Univerzita Pardubice
Dopravní fakulta Jana Pernera

Zabezpečení objektu

David Špinar

Bakalářská práce

2020

Univerzita Pardubice
Dopravní fakulta Jana Pernera
Akademický rok: 2019/2020

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

Jméno a příjmení:	**David Špinar**
Osobní číslo:	**D16151**
Studijní program:	**B3709 Dopravní technologie a spoje**
Studijní obor:	**Aplikovaná informatika v dopravě**
Téma práce:	**Zabezpečení objektu**
Zadávající katedra:	**Katedra informatiky v dopravě**

Zásady pro vypracování

Cílem práce je posouzení možností zabezpečení budovy pomocí elektronických systémů, jejich funkce, možností zapojení a komunikace, zejména z hlediska informačních technologií.

Rozsah pracovní zprávy: **30 normostran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z : technologie pro datovou, hlasovou i multimediální komunikaci. 2. aktualiz. vyd. [s.l.] : [s.n.], 2006. 430 s. ISBN 80-251-1278-0.
2. Cisco Networking Academy Program: CCNA 1 and 2 Lab Companion. USA: Cisco Press, 2003.
3. EArchiv.cz: Archiv článků a přednášek Jiřího Peterky [online]. 2019 [cit. 2019-11-28]. Dostupné z: www.earchiv.cz

Vedoucí bakalářské práce: **Ing. Zdeněk Drvota**
Katedra informatiky v dopravě

Datum zadání bakalářské práce: **28. listopadu 2019**
Termín odevzdání bakalářské práce: **31. ledna 2020**

L.S.

doc. Ing. Libor Švadlenka, Ph.D.
děkan

doc. Ing. Karel Greiner, Ph.D.
vedoucí katedry

V Pardubicích dne 28. listopadu 2019

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

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

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

V Pardubicích dne 24. 1. 2020

David Špinar

PODĚKOVÁNÍ

Chtěl bych poděkovat Ing. Zdeňku Drvotovi, za volnost, kterou mi poskytl při výběru tématu a za vedení mé práce. Děkuji také své rodině za podporu, kterou mi poskytli nejen při psaní této práce, ale po celou dobu studia.

ANOTACE

Bakalářská práce řeší problematiku zabezpečení objektu pomocí elektronických systémů. Je rozdělena na tři hlavní části a to senzory, kde vysvětlí funkčnost, použití a možnosti senzorů. Druhá část je věnovaná kamerovému systému, principu získání obrazu, druhům kamer a způsobům přenosu signálu. Třetí část je zaměřena na bezpečnost samotné sítě, popis bezpečnostních hrozeb a ochrana před útokem po síti.

KLÍČOVÁ SLOVA

Senzory, kamerové systémy, počítačová síť, bezpečnost

TITLE

Building security

ANNOTATION

The thesis covers building security using electronic systems. It is divided into three main parts. The sensor part explains the functionality, usage and possibilities of the sensors. The second part is devoted to the CCTV, principle of image acquisition, types of cameras and methods of signal transmission. Third part is focused on the network security, description of security threats and protection against network attacks.

KEYWORDS

Sensors, CCTV, network, security

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

ACL	Access Control List = seznam pro řízení přístupu
CCD	Charge-coupled device
CCTV	Closed-circuit television = kamerový systém
CMOS	Complementary Metal-Oxide-Semiconductor
DC	Direct current = stejnosměrné napětí
DoS	Denial of Service = odepření služby
DVR	Digital Video Recorder = digitální videorekordér
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPS	Intrusion Prevention Systems = systémy prevence průniku
LAN	Local Area Network = místní síť
NVR	Network Video Recorder
PIR	Pasivní infračervené detektory
PoE	Power over Ethernet
VPN	Virtual Private Network = virtuální privátní síť

ÚVOD

Jak zabezpečit svůj dům nebo společnost proti krádeži, je stále aktuálním tématem. A nemusí jít jen o krádeže, může jít například ochranu majetku proti vandalizmu, nebo kontrolu pohybu osob v místech, kam mají mít přístup jen autorizované osoby. S výzkumem nových technologií se otevírají další možnosti zabezpečení, ale i naši nezvaní hosté přichází stále s novými nápady, jak naše zabezpečení prolomit.

Cílem práce je projít možnosti, které nám poskytují elektronické zabezpečovací systémy. Senzorové systémy jsou schopny odhalit přítomnost narušitele a spustit jak lokální akustický poplach, tak i poplach tichý, který oznámí vniknutí policii nebo ochrance. Nicméně nedokáží identifikovat pachatele, proto se často kombinují i se systémem kamer, kvalitní kamerový záznam pak dokáže pachatele jednoznačně identifikovat.

Dnešní kamerové systémy nejčastěji posílají záznamy po síti, aby pachatel neměl možnost zničit záznamy, poškozením lokálního disku. Síťový přenos také umožňuje zobrazení záznamů z jakéhokoli místa s přístupem k internetu. Nicméně aby byl tento přenos bezpečný je potřeba mít i bezpečnou síť po které budeme záznamy posílat. Sítí jsou různé druhy a mají různé využití, ale jedno mají společné, všechny je potřeba zabezpečit proti útokům. Druhům sítí a hrozbám, kterým musí síť čelit se bude věnovat poslední část této práce.

1 SENZOROVÉ SYSTÉMY

Senzory jsou dnes snad v každém odvětví lidské činnosti, běžně se s nimi setkáváme, bez toho, aniž bychom si to uvědomili, ať už se jedná o dveře na fotobuňku, parkovací senzory nebo automatické rozsvícení světel.

Bezpečnostní senzory dělíme do dvou hlavních kategorií aktivní a pasivní. Zatímco pasivní čekají na nějakou změnu ve svém okolí, například, než narušitel například otevře dveře, nebo vejde do zabezpečené místnosti. Aktivní senzory si vytvoří své pracovní prostředí a aktivně prohledávají chráněnou oblast.

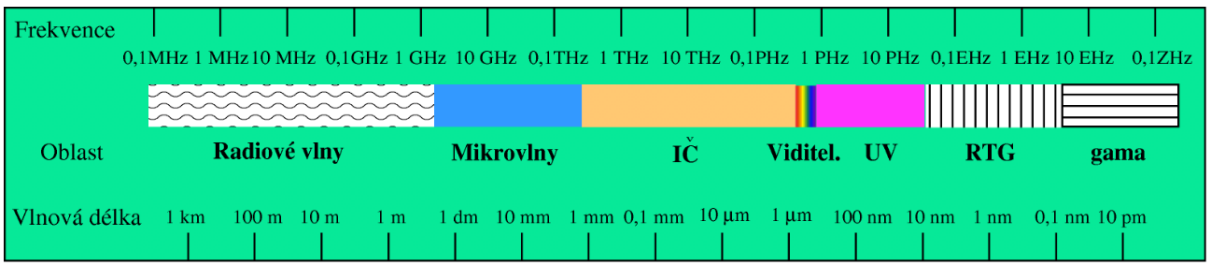
Přestože senzorové systémy nezabrání vstupu narušitele do chráněného objektu, informují ostrahu o narušení bezpečnosti, a to vyhlášením lokálního akustického poplachu, nebo dálkovým předáním zprávy. Samotná viditelná přítomnost senzorových systémů také může případného pachatele odradit.

1.1 Pasivní infračervené detektory pohybu (Passive Infrared detector)

Pasivní infračervené detektory patří mezi nejčastěji používané prvky poplachových zabezpečovacích systémů. Tyto detektory jsou schopny zachytit pohyb těles, která mají jinou teplotu než dané pozadí. [1] Čidlo funguje na principu pyroelektrického jevu, který lze obecně definovat jako schopnost materiálu generovat dočasný elektrický potenciál při změně jeho teploty.[3]

1.1.1 Infračervené záření

Je elektromagnetické záření s vlnovou délku 760nm – 1 mm, není tedy lidským okem viditelným, protože jeho vlnová délka je větší než viditelné světlo. [7]



Obrázek 1: Spektrum elektromagnetického záření [2]

Infračervené záření emituje každé těleso s teplotou větší než absolutní nula (-273 °C) a jeho intenzita se odvíjí od teploty tělesa.[4]

Záření se dále dělí podle vlnového rozsahu na pásma A,B,C. Toto dělení však není jednoznačně dané a jedno ze schémat je například toto:

- NIR – blízké (near)
  IR-A, vlnová délka 0,76–1,4 μm, definováno podle vodní absorpce; často používané v telekomunikacích optických vláken
- SWIR - krátké vlnové délky (short wave)
  IR-B, vlnová délka 1,4–3 μm, při 1450 nm značně roste vodní absorpce
- MWIR – střední vlnové délky (medium wave)
  IR-C, též prostřední (intermediate-IR neboli IIR), 3–8 μm
- LWIR – dlouhé vlnové délky (long wave)
  IR-C 8–15 μm
- FIR – vzdálené (far)
  15–1000 μm

Další často používané rozdělení:

