napravo. Z varnostnimi nastavitvami na ravni storitve lahko omejimo tudi vrste dejavnosti, ki jih naša naprava sme izvajati med povezavo Bluetooth. Kot pri vsaki brezžični tehnologiji pa vedno obstaja neko varnostno tveganje. Osebe ali skupine ljudi, ki se ukvarjajo z vdori v omrežja so razvili različne zlonamerne napade, ki uporabljajo omrežje Bluetooth. Na primer, "bluesnarfing" se nanaša na napadalca, ki pridobi dovoljen dostop do informacij o napravi prek Bluetootha; "bluebugging" je, ko napadalec prevzame naš mobilni telefon in vse njegove funkcije. Za povprečnega človeka Bluetooth ne predstavlja resnega varnostnega tveganja, če ga uporabljamo z mislijo na varnost in se povežemo samo na znane naprave Bluetooth. Za največjo varnost, medtem ko smo v javnosti ne uporabljajmo Bluetootha in ga izklopimo (Uy, 2020).

Čeprav Bluetooth uporablja enak standardni domet signala kot običajni Wi-Fi, ne more zagotoviti enake ravni brezžične povezave. V primerjavi z Wi-Fi je omrežje Bluetooth počasnejše, bolj omejeno v dosegu in podpira manj enakovrednih naprav. Hkrati lahko povežemo do osem naprav, ki podpirajo Bluetooth. Nekatere naprave Bluetooth pa lahko pridejo do konflikta, če za povezavo uporabljajo isti profil (Mitchell, 2021).

4.2.6 Omrežni kabel

Omrežni kabel se uporablja z žičnimi omrežji. Omrežni kabli povezujejo naprave, kot so osebni računalniki, usmerjevalniki in stikala v lokalnem omrežju. Ti fizični kabli so omejeni z dolžino in vzdržljivostjo. Če je omrežni kabel predolg ali slabe kakovosti, ne bo prenašal dobrega omrežnega signala. Te omejitve so eden od razlogov, da obstajajo različne vrste omrežnih kablov, ki so optimizirani za opravljanje določenih nalog v določenih situacijah. Omrežni kabel je podoben tradicionalnemu telefonskemu kablu, vendar je večji in ima več žic. Oba kabla imata podobno obliko in vtič, vendar ima omrežni kabel osem žic, telefonski kabli pa štiri. Priključki za omrežni kabel so tudi večji. Omrežni kabli so v različnih barvah, vendar so telefonski kabli običajno sivi. Omrežni kabli se priključijo na omrežna vrata, ki so večja od vrat za telefonske kable. Omrežna vrata v računalniku so dostopna prek omrežne kartice na matični plošči. Ta vrata so običajno na hrbtni strani namiznega računalnika ali na strani prenosnika. Omrežni kabli podpirajo enega ali več industrijskih standardov, vključno s kategorijo 5 in kategorijo 6. Večina tehnikov te standarde imenuje CAT5 oziroma CAT6. Zaradi tega številne spletne trgovine, ki prodajajo omrežne kable, uporabljajo tudi ta skrajšani jezik. Omrežni kabli so izdelani v dveh osnovnih oblikah. Trdni omrežni kabli ponujajo nekoliko boljše delovanje in izboljšano zaščito pred električnimi motnjami. Pogosto se uporabljajo tudi v poslovnih omrežjih, pri ožičenju znotraj pisarniških sten ali pod laboratorijskimi tlemi na fiksne lokacije. Standardni omrežni kabli so manj nagnjeni k fizičnim razpokam in prekinitvam, zato so bolj primerni za popotnike ali domače omrežne nastavitve. Enojni omrežni kabel ima največjo zmogljivost razdalje, kar pomeni, da ima kabel zgornjo mejo, koliko časa lahko traja, preden pride do izgube signala (imenovano slabljenje). Do te težave pride, ker električni upor dolgega kabla vpliva na delovanje. Oba konca kabla morata biti dovolj blizu drug drugemu za hiter sprejem signalov in dovolj oddaljena od zunanjih električnih motenj, da se preprečijo prekinitve. Vendar ta previdnostni ukrep ne omejuje velikosti omrežja, saj lahko strojna oprema, kot so usmerjevalniki ali vozlišča, združi več omrežnih kablov v istem omrežju. Ta razdalja med obema napravama se imenuje premer omrežja. Največja dolžina kabla CAT5, preden pride do oslabitve, je 100 m. CAT6 lahko doseže do 213 metrov. Omrežni kabli so lahko daljši,

vendar lahko izgubijo signal, še posebej, v bližini velikih električnih naprav. Brezžična tehnologija, kot sta Wi-Fi in Bluetooth, sta zamenjali omrežne kable v številnih domačih in poslovnih omrežjih. Večina tabličnih računalnikov in drugih mobilnih naprav nima omrežnih vrat. Te brezžične tehnologije so ugodne, če kabel poteka zunaj ali na lokacijah z večjo nevarnostjo poškodb žice (Mitchel, 2021).

4.3 Postavitev opreme

Kamero DG-BM01 smo pritrdili na zunanjo steno s priloženimi vijaki in osnovnim nosilcem. Postavitev je poljubna in se zanjo odločimo glede na območje ki ga želimo pokriti s kamero. Enako smo naredili s kamero DG-K2.
Senzorja DG-ZXD-21 smo pritrdili na okna in vrata in sicer smo enega pritrdili na dvokrilno okno s priloženim lepilnim trakom 3M in drugega na vrata s priloženim lepilnim trakom 3M. Višina kjer pritrdimo senzorje je poljubna paziti moramo le da sta eden zraven drugega.