- blízké (0,76–5 μm)
- střední (5–30 μm)
- dlouhé (30–1000 μm) [7]

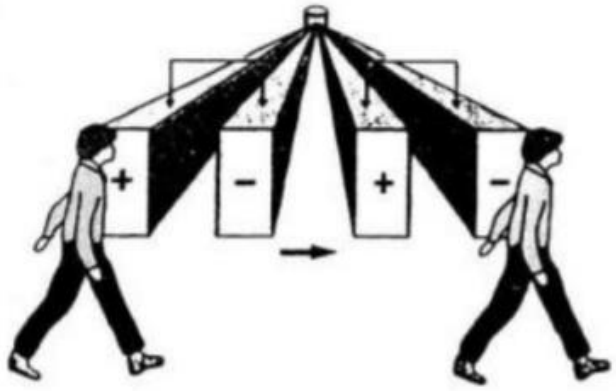
1.1.2 Pyroelement

Pro teplotu těla člověka kolem 35 °C je dána vlnová délka 9,3-9,4μm. Toto záření je detekováno pyroelementem.[1] Je to polovodičová součástka, ze sloučenin na bázi lithia a tantalu. Pyroelektrické detektory začnou při dopadu infračerveného záření generovat povrchový náboj, při změně infračerveného záření se změní i hodnota povrchového náboje. Tato změna je měřena citlivým FET tranzistorem, který je přímo vestavěný ve snímači. Pyroelektrický snímač je citlivý ve velkém vlnovém rozsahu, a proto je před něj aplikován filtr záření, který propouští infračervené záření o vlnových délkách v rozsahu 8 až 14μ.[3]

Obrázek 2: Pyroelement [3]

V současné době se častěji využívá dvojitého pyroelementu. Jednoduchý pyroelement reaguje stejně jak na pohybující, tak na nepohybující předmět stejně, pokud je tento předmět například radiátor, který se nepohybuje, ale mění teplotu, mohlo by docházet k falešným poplachům. Dvojitý pyroelement, jsou dva pyroelementy, které jsou zapojeny s opačnou polaritou, pokud tedy dojde ke změně teploty na nepohybujícím se předmětu, jsou signály díky opačné polaritě vyrušeny a k vyhlášení poplachu nedojde. [4]

Pro další navýšení spolehlivosti se používají quad pyroelementy, jedná se o dva dvojité pyroelementy společně zapouzdřené a opačně polarizované. [6]

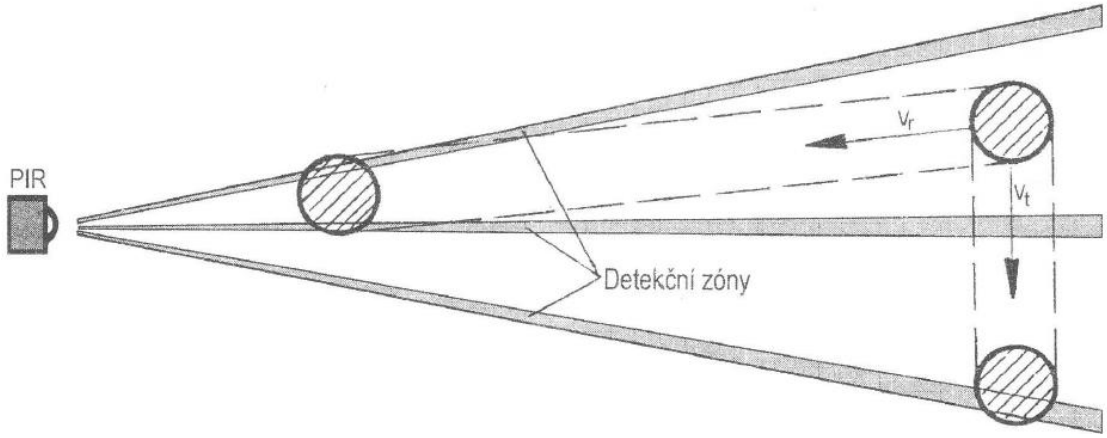


Obrázek 3 Detekce quad pyroelementem [6]

1.1.3 Optika

Optika slouží k rozdělení prostoru na takzvané detekční zóny, infračervené záření v detekčních zónách je směřováno na pyroelement. Tímto rozdělením prostoru na detekční zóny docílíme toho, že se narušitel bude pohybovat z jedné detekční zóny do druhé a každý vstup a výstup z detekční zóny má za následek generování impulzu na výstupu pyroelementu.

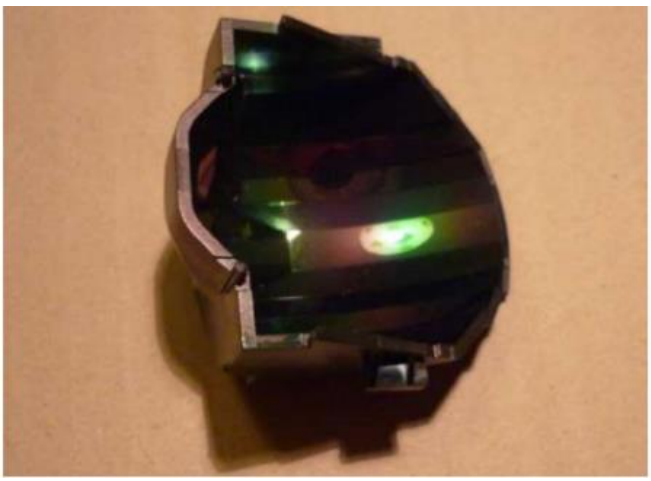
Citlivost PIR detektoru je závislá na pohybu narušitele vzhledem k detektoru. (Obrázek 4) Pokud se bude narušitel pohybovat přímo k detektoru (radiální pohyb – v_r) urazí větší vzdálenost, než bude detekován oproti případu, kdy se bude pohybovat kolmo k detektoru (tangenciální pohyb – v_t). [4]



Obrázek 4 Závislost citlivosti PIR detektoru na pohybu narušitele [4]

1.1.3.1 Zrcadlová optika

Využívá segmentovaného zrcadla, které je vyrobeno z plastu s napařenou kovovou odrazovou vrstvou, počet detekčních zón je dán počtem segmentů zrcadla. Aby na pyroelement dopadalo pouze infračervené záření, mohou být zrcadla opatřena černou vrstvou, touto úpravou vznikne takzvané „černé zrcadlo“.

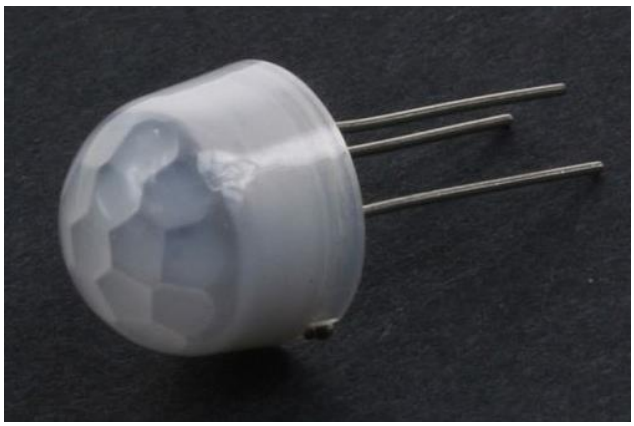


Obrázek 5 Černé zrcadlo [4]

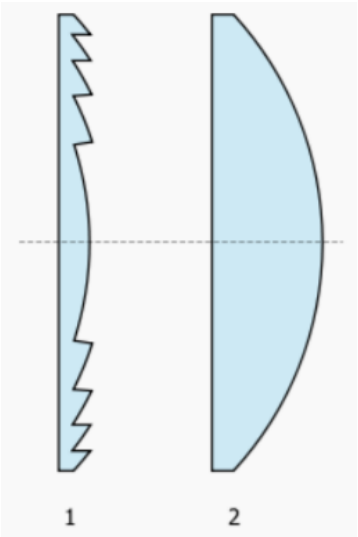
Výhodou zrcadlového systému je delší dosah a přesnější zaostření detekčních zón, než je tomu u Fresnelovy čočky, ale jsou oproti nim náročnější na výrobu a jsou tedy dražší.

1.1.3.2 Fresnelova čočka

Tato čočka má oproti běžné čočce odstraněny ty části, které se přímo nepodílejí na lomu paprsků. Její výhodou oproti zrcadlové optice je jednoduchost na výrobu, protože se jedná o výlisek z plastické hmoty, který obsahuje soustavu čoček. Počet detekčních zón je dán počtem čoček. Jejich nevýhodou, ale je, že jednotlivé čočky neposkytují různé ohniskové vzdálenosti, a proto nejsou přímo zostřeny na pyroelement.[4]



Obrázek 6 Fresnelova čočka [5]



Obrázek 7 Porovnání čoček: 1 – Fresnelova, 2 – klasická[4]

1.1.4 Zpracování signálu

Dopadající infračervené záření na pyroelement má podobu spojitého (analogového) signálu a informace o detekovaném objektu nese každá vlna, proto je důležité mít pro detektor kvalitní zpracování získaného analogového signálu. Zpracování signálu je závislé na kvalitě optického systému a používají se dva způsoby zpracování signálu analogový a digitální.

1.1.4.1 Analogové zpracování signálu

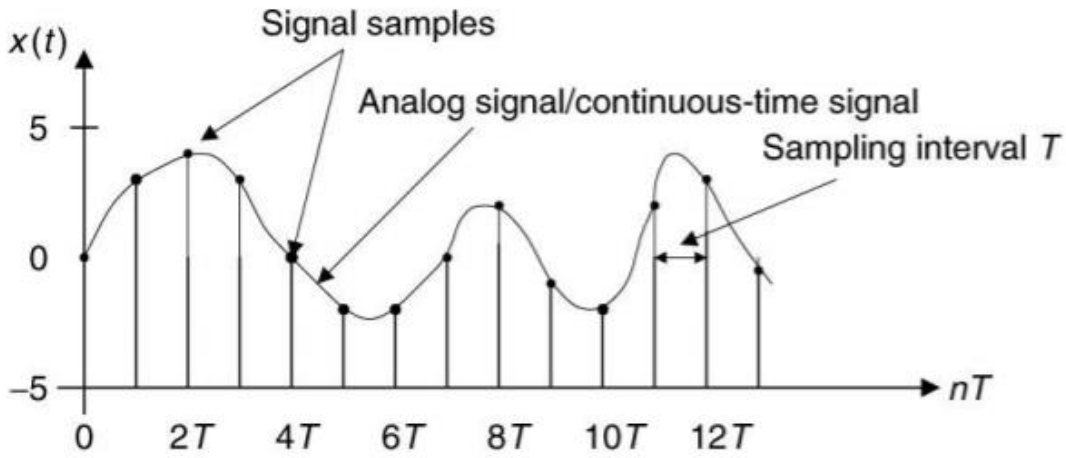
Při tomto zpracování je vyhodnocována prahová úroveň signálu, pokud dojde k jejímu překročení dojde k vyhlášení poplachu. Tento způsob vyhodnocení bývá kombinován s čítačem pulsů, poplach je tedy vyhlášen až po překročení prahové úrovně několikrát v daném čase.

1.1.4.2 Digitální zpracování signálu

Digitální signál je signál, který je nejdříve vzorkovaný a následně kvantovaný. Tvoří ho posloupnost vzorků, které mohou nabývat pouze omezeného počtu hodnot v přesně daných časových intervalech.

Vzorkovaný signál

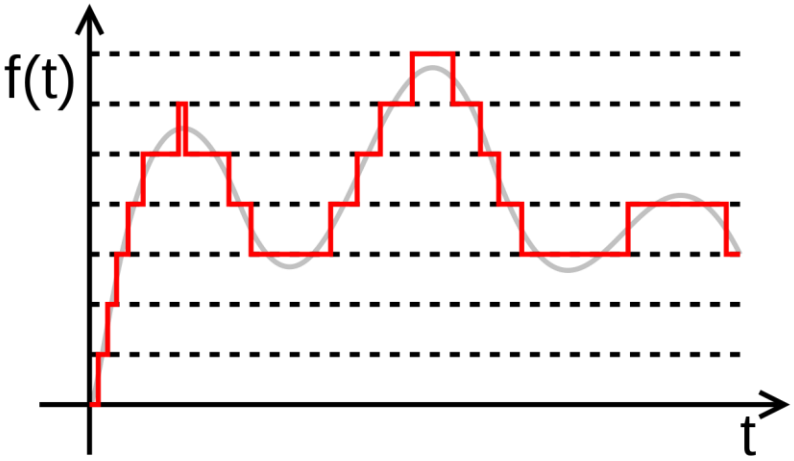
Tento signál není spojitý v čase, ale je tvořen posloupností vzorků. Obvykle vzniká vzorkováním, tedy odebíráním vzorků vždy v určité periodě (T), převrácená hodnota periody udává vzorkovací frekvenci $f_v = \frac{1}{T}$. [6], [8]



Obrázek 8 Vzorkovaný signál [8]

Kvantovaný signál

Který obvykle vzniká kvantováním je signál, který nemá spojitý průběh, ale jeho hodnota se mění skokem. Signál nabývá pouze omezeného počtu úrovní a ke změně hodnoty signálu může dojít obecně v libovolném čase. [6]



Obrázek 9 Kvantovaný signál [9]

Digitální signály jsou oproti analogovým méně náchylné k poruchám, lze je také lépe zpracovávat a vyhodnocovat, proto je snaha výrobců digitalizovat signál již po jeho detekování senzorem a tím eliminovat nepřesnosti, které vznikají jeho snímáním. [6]

1.2 Ultrazvukové detektory (Ultrasonic detector)

Ultrazvukové senzory spadají do kategorie aktivních senzorů, protože neustále vysílají ultrazvukové vlny a odražená vlna je následně vyhodnocena v přijímači. V prostoru vytvoří konstantní vlnění, a to je chápáno jako klidový stav. Pohyb narušitele změní hodnotu přijatého vlnění a spustí se poplach. Pracují na frekvenci 20 - 45kHz, což je frekvence lidským uchem neslyšitelná. Jejich dosah je přibližně 10 m. [1]

Při montáži těchto senzorů mají být čidla instalována tak, že pravděpodobný pohyb pachatele směřuje směrem k čidlu. Navíc prostor musí být uzavřený, aby dosah čidla nemohl přesahovat mimo prostor určený ke střežení.

Nevýhodou těchto čidel je, že pokud jsou v místnosti koberce nebo pěnové materiály, které absorbují ultrazvuk, může se citlivost čidel značně změnit posunutím těchto předmětů, čidlo může být potom příliš citlivé, nebo málo. Také pro instalaci více ultrazvukových čidel v jedné místnosti je nutno dbát na to, aby byli vysílače synchronizovány, aby se vzájemně neovlivňovali. [10]

Při porovnání ultrazvukových senzorů s PIR detektory, je nevýhoda ultrazvukových v jejich spotřebě, která je vyšší z důvodu konstantního vysílání vln, nicméně jejich výhoda je v nesegmentovaném detekčním poli, nemají tedy žádné slepé body, ve kterých není možné pachatele detekovat. [11]

1.2.1 Ultrazvuk

Je zvuk s frekvencí větší než 16kHz, jeho vlnová délka je mnohem menší (řádově v milimetrech) a to mu umožňuje šíření přímočaré ve formě úzkých paprsků, které se lámou, odrážení a mohou se soustředit do jednoho ohniska. Ultrazvuk může procházet i neprůhlednými materiály, ale stejně jako zvuk se nemůže šířit ve vakuu.

1.2.2 Dopplerův jev

Je fyzikální jev, který nastává u jakéhokoliv vlnění. Pokud uvažujeme příklad, kdy z loďky na hladině rybníka hodíme do vody kámen, tak se od místa dopadu začnou na hladině šířit vlny, které mají vlnovou délku $\lambda = c/f$. a periodu $T = 1/f = \lambda/c$. Pokud začneme pádlovat směrem proti šíření vln rychlostí v, naše rychlost a rychlost vln se sečtou $c+v$, vlnová délka zůstává stejná.

Pokud, ale loďka zůstane stát a vlnění se začne pohybovat směrem k nám (například plovoucí kachna) o stálé frekvenci f, dojde ke změně vlnové délky λ na λ-v. $T = (\lambda - v)/c$ Z příkladu tedy vyplývá, že pokud se bude vysílač a přijímač vzájemně pohybovat nenulovou rychlostí, bude docházet ke změnám frekvence a vlnové délky mezi vyslaným a přijatým signálem.

Vysílač emituje do prostoru ultrazvukové vlny o kmitočtu f_v , vlnění se odrazí od objektů a vrátí se zpět do přijímače o kmitočtu f_p. Při prvním uvedení do provozu si detektor provede detekční zkoušku okolního prostředí a nastaví porovnávací hodnotu pro přijatý kmitočet. Pokud je přijímaný kmitočet vyšší narušitel se pohybuje směrem k vysílači, pokud je nižší pohybuje se od vysílače. Je porovnána změna přijímaného kmitočtu a při překročení prahové hodnoty je na výstupu detektoru generován poplachový signál.