4.4 Konfiguriranje opreme

Kamero DG-BM01 smo postavili v bližino usmerjevalnika (router) in jo povezali z USB kablom, ki je bil priložen na napajanje. Mobilni telefon z operacijskim sistemom Android smo povezali z Wi-Fi omrežjem in zagnali aplikacijo YCC365 Plus. Aplikacijo YCC365 Plus si lahko naložimo iz aplikacije trgovina play. V kamero smo vstavili spominsko kartico za shranjevanje posnetkov lahko pa uporabimo tudi oblak za shranjevanje vsebine. Za samo delovanje kamere ni potrebno shranjevanje posnetkov. V aplikaciji YCC365 Plus smo se registrirali in ustvarili račun, ki je brezplačen. Ko vstopimo v aplikacijo izberemo ikono +, ki se nahaja v zgornjem desnem kotu zaslona da dodamo napravo. Nato izberemo možnost pametna kamera (Intelligent camera) in opcijo skeniranje kode za dodajanje opreme (Scan code to add). Kamero smo priklopili z USB kablom na napajanje in počakali na pisk kamere. Pisk pomeni da je kamera pripravljena in nato izberemo naprej (Next). V naslednjem meniju, smo napravo povezali z omrežjem Wi-Fi, vpisali uporabniško ime in geslo od Wi-Fi omrežja na katero se želimo povezati in izberemo naprej (Next). Wi-Fi omrežje mora biti

enako na mobilnem telefonu in na kameri, ki jo povezujemo. Na mobilnem zaslonu se nam je prikazala QR koda in smo jo približali kameri na 10-20 cm in po zvočnem signalu kamere pritisnili tipko slišal sem pisk (i heard the beep voice). Nato počakamo 1-2 minuti da se kamera poveže. Po zvočnem signalu je kamera povezana in lahko jo poimenujemo in pritisnemo možnost začnite doživljati (start to experience). Dodatno lahko v aplikaciji izberemo veliko različnih nastavitev.

Na kamero se lahko povežemo preko mobilne aplikacije YCC365 Plus na mobilen telefonu ali preko računalnika z operacijskim sistemom Windows. Na računalniku odpremo poljuben spletni brskalnik in se povežemo na naslov www.ucloudcam.com/login, kjer ustvarimo račun in se vpišemo. Na voljo imamo več opcij, od premikanja kamere do povečave, ki si jih lahko prilagodimo. Imamo tudi možnost dokupa shranjevanje v oblaku kamor lahko nato shranjujemo videoposnetke.

Kamero postavimo na izbrano mesto, v primeru da jo želimo pritrditi na steno, so v kompletu priloženi vijaki.

Kamero DG-K2 smo postavili v bližino usmerjevalnika (router) in jo povezali z USB kablom, ki je bil priložen na napajanje. Mobilni telefon z operacijskim sistemom Android smo povezali z Wi-Fi omrežjem in zaženemo aplikacijo YCC365 Plus. Aplikacijo YCC365 Plus si lahko naložimo iz aplikacije trgovina play. V kamero smo vstavili spominsko kartico za shranjevanje posnetkov, lahko pa uporabimo tudi oblak za shranjevanje vsebine. Za samo delovanje kamere ni potrebno shranjevanje posnetkov. Kamere ni bilo možno dodati v aplikacijo YCC365 Plus, ker ne podpira te možnosti, zaradi česar smo uporabili aplikacijo z imenom DigooLife. DigooLife aplikacijo prav tako naložimo iz aplikacije trgovina play in jo zaženemo. V zgornjem desnem kotu zaslona pritisnemo ikono + da dodamo napravo. Poiščemo ikono pametna kamera (Smart Camera Wi-Fi) in pritisnemo. Nato se prepričamo da na kameri hitro utripa indikator ali slišimo ton na kameri (Make sure the indicator is flashing quickly or a prompt tone is heard) označimo kvadratek da potrdimo in pritisnemo naprej (Next). Mobilni telefon mora biti povezan na enako Wi-Fi omrežje kot bo povezana kamera, nato vpišemo ime Wi-Fi omrežja in geslo ter pritisnemo naprej (Next). Na zaslonu se prikaže QR koda ki jo optično preberemo s kamero iz razdalje 10-15 cm. Ko zaslišimo ton

kamere pritisnemo slišal sem pisk (I Heard a Prompt), počakamo do dve minuti, da se kamera doda, nato jo lahko poimenujemo in izbiramo med različnimi nastavitvami, ki nam jih aplikacija ponuja. Izberemo lahko tudi storitve v oblaku in zakupimo prostor za shranjevanje v oblaku ni pa nujno potrebno za delovanje kamere.

Senzor za vrata in okno z oznako DG-ZXD21 smo postavili v bližino usmerjevalnika (router) vstavili vanj baterijo in ga vklopili. Zagnali smo aplikacijo DigooLife na mobilnem telefonu, nato pritisnemo na ikono + da dodamo napravo, ki se nahaja v zgornjem desnem kotu zaslona. Poiščemo možnost vrata/okna (Door/Window (Wi-Fi)) in nanj kliknemo. Vpišemo podatke na katero brezžično omrežje se želimo povezati in na senzorju pritisnemo in držimo stikalo za nastavitve da začne LED indikator utripati. V aplikaciji potrdimo, da indikator utripa hitro (Confirm indicator is blinking rapidly) in pritisnemo naprej (Next), ter počakamo do dve minuti da se naprava doda. Senzor lahko nato poimenujemo in izbiramo med nastavitvami, da nam javlja alarm v primeru odprtja in zaprtja okna in vrat.
V našem primeru smo postopek ponovili dvakrat, saj smo dodali dva senzorja.