Rychlost pohybu narušitele můžeme určit podle následujícího vztahu:

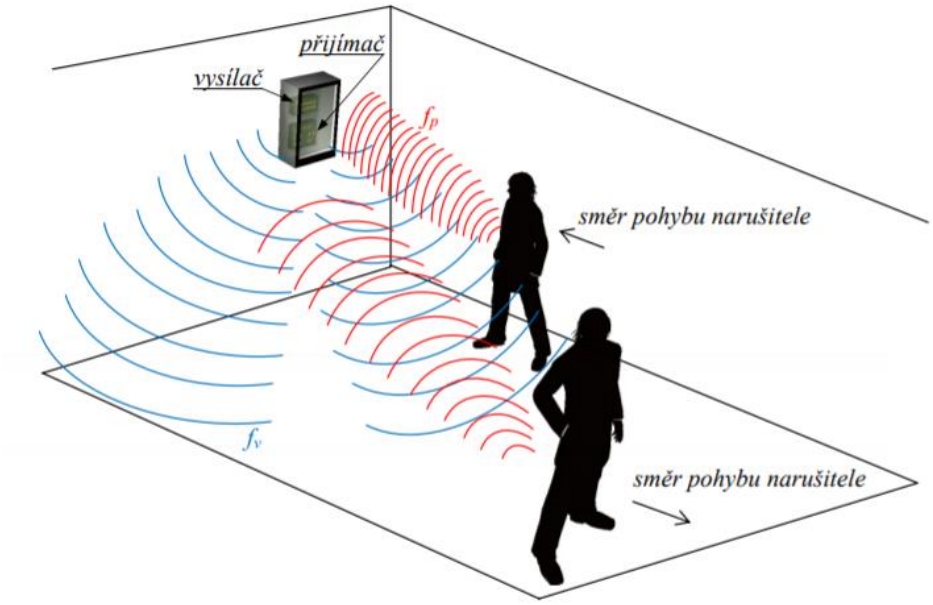
$$v = \frac{(f_p - f_v) * c}{f_p} \quad [m * s^{-1}]$$

v – rychlost pohybu narušitele

f_p – přijatý kmitočet

f_v – vysílaný kmitočet

c – rychlost vlnění



Obrázek 10 Dopplerův jev [12]

1.2.3 Ultrazvukový senzor

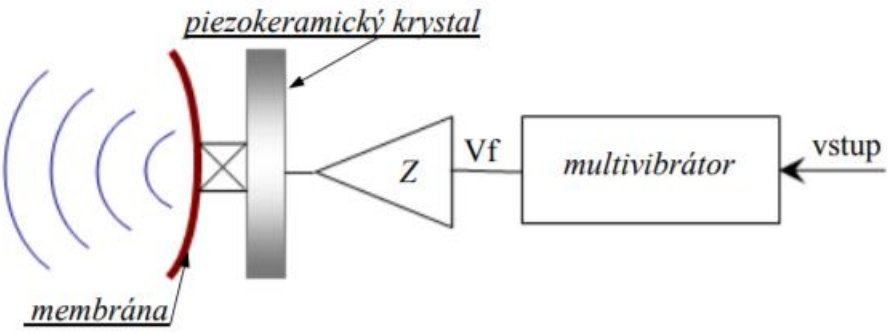
Základní části ultrazvukového detektoru jsou dva ultrazvukové senzory – vysílač a přijímač ultrazvukových vln. Ultrazvukový vysílač přeměňuje elektrický signál na ultrazvukové vlny, je složen z piezoelektrického krystalu a membrány. [12]

1.2.3.1 Piezoelektrický jev

Je schopnost krystalu generovat elektrické napětí při jeho deformaci, případně opačný jev, kdy se krystal v elektrickém napětí deformuje. Vyskytuje se pouze u krystalů, které nemají střed symetrie. Nejčastěji je využíván piezokeramický materiál na bázi oxidu křemičitého (křemene).

„Vznik tohoto jevu vysvětlujeme takto: Deformací se ionty opačných nábojů posunou v krystalové mřížce tak, že elektrická těžiště záporných a kladných iontů, která v nezdeformovaném krystalu souhlasí, se od sebe vzdálí. Na určitých plochách krystalu se objeví elektrický náboj. Při obráceném piezoelektrickém jevu, při tzv. elektrostrikci, působí vnější elektrické pole posunutí iontů, což vede k deformaci krystalu.“ [14]

Při přivedení vysokofrekvenčního střídavého napětí na ultrazvukový vysílač, se bude měnit rozměr piezokeramického krystalu. Krystal je mechanicky spojen s membránou, která tak produkuje zvukové vlny o vysokých frekvencích. Pro získání vysokofrekvenčního signálu senzor vysílače obsahuje multivibrátor a zesilovač. [12]

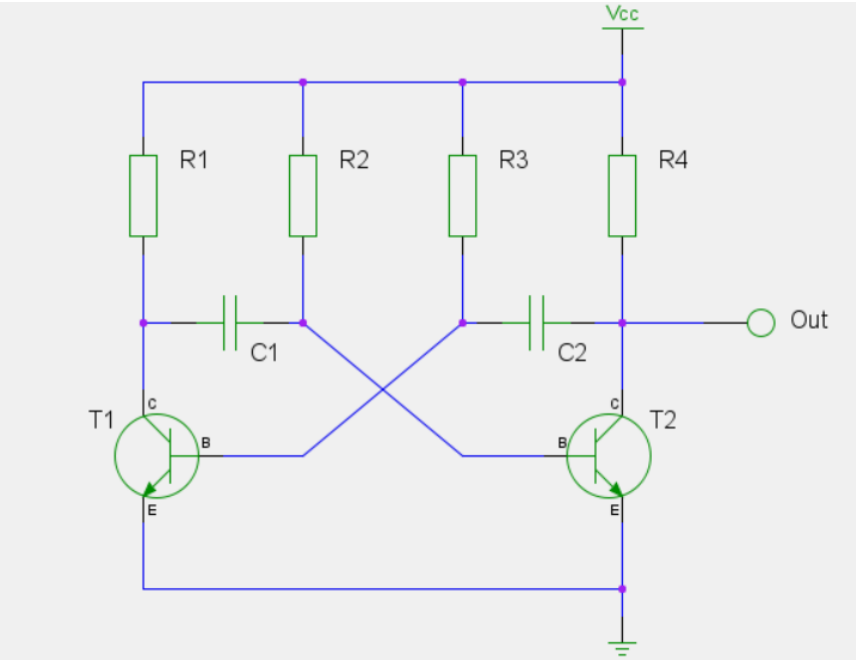


Obrázek 11 Ultrazvukový vysílač [12]

1.2.3.2 Multivibrátor (astabilní klopný obvod)

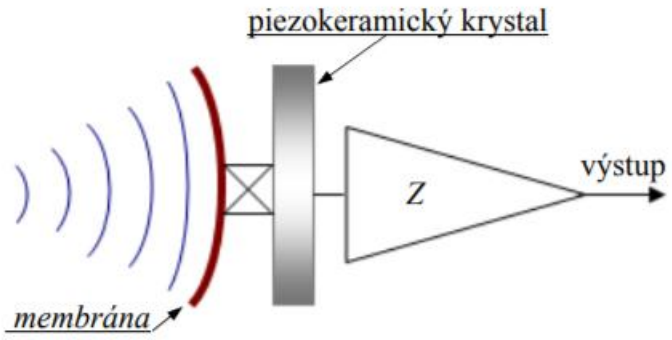
Tento obvod vyrábí impulsy délky dané hodnotou jeho součástek, tedy odporů (R) a kondenzátorů (C). Jedná se v podstatě o dvojstupňový zesilovač, u kterého je výstup jednoho stupně zaveden na vstup druhého a obráceně. Při zapnutí napájení se vždy jeden ze stupňů (libovolný) otevře, zatímco druhý zůstane zavřený.

Pokud se například otevře tranzistor T1, kondenzátor C1 je nabit napětím blízkým napájecímu napětí a vybíjí se přes odpory R1 a R2. Při jeho vybíjení se postupně zmenšuje závěrné napětí na bázi tranzistoru T2, dokud nedojde k jeho otevření. Tím se začne nabíjet kondenzátor C2, který svým napětím drží vypnutý tranzistor T1 a proces se opakuje. [15]



Obrázek 12 Multivibrátor [13]

Ultrazvukový přijímač je řešený opačně jako vysílač. Ultrazvukové vlnění dopadá na plochu membrány a jejím pohybem dochází k deformaci piezokeramického krystalu, který generuje napětí. [12]



Obrázek 13 Ultrazvukový přijímač [12]

1.3 Mikrovlnné detektory pohybu

Mikrovlnné detektory (Microwave detectors) jsou velice podobné ultrazvukovým detektorům, jedná se také o aktivní detektory, ale hlavním rozdílem je že mikrovlnné detektory emitují elektromagnetické vlny namísto vln zvukových. [11]

1.3.1 Mikrovlnné záření

Mikrovlnné záření má vlnovou délku od 1 mm – 1 m a jeho frekvence se pohybuje od 300GHz do 300MHz. Stejně jako viditelné záření se šíří přímočaře a na rozhraní dvou materiálů s rozdílnými dielektrickými vlastnostmi dochází k jeho lomu a odrazu. Podíl odrazu a dále postupujícího záření je dán především rozdílem elektrických vlastností obou prostředí a také úhlem dopadu mikrovln na plochu rozhraní. Také záleží na tom, kolik procent objemu vody daný materiál obsahuje, protože voda má schopnost mikrovlnné záření silně pohlcovat. [12], [16]

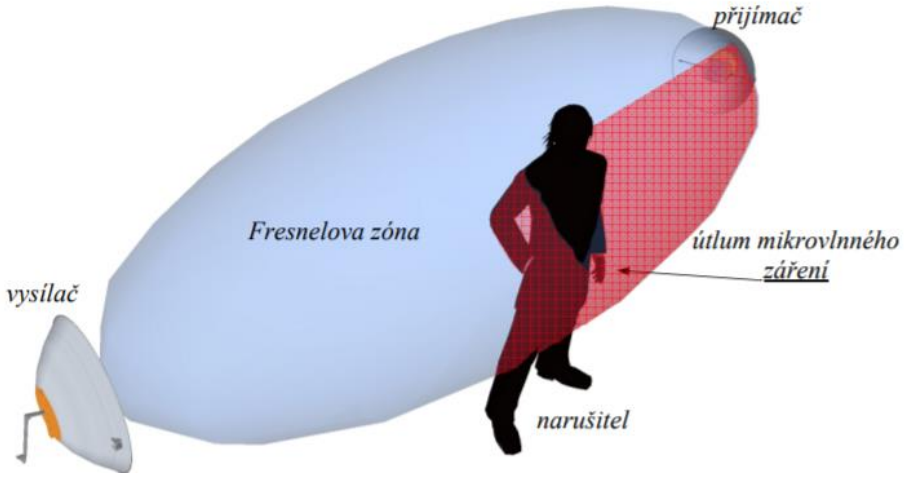
1.3.2 Metody detekce

Narušitel je u mikrovlnných detektorů detekován dvěma způsoby, a to metodou Fresnelovy zóny a metodou Dopplerova jevu.

1.3.2.1 Metoda Fresnelovy zóny

Tato metoda využívá toho, že mikrovlnné záření je snadno pohlceno nebo odraženo od okolních objektů. Používají se vysílací a přijímací parabolické antény. Střežený prostor je prostor mezi anténami, má tvar elipsoidu a nazývá se Fresnelova zóna.

Podstatou detekce je narušení Fresnelovy zóny. Lidské tělo je tvořeno z více jak 60% vody, proto při vstupu narušitele dojde k útlumu mikrovlnného signálu. Tato změna je detekována na přijímací anténě. Tato metoda detekce se využívá na mikrovlnné zábrany a bariéry, pro správnou funkčnost je také potřeba, aby se v chráněné zóně nevyskytovaly předměty, za které by se mohl narušitel schovat.



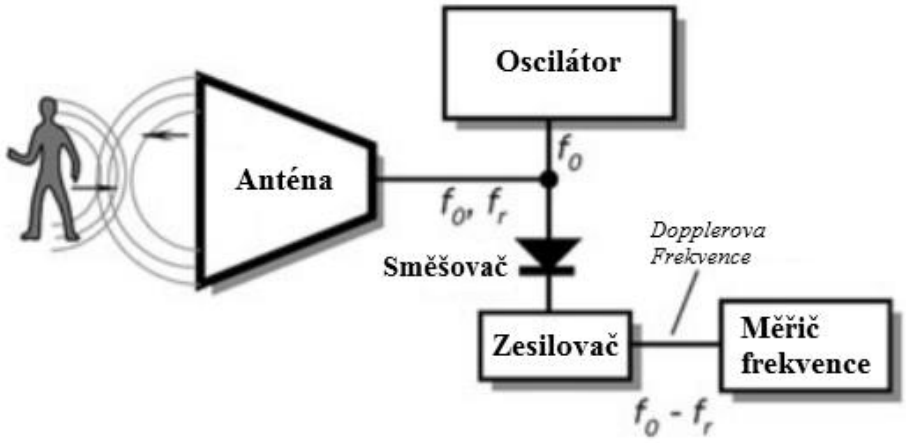
Obrázek 14 Metoda Fresnelovy zóny [12]

1.3.2.2 Metoda Dopplerova jevu

Dopplerův jev, jak již byl popsán v kapitole 1.2.2 je fyzikální děj, který nastává u jakéhokoliv vlnění a udává, že pokud se bude vysílač a přijímač vlnění vzájemně pohybovat nenulovou rychlostí, dojde ke změnám frekvence a vlnové délky mezi vysílaným a přijímaným signálem.

Metoda využívá rozdílu mezi vysílanou a přijímanou frekvencí a základem metody je tedy vysílač a přijímač mikrovlnného vlnění. Jsou umístěny v jednom bodě a chráněná oblast je ohraničena maximálním dosahem mikrovlnného vlnění, tedy zdmi místnosti. Při prvním spuštění je provedena detekční zkouška okolního prostředí a detektor si nastaví svůj výchozí kmitočet, přijatý kmitočet je poté uložen jako porovnávací hodnota. [12]

1.3.3 Součásti mikrovlnného detektoru



Obrázek 15 Blokové schéma mikrovlnného detektoru [17] (Přeložil autor)

f_o – frekvence oscilátoru

f_r – odražená frekvence

1.3.3.1 Gunn oscilátor

Jejich hlavním prvkem je Gunn dioda, která je umístěna v rezonanční dutině a skládá se ze dvou hlavních složek DC Bias a ladícího obvodu.

Gunn dioda

Nejedná se o klasickou diodu, pod kterou si představíme P-N přechod, ale jedná se o polovodičovou součástku, která se skládá ze tří vrstev typu N a neobsahuje žádnou vrstvu polovodiče typu P.

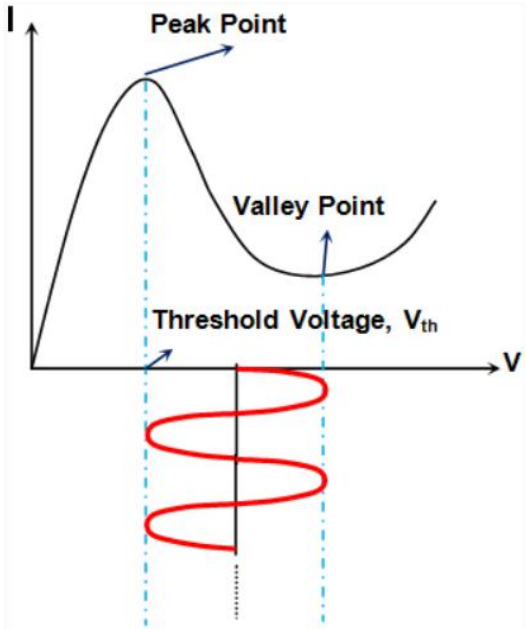
Dvě z těchto vrstev (krajní) jsou vysoce N-dopované (přidáním materiálu s vyšším množstvím elektronů ve valenční vrstvě, než mají atomy polovodiče), prostřední vrstva je užší a méně dopovaná. Častým materiálem na výrobu gunn diod je arsenid galia (Chemický vzorec GaAs). [18], [19], [20]

Obrázek 16 a) Gunn dioda b) Schématická značka [19]

DC Bias

Pokud budeme zvyšovat stejnosměrné napětí procházející gunn diodou tak se bude proud zvyšovat, dokud při prahovém napětí (Treshold Voltage) nedosáhne vrcholu (Peak Point). Poté se začne proud snižovat, dokud v údolí (Valley Point) nedosáhne poruchového napětí. Oblast mezi vrcholem a údolím se nazývá oblast záporného odporu.

Za předpokladu, že bude přes gunn diodu protékat optimální hodnota proudu, bude se chovat jako oscilátor. Důvodem je vlastnost záporného odporu zařízení , která vylučuje vliv skutečného odporu v obvodu, a to má za následek vznik kmitů.

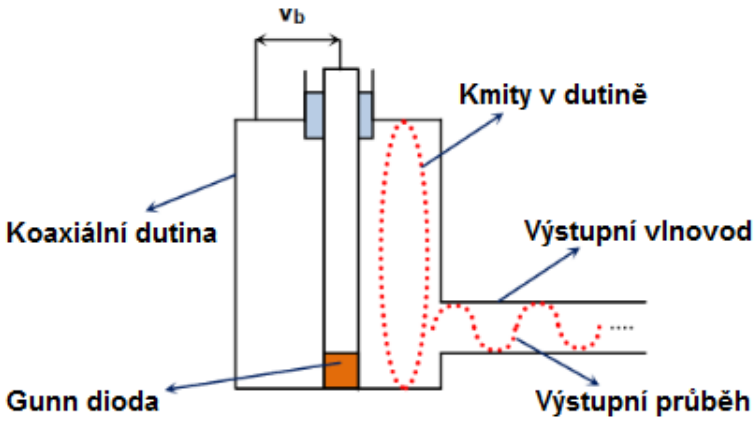


Obrázek 17 Kmity na Gunn diodě [21]

Ladící obvod

V případě Gunnových oscilátorů závisí frekvenci kmitání převážně na střední aktivní vrstvě Gunnovy diody. Frekvence však může být nastavena buď mechanicky nebo externě elektricky. Pro elektrické ladění se používá vlnovod, mikrovlnná dutina, varaktorová dioda nebo YIG koule. Mechanické ladění se provádí pomocí nastavovacího šroubu, kterým se mechanicky mění velikost dutiny nebo velikost magnetického pole v případě YIG koule.