4.5 Preizkušanje delovanja sistema

Po zaključenem konfiguriranju in postavitvi kamer in senzorjev smo preizkusili kako se le-te obnesejo v praksi. Ugotovili smo da ob odpiranju ali zapiranju oken in vrat senzorja delujeta zelo dobro. Že če smo odprli in zaprli okno ali vrata za zelo kratek čas, nam je alarm v aplikaciji DigooLife javil alarm in nam to sporočil. Prav tako ima senzor še eno možnost in sicer ob fizični prestavitvi senzorja na drugo lokacijo, nam je le to tudi javil z alarmom. Če razbijemo steklo na oknu in fizično odstranimo senzor iz okna preden odpremo okno nam le to alarm javi.
Kamere delujejo in so povezane, ter se lahko na njih povežemo in spremljamo dogajanje v živo. Ugotovili smo, da je alarm zelo občutljiv in se sproži že ob premikanju dreves, listja, trave, čeprav bi nam javljal le premike večjih objektov ali ljudi.

5 SISTEM ZA OBVEŠČANJE UPORABNIKA

5.1 Kamera DG-BM01

Za kamero DG-BM01 smo uporabili aplikacijo YCC365 Plus na mobilnem telefonu z operacijskim sistemom Android. V aplikaciji smo v nastavitvah vklopili obvestila (Notice) in v nastavitvah sporočil vklopili detektor gibanja (Motion detection). Nato smo nastavili občutljivost gibanja (Motion sensitivity) na nizko (Low). V tem primeru nas bo aplikacija obvestila ob zaznavi premika večjih objektov ali ljudi. V nastavitvah smo izbrali shranjevanje na spominsko kartico (Memory card management) in shranjevanje posnetkov v primeru sprožitve alarma.

Na računalniku imamo v nastavitvah možnost vklopa pogostost obveščanja (Notification frequency). V tem meniju lahko nastavimo obveščanje ob zaznavi gibanja (Motion detection) in zaznavi zvoka (Sound detection). Nastavimo lahko tudi pogostost obveščanja. Obveščanje, učinkovito deluje na mobilnem telefonu, saj nas aplikacija YCC365 Plus z alarmom opozori na zaznavo gibanja in/ali zvoka. Pri nadzoru kamere preko računalnika pa nam spletni brskalnik ni javil zaznave gibanja in/ali zvoka.

5.2 Kamera DG-K2

Pri kameri DG-K2 smo uporabili aplikacijo DigooLife na mobilnem telefonu z operacijskim sistemom Android. V nastavitvah aplikacije smo izbrali nastavitve alarma za zaznavanje (Detection Alarm Settings) in vklopili možnost detektor alarma za zaznavanje gibanja (Motion Detection Alarm). Sistem za obveščanje učinkovito deluje in nam pošilja opozorilo na mobilni telefon, v primeru da je kamera zaznala gibanje.

5.3 Senzor DG-ZXD21

Obveščanje senzorja ob odpiranju ali zapiranju okna in vrat deluje dobro in na mobilni telefon smo prejeli obvestilo v primeru, da se je okno ali vrata zaprla ali odprla. Učinkovito deluje tudi možnost senzorja, v primeru da je le-ta odstranjen. Opozorilno sporočilo smo prejeli na mobilni telefon preko aplikacije DigooLife.

6 TESTIRANJE HIPOTEZ

Hipoteza številka 1 se je glasila »Sistem tehničnega varovanja z opremo nižjega cenovnega razreda, postavljen v lastni režiji je učinkovit način zaščite premoženja pred morebitnimi vlomilci.

Pri proučevanju smo ugotovili, da je oprema nižjega cenovnega razreda učinkovito vključena v naš sistem zaščite doma. Oprema snema dogajanje v območju, ki ga pokriva video nadzorni sistem in javlja zaznavo gibanja na mobilni telefon. V primeru vloma imamo video posnetek morebitnega storilca in bi ga bilo možno prepoznati.

Na podlagi proučevanja smo hipotezo številko 1, ki se je glasila »Sistem tehničnega varovanja z opremo nižjega cenovnega razreda, postavljen v lastni režiji je učinkovit način zaščite premoženja pred morebitnimi vlomilci« potrdili.

Hipoteza številka 2 se je glasila »Objekti varovani z video nadzorom niso tarča vlomilcev«.

Pri proučevanju smo ugotovili, da so objekti varovani z videonadzorom lahko potencialna tarča vlomilcev.

Na podlagi proučevanja smo hipotezo številko 2, ki se je glasila »Objekti varovani z video nadzorom niso tarča vlomilcev« zavrnili.