Na následujícím obrázku je zobrazen koaxiální rezonátor založen na Gunn oscilátoru, který se používá ke generování frekvencí od 5 do 65 GHz. Pro frekvenci oscilátoru můžeme použít následující vzorec: $f = \frac{nc}{2l}$, kde n je počet vln, které se vejdou do dutiny pro danou frekvenci, l je délka dutiny a c je rychlost světla. [21], [22]



Obrázek 18 Oscilátor Gunn s koaxiální dutinou [21] (Přeložil autor)

1.3.3.2 Směšovací dioda

Směšovač je nelineární nebo parametrický obvod (obsahují nelineární prvky, např: diody). Jedná se o měnič kmitočtu, který dokáže obecně vytvořit nejrůznější kombinace obou vstupních signálů beze změny informačního obsahu. Obecný vzorec: $f_{mf} = kf_h + lf_s$, kde f_{mf} je kmitočet mezifrekvenční (získaný), f_h a f_s jsou vstupní kmitočty a koeficienty k a l nabývají hodnot celých čísel. V našem případě jde o rozdíl frekvence oscilátoru a referenčního kmitočtu tedy $fo - fr$. Nejjednodušším prvkem pro směšovač je polovodičová dioda. [23]

1.4 Magnetické detektory

Používají se k detekci otevření oken a dveří. Skládají se ze dvou částí, magneticky citlivého spínače a magnetu. Jejich výhodou je spolehlivost, jednoduchá instalace a cena. Velký problém s jednoduchými magnetickými detektory je, ale ten, že narušitel může při otevírání okna nebo dveří přiblížit magnet ke spínači a tím detektor oklamat. Nicméně detektor nemusí být viditelně na povrchu, ale může být skryt uvnitř dveří a tím narušiteli oklamáni detektoru značně ztížit. Tyto detektory také mohou pracovat bezdrátově a být napájeny z vlastní baterie. [24], [25]

1.4.1 Jazýčkový spínač (Reed Switch)

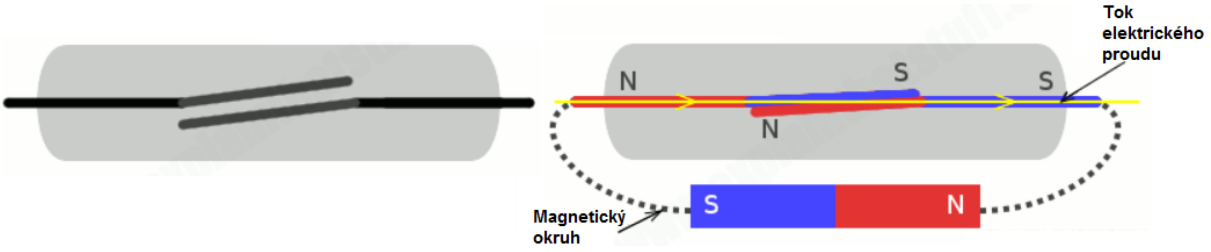
Klasický spínač se skládá ze dvou kontaktů, které spojí obvod při stisku tlačítka a po jeho uvolnění se zase vrátí do původní polohy, kolébkový spínač zase drží sepnutou nebo rozepnutou polohu. U jazýčkového spínače jsou kontakty spínány magnetickým polem, jejich vzdálenost je několik mikronů (miliontina metru), pohyb kontaktů není tedy pouhým okem viditelný.

Typický jazýčkový spínač má kontakty z feromagnetického materiálu (materiál lze jednoduše zmagnetizovat, například slitina železa a niklu) a jsou pokryty vrstvou odolného materiálu (rhodium nebo ruthenium). Tato vrstva zajistí delší životnost, při spínání a rozepínání kontaktů. Dále jsou kontakty uloženy ve skleněném pouzdru naplněném nereaktivním plynem, typicky dusíkem.

Obrázek 19 Jazýčkový spínač [26]

1.4.1.1 Normálně otevřený jazýčkový spínač

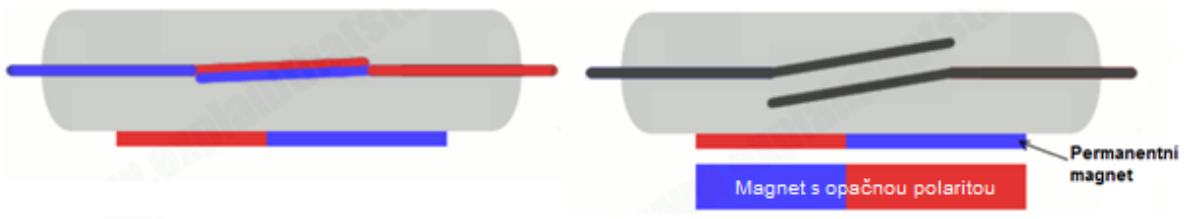
Při přiblížení magnetu ke spínači se celý spínač stane součástí magnetického obvodu. Kontakty jazýčkového spínače se stanou opačnými póly a spojí se. Nezáleží na tom, který konec magnetu se přiblížil první, vždy se polarizují tak aby se přitahovali. Tento spínač je tedy normálně otevřený (normálně rozepnutý), do té doby, dokud nepřiblížíme magnet a sepneme tak elektrický obvod. Při oddálení magnetu se kontakty opět rozepnou, protože jsou vyrobeny z pružného materiálu a vrátí se do původní polohy.



Obrázek 20 Normálně otevřený jazýčkový spínač [26] (Přeložil autor)

1.4.1.2 Normálně uzavřený jazýčkový spínač

Normálně uzavřený spínač je přesný opak otevřeného. Kontakty jsou normálně spojené, ale jen do doby, co se k nim přiblíží magnet, který je rozepne. Nejjednodušší způsob, jak vyrobit normálně uzavřený spínač je použít normálně otevřený spínač a permanentně připevnit magnet k jeho skleněnému pouzdru. Při přiblížení magnetu s opačnou polaritou k takto získanému uzavřenému jazýčkovému spínači se magnetická pole vyruší a kontakty se rozepnou. [26]



Obrázek 21 Normálně uzavřený jazýčkový spínač [26] (Přeložil autor)

1.5 Detektory rozbití skla

Detektory rozbití skla jsou vyrobeny a nastaveny tak, aby reagovaly na první trvalou změnu střežené plochy. Požadujeme u nich, aby dokázali detekovat zásahy jako vyřezávání otvoru diamantovým nářadím, ale zároveň nespustili poplach při přenosu vibrací z průjezdu dopravních prostředků, zvuku rozbíjených lahví nebo při zaklepání na okno.

1.5.1 Kontaktní detektory

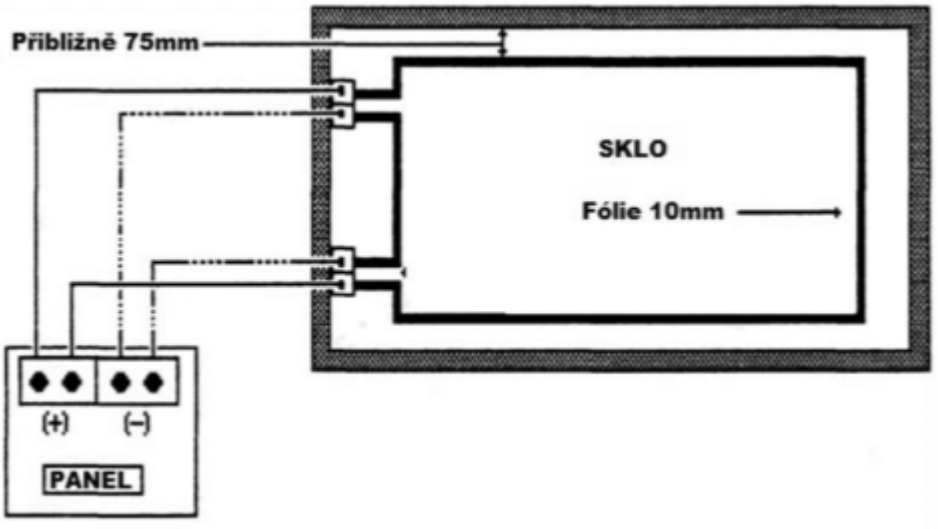
Tyto detektory jsou přímo v kontaktu s chráněnou plochou. Jejich princip je založen na vyhodnocování mechanických změn vyvolaných destrukcí skla.

1.5.1.1 Poplachové fólie, tapety a skla

Jejich princip je založen na přerušení vodivého média, kterým je vodivý drátek, nebo speciálně napařená vodivá cesta umístěná na chráněné ploše. Poplachová skla mají přímo z výroby vodivý drát zalitý ve skle, na rozdíl od fólií a tapet, které jsou realizovány pomocí polepů na sklo a je tedy mnohem jednodušší jejich montáž.

1.5.1.2 Fóliové polepy

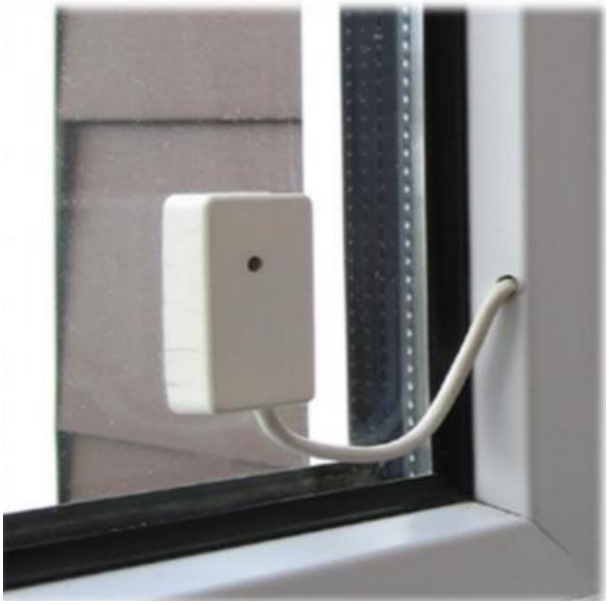
„Jsou realizovány jako tenká hliníková vodivá fólie, která je umístěna po obvodu chráněné skleněné plochy ve vzdálenosti 50 až 100 mm od rámu. Fólie je vyráběná v rozměrech na šířku 8 až 12 mm a s tloušťkou 80μ. Jejich činnost je založena stejně jako u poplachových fólií, tapet a skel na přerušení vodivého média a tím přerušení obvodu. Instalace fólie do poplachové smyčky se provádí v horní části okna, z důvodu nižší koncentrace kondenzovaných par, způsobující snižování spolehlivosti. Fóliové polepy nejsou odolné proti vyřezání otvoru mimo nalepenou plochu. Lze je tedy relativně lehce překonat.“



Obrázek 22 Fóliové polepy [27]

1.5.1.3 Pasivní kontaktní detektory

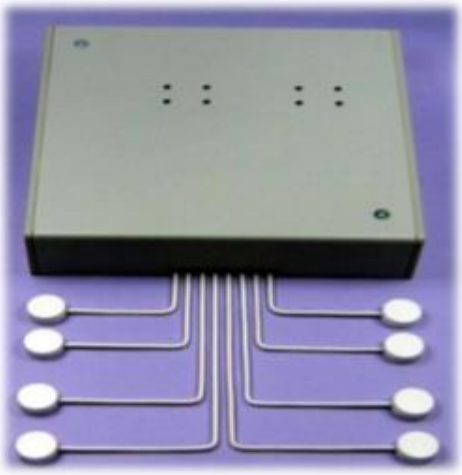
Jsou řazeny do kategorie elektromechanických detektorů. Jejich hlavní část je tvořena piezoelektrickým senzorem, naladěným na rezonanční kmitočet v rozmezí 40 kHz až 120 kHz. Tento senzor je nalepený na sklo a při mechanickém namáhání chráněné plochy generuje střídavé napětí, to je poté při určité úrovni vyhodnoceno jako poplach. Kmitočet odpovídá kmitání skleněné plochy, elektronika porovná tento kmitočet s kmitočty odpovídajícími tříštění, škrábání nebo řezání skla. Pro různé druhy skel se vyrábí odlišné typy detektorů a jejich dosah je závislý na šířce a typu skla. Detektor je na rozdíl od fóliových polepů v dolní části chráněné plochy ve vzdálenosti 5 cm od hrany rámu. Detektory jsou odolné proti rušivým zvukům a jsou tedy vhodné pro trvalé monitorování střeženého objektu, nicméně jejich nevýhodou je, nutnost použití samostatného detektoru pro jednotlivá skla a potřeba vývodu kabelu, který by měl směřovat do strany nebo dolů.



Obrázek 23 Pasivní kontaktní detektor [27]

1.5.1.4 Aktivní kontaktní detektory

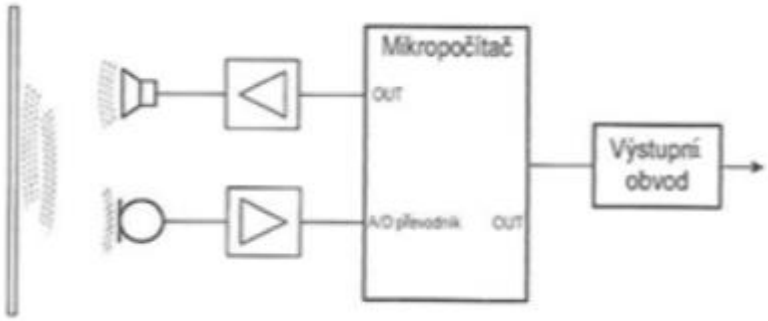
Skládají se z vyhodnocovací jednotky a dvou stejných senzorů (vysílač a přijímač) přilepených na tabuli skla. Princip je založený na vysílání vibrací vysílačem a ty jsou zachyceny přijímačem na jiném místě skla. Rozbití skla zapříčiní změnu signálu a tím je aktivován poplach. Monitorují se hodnoty frekvence, časový interval a odraz signálu. Výhodou těchto detektorů je, že po montáži nejsou nutné žádné seřizovací práce, jsou také velmi odolné proti planým poplachům, a to i při velkých změnách způsobených teplem, chladem nebo stárnutím oproti automatickému nastavení senzorů, nevýhodu je ale vyšší cena oproti jiným detektorům.



Obrázek 24 Aktivní kontaktní detektor [27]

1.5.2 Bezkontaktní detektory

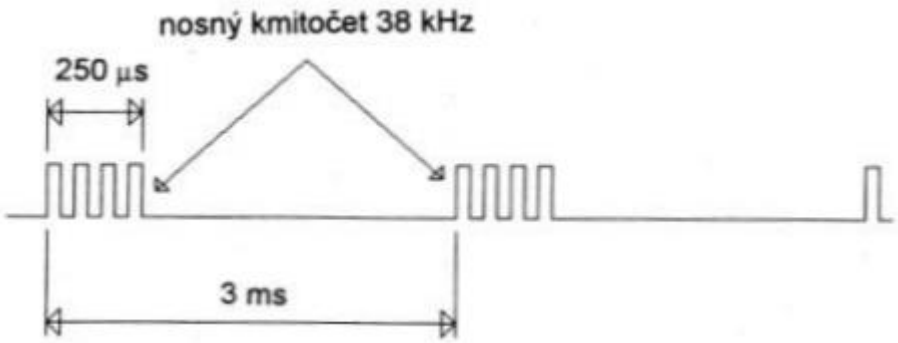
Tyto detektory nemají fyzický kontakt se střeženým objektem, ale hlídají plochu na dálku prostřednictvím aktivních nebo pasivních bezkontaktních detektorů rozbití skla. Aktivní detektory pracují v oblasti infračerveného záření nebo ultrazvuku a využívají ke své činnosti vysílání signálu, potřebného ke zjištění stavu skleněné plochy. Mají tedy část vysílací a část přijímací a vyhodnocují změny mezi vyslaným a přijatým signálem. Pasivní detektory snímají akustické vlny v prostoru, které jsou způsobeny destrukcí skla.



Obrázek 25 Princip činnosti aktivních bezkontaktních detektorů skla [27]

1.5.2.1 Aktivní infračervené detektory

Využívají ke své funkci vysílání a přijímání odraženého infračerveného paprsku, kterým se zjišťuje celistvost skleněné plochy. Vlnová délka infračerveného záření je v rozmezí 760 nm a 1 mm. Infračervený paprsek navíc bývá modulován, aby nebyla možnost nahradit vysílací zařízení jiným, které by imitovalo originální vysílací LED diodu. Poplach je spuštěn, pokud se vyslaný paprsek nevrátí, v potaz je zde brán i útlum signálu, který může být způsoben zaprášením detektoru nebo změnou odrazu chráněné plochy. Detektor i odrazná část musí být nastaveny tak, aby vyslaný paprsek byl přesně odražen na snímací část detektoru.



Obrázek 26 Příklad modulace infračerveného paprsku [27]

1.5.2.2 Aktivní ultrazvukové detektory

Detektory ultrazvuku jsou založeny na digitálním porovnávání frekvence přijatého signálu s vyslaným. V případě narušení skleněné plochy se změní frekvence odražené vlny. To je vyhodnoceno jako poplach, pokud se tato změna frekvence shoduje s frekvencí odpovídající tříštění skla, uloženou v paměti mikropočítače. Výhodou ultrazvukových detektorů je jejich velký dosah, který je 20 až 25 m. Nevýhodou, ale je, že jsou náchylné na plané poplachy způsobené proudícím vzduchem od zdrojů tepelného záření a výskytem pohyblivých předmětů před detektorem, proto je vhodné je umístit na protější stěnu od chráněné plochy se zajištěním volného zorného pole detektoru. Navíc není vhodné používat několik ultrazvukových detektorů v jedné místnosti, z důvodu vzájemného ovlivnění signálů. Řešením tohoto problému může být zajištění vzájemné synchronizace jednotlivých detektorů.