7 REZULTATI ANALIZE PROGRAMA DEXI

V nalogi smo se hoteli tudi prepričati ali se postavitev sistema tehničnega varovanja dejansko izplača. Zato smo uporabili program DEXi. V programu DEXi smo vnesli vse spremenljivke (nabavna cena, dobavljivost tehnične opreme, zahtevnost uporabe sistema, zahtevnost postavitve sistema in vpliv na našo varnost) našega sistema za tehnično varovanje, da nam je pomagal pri odločitvi ali je naš sistem tehničnega varovanja vredno postaviti ali ne. Poročilo programa DEXi je naslednje:

7.1 Drevo kriterijev

Kriterij	Opis
Sistem tehničnega varovanja	Ali je vredno imeti sistem tehničnega varovanja
Cena	Nabavna cena
Nabavna cena	
Dobavljivost opreme	Dobavljivost tehnične opreme
Nakup tehnične opreme	Kako zahtevno je kupiti tehnično opremo
Uporaba sistema	Zahtevnost uporabe sistema
Zahtevnost uporabe sistema	Kako zahtevna je uporaba tehničnega sistema
Postavitev sistema	Zahtevnost postavitve sistema
Zahtevnost postavitve sistema	Kako zahtevna je postavitev tehničnega sistema
Varnost	Vpliv na našo varnost
Varnost tehničnega sistema	Kako naš tehnični sistem vpliva na našo varnost

7.2 Zaloge vrednosti

Kriterij	Zaloga vrednosti
Sistem tehničnega varovanja	Ni priporočljivo; priporočljivo
Cena	Ni priporočljivo; priporočljivo
Nabavna cena	Nad 250 eur; do 250 eur
Dobavljivost opreme	Ni priporočljivo; priporočljivo
Nakup tehnične opreme	Zahtevno; enostavno
Uporaba sistema	Ni priporočljivo; priporočljivo
Zahtevnost uporabe sistema	Zahtevno; enostavno
Postavitev sistema	Ni priporočljivo; priporočljivo
Zahtevnost postavitve sistema	Zahtevno; enostavno
Varnost	Ni priporočljivo; priporočljivo
Varnost tehničnega sistema	Brez tehničnega sistema; tehnični sistem, ki vsebuje kameri in senzorja

Sistem tehničnega varovanja
Ali je vredno imeti sistem tehničnega varovanja
1. ni priporočljivo
2. priporočljivo

Cena
Nabavna cena
1. ni priporočljivo
2. priporočljivo

Nabavna cena
1. nad 250 eur
2. do 250 eur

Dobavljivost opreme
Dobavljivost tehnične opreme
1. ni priporočljivo
2. priporočljivo

Nakup tehnične opreme
Kako zahtevno je kupiti tehnično opremo
1. zahtevno
2. enostavno

Uporaba sistema
Zahtevnost uporabe sistema
1. ni priporočljivo
2. priporočljivo

Zahtevnost uporabe sistema
Kako zahtevna je uporaba tehničnega sistema
1. zahtevna
2. enostavna

Postavitev sistema
Zahtevnost postavitve sistema
1. ni priporočljivo
2. priporočljivo

Zahtevnost postavitve sistema
Kako zahtevna je postavitev tehničnega sistema
1. zahtevno
2. enostavno

Varnost
Vpliv na našo varnost
1. ni priporočljivo
2. priporočljivo

Varnost tehničnega sistema
Kako naš tehnični sistem vpliva na našo varnost
1. brez tehničnega sistema
2. tehnični sistem, ki vsebuje kameri in senzorja

7.3 Funkcije

Kriterij	Pravil	Definiranost	Določenost	Vrednosti
Sistem tehničnega varovanja	25/32	78,13%	100,00%	Ni priporočljivo; 24, priporočljivo 8
Cena	2/2	100,00%	100,00%	Ni priporočljivo; 1, priporočljivo 1
Nabavna cena				
Dobavljivost opreme	2/2	100,00%	100,00%	Ni priporočljivo; 1, priporočljivo 1
Nakup tehnične opreme				
Uporaba sistema	2/2	100,00%	100,00%	Ni priporočljivo; 1, priporočljivo 1
Zahtevnost uprabe sistema				
Postavitev sistema	2/2	100,00%	100,00%	Ni priporočljivo; 1, priporočljivo 1
Zahtevnost postavitve sistema				
Varnost	2/2	100,00%	100,00%	Ni priporočljivo; 1, priporočljivo 1
Varnost tehničnega sistema				

7.4 Tabele odločitvenih pravil

Cena	Dobavljivost opreme	Uporaba sistema	Postavitev sistema	Varnost	Sistem tehničnega varovanja
50%	0%	0%	0%	50%	
1. Ni priporočljivo	*	*	*	*	Ni priporočljivo
2. *	*	*	*	*	Ni priporočljivo
3. Priporočljivo	*	*	*	Priporočljivo	Priporočljivo

7.5 Povprečne uteži

Kriterij	Lokalne	Globalne	Lok.norm.	Glob.norm.
Sistem tehničnega varovanja				
Cena	50	50	50	50
Nabavna cena	100	50	100	50
Dobavljivost opreme	0	0	0	0
Nakup tehnične opreme	100	0	100	0
Uporaba sistema	0	0	0	0
Zahtevnost uporabe sistema	100	0	100	0
Postavitev sistema	0	0	0	0
Zahtevnost postavitve sistema	100	0	100	0
Varnost	50	50	50	50
Varnost tehničnega sistema	100	50	100	50

7.6 Rezultati vrednotenja

Kriterij	Sistem tehničnega varovanja
Sistem tehničnega varovanja	Priporočljivo
Cena	Priporočljivo
Nabavna cena	Do 250 eur
Dobavljivost opreme	Priporočljivo
Nakup tehnične opreme	Enostavno
Uporaba sistema	Priporočljivo
Zahtevnost uporabe sistema	Enostavno
Postavitev sistema	Priporočljivo
Zahtevnost postavitve sistema	Enostavno
Varnost	Priporočljivo
Varnost tehničnega sistema	Tehnični sistem, ki vsebuje kameri in senzorja

Rezultati analize programa DEXi so pokazali, da je naš sistem priporočljiv v vseh kategorijah in pod kategorijah.

Naše ugotovitve, da se sistem tehničnega varovanja doma izplača in pomaga proti vlomom smo potrdili tudi z analizo stroškov in koristi, ki smo jo izvedli s programom DEXi. Opravljena analiza je pokazala, da je v diplomskem delu predstavljen sistem tehničnega varovanja priporočljiv v vseh analiziranih kategorijah.

8 RAZPRAVA

Mnogi ljudje niso prepričani, da lahko varnostne kamere dejansko odvrnejo kriminal. Jasno je, da varnostne kamere ne morejo odvrniti 100 odstotkov kriminala, vendar je večina akademskih študij ugotovila, da varnostne kamere zmanjšujejo kriminalna dejanja. Lokalna televizijska postaja v Oregonu, imenovana KTVB7, je intervjuvala 86 zapornikov, ki so prestali čas zaradi vloma na oddelku za rehabilitacijo v Oregonu. Po pogovoru o njihovih vlomih, so ugotovili, da bi večina zapornikov takoj odšla, če bi se sprožil varnostni alarm. Na splošno so varnostne kamere storilce odvračale od vlomov v domove, čeprav je manjšina priznala, da bi prisotnost varnostnih kamer lahko nakazovala na prisotnost več dragocenosti, ki bi jih bilo vredno zaščititi in spodbujale kriminal. Obsežen pregled več akademskih študij je pokazal, da so kamere za video nadzor učinkovitejše pri odvračanju od kriminala, če so povezana z drugimi elementi, kot je osvetlitev. Z raziskavo 422 vlomilcev po Severni Karolini, Ohiu in Kentuckyju je Oddelek za kazensko pravosodje in kriminologijo Univerze v Severni Karolini ugotovil, da je večina vlomilcev upoštevala zunanje kamere in druge nadzorne znake in opremo, ko so izbirali domove. 60 odstotkov vlomilcev je reklo, da bi, če bi našli alarm, izbrali drugo tarčo, polovica pa je rekla, da takoj odidejo, če so med vlomom našli alarm. Študija mesta Newark v New Jerseyju je pokazala, da stanovanjski protivlomni alarmni sistemi zmanjšujejo kriminal na domovih in v celotnem mestu. Medtem ko mnogi verjamejo, da varnostne kamere zgolj izpodrivajo kriminal v druge hiše, je študija Rutgers pokazala, da naredijo celotne soseske varnejše. Soseske, v katerih so bili gosto nameščeni alarmi proti vlomu po stanovanjih, imajo manj primerov vlomov kot soseske z manj nameščenih alarmov, je pokazala študija. Drug mit o varnostnih kamerah je, da cene kamer kljub odvračanju od kriminala se še vedno izplačajo. Čeprav lahko najcenejše varnostne kamere stanejo le 20 dolarjev in glede na dejstvo, da je bila povprečna škoda na vlom leta 2017, po podatkih FBI, 2416 dolarjev. Glede na izračun bi lahko s tem denarjem namestili 5 takšnih kamer, ki bi se desetkrat poplačale. Študija opravljena na Urban Institute je postavila kamere v Baltimore, Chicagu in Washingtonu, DC. V središču Baltimora je 500 kamer privedlo do velikega zmanjšanja kriminala in sicer za povprečno 30 primerov na mesec, brez dokazov da bi se kriminal prestavil na drugo območje. Podobno je

bilo po celem Chicagu nameščenih več kot 8.000 kamer, ki so bile zaslužene za skoraj 12 - odstotno zmanjšanje kriminala. Vendar niso bili vsi podatki tako pozitivni. Čeprav delujoče varnostne kamere dokazano odvračajo od kriminala, je to le v primeru, ko delujejo pravilno. Če pogledamo sisteme kamer od leta 2001 do 2003, je Center za nadzorne študije Queen's University ugotovil 168 tehničnih napak, ki preprečujejo uporabo dokazov v kazenskih postopkih. Seveda se je tehnologija pametnega doma od leta 2003 močno izboljšala, čeprav se seveda lahko še vedno pojavljajo tehnične napake. Vse varnostne kamere niso pokazale odvračanja od kriminala. Na primer, kamere, ki so bile postavljene v ulici v centru mesta v Lincolnu v Nebraski, niso pomagale policistom pri identifikaciji kriminalcev, krepitvi njihovih dokazov ali preprečevanju zločinov. Pravzaprav, je bilo v razdali 152 metrov medtem ko so bile kamere vklopljene, 128 kriminalnih dejanj, zato kamere v tem primeru niso storile ničesar, da bi odvrnile kriminal. Čeprav je bilo odvračanje od kriminala v središču Baltimora in v Chicagu, je Urban Institute ugotovil, da imajo nadzorni sistemi svoje omejitve.

Ne glede na to, ali gre za napačen čas, če dogodkov ne zajamete v celoti ali ponoči ali v slabem vremenu izgubite jasno sliko, varnostne kamere niso popolne. Poleg tega niso vplivali na stopnjo kriminala v DC ali na drugih območjih Baltimora, zato so bili zaključki študije mešani, čeprav je bila glede na celoto pozitivna. Druga možnost, o kateri razmišlja veliko ljudi je, da postavijo opozorilne table da je objekt pod videonadzorom, da bi odvrnili vlomilce, čeprav so le-ta včasih neresnična. Opozorilne table, da je objekt pod video nadzorom zagotovo niso tako učinkovita kot varnostne kamere ali alarmi, vendar lahko kljub temu odvrnejo nekatere vlomilce, približno 25 odstotkov po študiji oddelka za kazensko pravosodje in kriminologijo. Raziskava KTVB7 je odkrila tudi mešane rezultate v zvezi z opozorilnimi tablami, da je objekt pod videonadzorom kot odvračilnimi ukrepi. Medtem ko opozorilne table nekaterih vlomilcev niso motili, so jih nekateri vzeli kot znak za nadaljevanje. Na splošno so opozorilne table, da je objekt pod videonadzorom poceni in malo verjetno je, da bodo spodbujali kriminal, zato ni škode, če jih postavimo pred objekt. Ko pomislimo na varnostne kamere, lahko pomislimo na kamere, skrite za drevesi, prikrite kot skale ali drugače skrite pred očmi. Številne študije pa so pokazale, da so vlomilci, ki, dejansko vidijo domove z varnostnimi kamerami, redkeje odločijo da bodo vanje vlomili, zato skrite kamere izničijo ta namen. Zunanje kamere so bolj učinkovite, če so vidne, da

preprečujejo pojav kaznivih dejanj in ne le da pasivno snemajo. Zunanja razsvetljava, zlasti osvetlitev z aktiviranjem gibanja, lahko dobesedno osvetli kriminalce in poveča njihovo vidljivost. Druge oblike aktivnega odvračanja vključujejo kamere z vgrajenimi sirenami in zvočniki. Določene kamere imajo na primer obliko umetne inteligence, imenovano Smart Sentry. Na kratko, če kdo hodi, bodo kamere prižgale LED luči in zaigrale melodijo. Raziskava je pokazala da vklop nekaj utripajočih rdečih in belih luči, potencialnega kriminalca aktivno odvračale. Dober nočni vid je pri varnostnih kamerah nujen. Če nimajo luči, ki omogočajo barvni nočni vid, bi morale varnostne kamere imeti infrardeče LED-senzorje za ustvarjanje jasne slike v temi. Pomembno je, da je kamera odporna na različne vremenske razmere na določenem območju. Čeprav obstajajo določeni dokazi o nasprotnem, na splošno študije kažejo, da lahko varnostne kamere odvrnejo kriminal, tudi ne da bi ga premestile drugam. Seveda je pomembno, da imamo visokokakovostne varnostne kamere, ki lahko posnamejo jasne posnetke v vsakem času dneva ali vremenskih razmerah. V študiji Univerze v Severni Karolini je 25 odstotkov vlomilcev dejalo, da jih opozorilne table, da je objekt pod videonadzorom odvračajo od izbire hiše. Vendar so opozorilne table manj učinkovit odvračilni ukrep kot varnostne kamere in sistemi, ki bi odvrnili 53 odstotkov vlomilcev. Kamere so dobre za odvračanje od kriminala, saj bo 60 odstotkov večine vlomilcev izbralo drugo tarčo, če bodo našli alarme ali kamere, je pokazala študija Oddelka za kazensko pravosodje in kriminologijo Univerze v Severni Karolini (Turner, Vigderman, 2021).

V študiji opravljeni v Angliji in Walesu po podatkih urada za nacionalno statistiko med leti 2012 in 2013, kjer so merili učinkovitost tehničnih sredstev proti vlomom, so ugotovili, da je bilo v tem obdobju izvedenih 694.000 vlomov oziroma, da je bilo v vlomljeno v 2,1% gospodinjstev na tem območju. Avtorji študije ugotavljajo, da uporaba tehničnih sredstev kot so zunanje luči, dvojne ključavnice in alarmne naprave zagotavlja vsaj 20 krat večjo zaščito pred vlomi kot ne uporaba le-teh. Kombinacija več različnih protivlomnih naprav pa ustvarja pozitivne interakcijske učinke, ki povečujejo stopnjo zaščite. Čeprav so potrebne nadaljnje raziskave, so ugotovitve da ima izboljšana varnost pomembno vlogo pri dolgoročnem upadanju števila vlomov, skladne. Glede stroškovne učinkovitost, ki se porabi za sistem tehničnega varovanja so potrebne dodatne raziskave. Najboljše ugibanje, ki

temelji le na številu naprav in vplivu, bi bilo, da obstajajo predhodni dokazi, da se okna in vrata zaklenejo skupaj z zunanjimi lučmi ali varnostnimi verigami, kar je najbolj stroškovno učinkovito (Farrell, Grove, Thompson, Tilley, Tseloni, 2017).

Po našem mnenju in glede na opravljene raziskave v tujini, mislimo da kakšna koli oblika sistema tehničnega varovanja doma pomaga proti vlomom, naj bodo to kamere, senzorji ali alarmni sistemi. Opozorilne table pa so raziskave pokazale mešane rezultate, ponekod bi naj preprečevale kriminal, drugje pa celo spodbujale kriminal. Sistem tehničnega varovanja lahko postavimo že z malo denarnimi sredstvi, prav tako ni potrebno veliko znanja. Kar smo v našem primeru tudi predstavili. Prepreči pa nam lahko velike nevšečnosti, ki bi se zgodile zaradi vlome pa naj bo to le razbito steklo, vrata in razmetana notranjost prostorov ali pa celo ukradeni kakšni vrednejši predmeti.

9 ZAKLJUČEK

Naš zaključek je, da postavitev sistema za tehnično varovanje za fizične osebe ni zahteven in ga z ustreznimi navodili, postavi kdorkoli. Je cenovno majhen vložek v primerjavi s ponudbami podjetij, ki se ukvarjajo s postavitvijo video nadzornega sistema. Danes je že večina opreme povezljiva z Wi-Fi, kar nam zelo olajša delo, saj ne potrebujemo podrobnega znanja za povezljivost opreme.

V našem primeru smo se odločili za proizvajalca znamke Digoo, ker ima ugodne cene in relativno enostavna navodila. Slaba lastnost tega proizvajalca je, da ne odgovarja na elektronska pošto kot pomoč strankam. V 60. dneh namreč nismo dobili nobenega odgovora kljub več poslanim elektronskim sporočilom. Elektronska pošta je edini način za pomoč strankam pri kupljenih Digoo izdelkih.

Glede sistema delovanja, smo zadovoljni, lahko bi bil bolj enoten, da bi lahko vse izdelke dodali v eno aplikacijo na mobilnem telefonu ter vse uporabljali na računalniku, kar pa na žalost ni možno. Slaba stran kamer je tudi občutljivost detektorja gibanja, saj je kljub temu, da je bil nastavljen na najnižjo stopnjo občutljivosti, javljal alarme že pri premikanju trave, drevja in sence. Do tega ne bi smelo prihajati, saj v opisu piše da se sproži alarm ob premiku večjih objektov ali ljudi. Prav tako smo nezadovoljni z nočnim vidom kamere, saj se v popolni temi ne vidi skoraj ničesar.

Mi smo s sistemom relativno zadovoljni, saj je bil naš namen neprofesionalna raba za fizične osebe. Omembe vredno je le, da je priporočljivo biti pozoren pri podrobnostih in opisu izdelkov. Pomembno je namreč kakšne vrste povezave podpirajo, način shranjevanja vsebine, ločljivost video kamere in primernost izdelka za posamezne namene. Da se postavitev predstavljenega sistema tehničnega varovanja izplača smo dokazali tudi v analizi opravljeni s programom DEXi.

VIRI IN LITERATURA

Allen, J. (3. 5. 2021). What is a Network. Life Wire Pridobljeno na https://www.lifewire.com/what-is-a-network-5180410

Breščak, B. (n. d.). *Kaj je računalniško omrežje*. Pridobljeno na http://www.egradiva.net/drugo/omrezja/01_omrezja/01_datoteka.htm

Burt, P., Collins, R. T., Duggins, D., Enomoto, N., Fujiyoshi, H., Hasegawa, O., Kanade, T., Lipton, A. J., Tolliver, D., Tsin, Y. (2020). *A System for Video Surveillance and Monitoring. VSAM Final Report.* Pridobljeno na https://www.ri.cmu.edu/pub_files/pub2/collins_robert_2000_1/collins_robert_2000_1.pdf

Bohanec, M. (10. 5. 2021). *DEXi: A Program for Multi-Attribute Decision Making.* Pridobljeno na https://kt.ijs.si/MarkoBohanec/dexi.html

Digoo. (n. d. a). *1080P PTZ Smart IP Camera*. Pridobljeno na https://www.mydigoo.com/1080p-ptz-smart-ip-camera-p-179320.html

Digoo. (n. d. b). *720P HD 355° PTZ Smart WIFI IP Camera User Manual*. Pridobljeno na https://www.mydigoo.com/720p-hd-355-ptz-smart-wifi-ip-camera-p-230585.html

Digoo. (n. d. c). *WIFI Door & Window Sensor User Manual*. Pridobljeno na https://www.mydigoo.com/wifi-door-and-window-sensor-p-301406.html

Divjak, S. (20. 12. 2019). *Računalniško omrežje*. Pridobljeno na http://colos.fri.unilj.si/ERI/INFORMATIKA/RACUNALNISKA_OMREZJA/RacunalniskoOmrezje.html

Dobrišek, S., Štruc, V., Vesnicer, B., Mihelič, F. (2013). Bodo pametni nadzorni sistemi prisluhnili, razumeli in spregovorili slovensko?. *Slovenščina 2.0: Empirične, Aplikativne in Interdisciplinarne Raziskave*, *1*(2), 165-180. doi:/10.4312/slo2.0.2013.2.165-180

Eli The Computer Guy. (n. d.). *Networking: TCP/IP and Subnet Masking*. Pridobljeno na http://www.elithecomputerguy.com/2010/12/12/tcpip-and-subnet-masking-2/

Ellingwood, J. (12. 3. 2014). *Understanding IP Addresses, Subnets, and CIDR Notation for Networking*. Pridobljeno na

https://www.digitalocean.com/community/tutorials/understanding-ip-addresses-subnets-and-cidr-notation-for-networking

Fakulteta za računalništvo in informatiko [FRI]. (2007). *Usmerjevalnik*. Pridobljeno na http://colos.fri.unilj.si/ERI/RAC_SISTEMI_OMREZJA/html/medmerezno_povezovanje/usmerjevalnik.html

Farrell, G., Grove, L., Thompson, R., Tilley, N., Tseloni, A. (2017). The Effectiveness of burglary security devices. *Security Journal, 30*(2), 646–664.

Fisher, T. (25. 4. 2021). *What Is a Router and How Does It Work?*. Pridobljeno na https://www.lifewire.com/what-is-a-router-2618162

Forstnerič, J. (16. 6. 2020). Domače Omrežje. Monitor. Pridobljeno na https://www.monitor.si/clanek/domace-omrezje/199141/

Johnson, D. (7. 4. 2021). What is a Mesh Network? How Does It Work?. Life Wire. Pridobljeno na https://www.lifewire.com/what-is-a-mesh-network-4842178

Koščak, T. (3. 1. 2017). Varnost ljudi danes. Varen svet. Pridobljeno na http://www.varensvet.si/varnost-ljudi-danes/

Lee, S. (5. 2. 2009). *Rutgers Study Finds Alarm Systems Are Valuable Crime Fighting Tool*. Pridobljeno na https://www.rutgers.edu/news/rutgers-study-finds-alarm-systems-are-valuable-crime-fighting-tool

Manualslib. (2013). *Calix T07xG HGU ONT Operation and Maintenance Guide.* Pridobljeno na https://www.manualslib.com/manual/1291112/Calix-T072g.html#manual

Microsoft. (21. 9. 2020). *Understand TCP/IP Addressesing and Subnetting basics*. Pridobljeno na https://docs.microsoft.com/en-us/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting

Mitchell, B. (2. 2. 2021). Wireless Local Area Networking Explained. Life Wire. Pridobljeno na https://www.lifewire.com/wlan-816565

Mitchell, B. (17. 4. 2021). Ethernet Cables and How They Work. Life Wire. Pridobljeno na https://www.lifewire.com/what-is-an-ethernet-cable-817548

Mitchell, B. (22. 6. 2021). What Is a Wide Area Network (WAN)?. Life Wire. Pridobljeno na https://www.lifewire.com/wide-area-network-816383

Mitchell, B. (30. 7. 2021). What Is Bluetooth Wireless Networking?. Life Wire. Pridobljeno na https://www.lifewire.com/definition-of-bluetooth-816260

Mitchell, B., Selph, C. (11. 9. 2020). *802.11* Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a. Life Wire. Pridobljeno na https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553

Policija (2021). *Letno poročilo o delu policije | 2020.* Pridobljeno na https://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2020.pdf

Šrekl, J. (2014). Varno upravljanje informacijskih sistemov. V Taradi, J. (ur.), 9th International Scientific and Professional Conference Management and Safety (str. 225-235). Moravske Toplice: The European Society of Safety Engineers. Pridobljeno na http://www.european-safety-engineer.org/MS2014/MS%202014_Proceedings.pdf

Telekom Slovenije, d.d. (n. d. a). *Prvo 5G omrežje Slovenije*. Pridobljeno na https://www.telekom.si/5G

Telekom Slovenije, d.d. (n. d. b). *Storitev 5G*. Pridobljeno na https://www.telekom.si/zasebni-uporabniki/ponudba/telefonija/storitve/5g

Telemach. (n. d.). *Vodič za hitro namestitev WI-FI Mesh*. Pridobljeno na https://telemach.si/wp-content/uploads/2020/09/Navodila-WiFi-Mesh-A5-1-2020-NET.pdf

Tholen, C. (27. 5. 2021). How Does a Door Sensor Work?. Safe Wise. Pridobljeno na https://www.safewise.com/home-security-faq/how-door-sensors-work/

Tholen, C. (27. 5. 2021). How Does a Window Sensor Work?. Safe Wise. Pridobljeno na https://www.safewise.com/home-security-faq/how-window-sensors-work/

Turner, G., Vigderman, A. (21. 8. 2021). Do Security Cameras Deter Crime? Security.org. Pridobljeno na https://www.security.org/security-cameras/deter-crime/

Unuth, N. (18. 11. 2019). What IP Means and How It Works. Life Wire. Pridobljeno na https://www.lifewire.com/internet-protocol-explained-3426713

Unuth, N. (10. 5. 2020). Wi-Fi Explained: The Most Common Wireless LAN Network. Life Wire. Pridobljeno na https://www.lifewire.com/wifi-explained-3426413

Uy, M. (2. 2. 2020). What Is Bluetooth?. Life Wire. Pridobljeno na https://www.lifewire.com/what-is-bluetooth-2377412

Uy, M. (22. 6. 2021). Definitions and Examples of Wireless Technology. Life Wire. Pridobljeno na https://www.lifewire.com/what-is-wireless-2377432

Vavpotič, S. P. (16. 6. 2020). Varovanje in oddaljeni nadzor doma. *Monitor*, 2020 (posebna izd.). Pridobljeno na https://www.monitor.si/clanek/varovanje-in-oddaljeni-nadzor-doma/199143/

Wi-Fi Alliance, (2021). *Wi-Fi generacije.* Pridobljeno na https://www.wi-fi.org/discover-wi-fi

Wi-Fi Alliance, (2021). *Zgodovina.* Pridobljeno na https://www.wi-fi.org/who-we-are/history

Whitehead, C. T. (5. 2. 2020). What Is LAN? Life Wire. Pridobljeno na https://www.lifewire.com/what-is-lan-4684071

Zakon o varstvu osebnih podatkov (ZVOP-1). (2014). *Uradni list* RS, (94/07, 177/20).