1.5.2.3 Pasivní bezkontaktní detektory rozbití skla

Tyto detektory vyhodnocují akustické vlnění v prostředí způsobené rozbíjením nebo řezáním skla. Detektory jsou pasivní, protože nevysílají do prostředí žádné signály, pouze detekují již zmíněné akustické vlnění. Detekce se provádí pomocí mikrofonu sloužícího jako převodník z akustického vlnění na elektrický signál. Následně se signál přenese ke zpracování do detektoru, a to analogově nebo digitálně. Podobně jako u ultrazvukového detektoru se vyhodnocuje poplach na základě shody při porovnání sejmutého signálu se vzorky signálu v paměti detektoru. Jednotlivé zvukové vzorky uložené v paměti odpovídají tloušťce a materiálu, ze kterého je sklo vyrobeno. [27]

2 KAMEROVÉ SYSTÉMY

Kamerový systém nebo anglicky CCTV (Closed-circuit television), je systém, který umožňuje sledovat živé kamerové přenosy a rekordér archivuje záběry pro pozdější použití. Kamerové systémy jsou v dnešní době velmi rozšířené a nemusí jít jen o hlídání samotného objektu, aby nedošlo k vloupání, krádežím nebo vandalizmu. Ale mohou být použity i jako kontrola zaměstnanců nebo pro monitorování dopravy. [28]

2.1 Princip získání obrazu

Moderní kamerové systémy používají digitální video, neukládají tedy informaci ve formě po sobě jdoucích fotografiích, ale obrazy jsou uloženy ve formě řetězce čísel. K získání obrazu používají obrazový snímač, tedy světlo citlivý mikročip CCD (z anglického Charge-coupled device) nebo CMOS (Complementary Metal-Oxide-Semiconductor). [29]

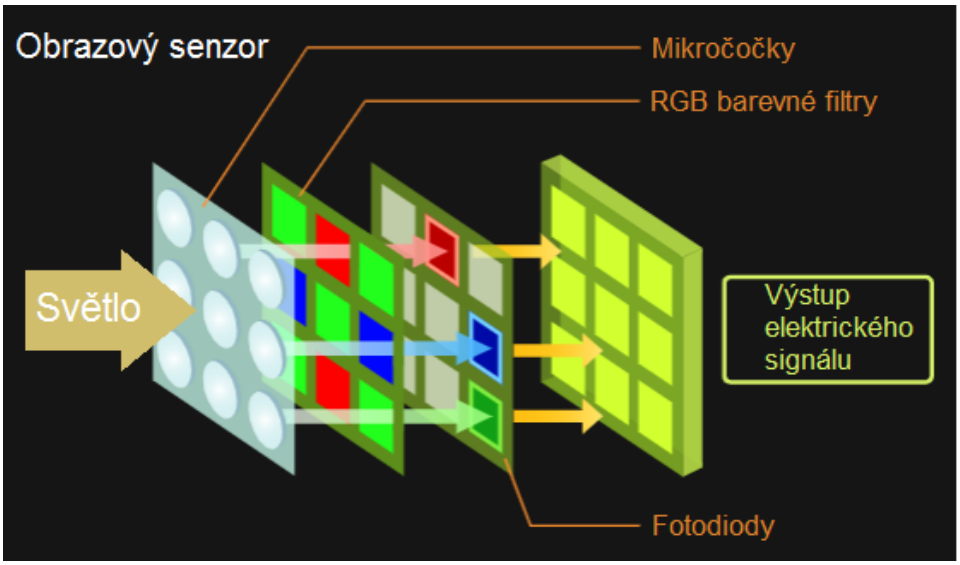
2.1.1 Obrazový snímač

CCD mikročip vynalezli Willard S. Boyle a George E. Smith, dva kolegové pracující u Bell Laboratories v roce 1969. Jedná se o polovodičový čip vytvořený z milionů světlo citlivých čtverců uspořádaných v mřížce. Tyto čtverce se nazývají pixely, označení kamery v mega pixelech tedy udává, kolik milionů pixelů kamera má.

CCD je analogový optický čip, který přeměňuje světlo na elektrické signály, které jsou předány dalším čipům, které je digitalizují. Má pole kondenzátorů, každý z nich nese elektrický náboj odpovídající intenzitě světla pixelu. Kontrolní obvod, převede náboj z každého kondenzátoru do jeho souseda a poslední kondenzátor předá svůj náboj zesilovači. Tento přenos dat pomocí kbelíkové brigády (bucket-brigade) je charakteristický pro CCD snímače.

Oproti tomu obrazový senzor CMOS má fotodiodu a CMOS tranzistorový spínač pro každý pixel, což umožňuje signálům pixelu, aby byly individuálně zesíleny. Ovládáním matice přepínačů, může být k signálům přistoupeno přímo a postupně, ve vyšších rychlostech než u CCD snímačů. Jako další výhoda je snížení šumu, který je způsoben čtením elektrických signálů převedených ze zachyceného světla a nižší cena než CCD. [30]

Ať už jsou obrazy generovány pomocí CMOS senzoru nebo CCD a dalšími prvky obvodu, princip je stejný. Čočka kamery zachytí světlo z objektu, a to je senzorem rozděleno na jednotlivé pixely. Senzor vyhodnotí barvu a světlost jednotlivých pixelů a uloží informaci v binárním kódu. [29], [30]

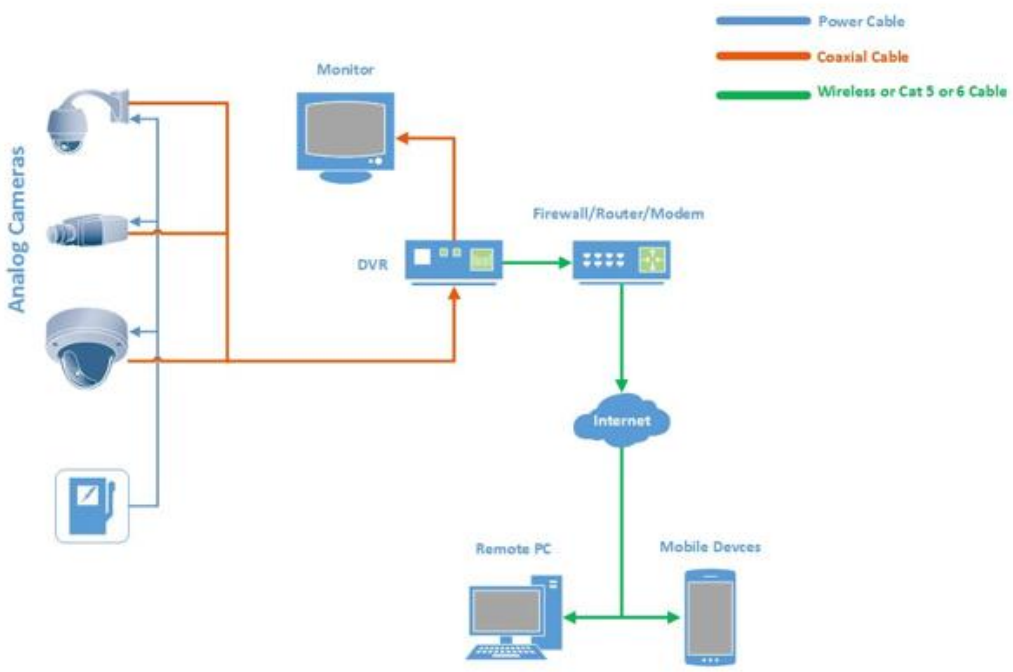


Obrázek 27 Obrazový senzor [30] (přeložil autor)

2.2 Analogové CCTV

U analogových kamer je digitální signál získaný obrazovým snímačem převeden opět na analogový (formát NTSC/PAL), aby ho bylo možné přenést po koaxiálním kabelu. Analogový signál je poté poslán k digitálnímu videorekordéru (DVR) Ten přemění video z analogového signálu na digitální, zkomprimuje a uloží ho na pevný disk, obvykle po dobu třiceti dnů. K zobrazení videa je DVR připojen k monitoru, případně může být připojen k routeru s modemem, aby bylo možné přenášet video po vnitřní síti. [31], [32]

Digitální videorekordér se používá k záznamu a zpracování videa, spoléhá na AD kodér, který je zodpovědný za převedení surových dat z kamery na čitelné videozáznamy. Jejich cena je nižší než NVR (Network Video Recorder), který je používán u IP kamer, a protože obraz je zpracován na rekordéru, tak mají i nižší nároky na kameru. Nevýhodou je to, že je nutné připojení každé kamery k rekordéru a koaxiální kabely také nepředávají kameře napájení, což má za následek vyšší počet kabelů, než je tomu u systému IP kamer. [33]

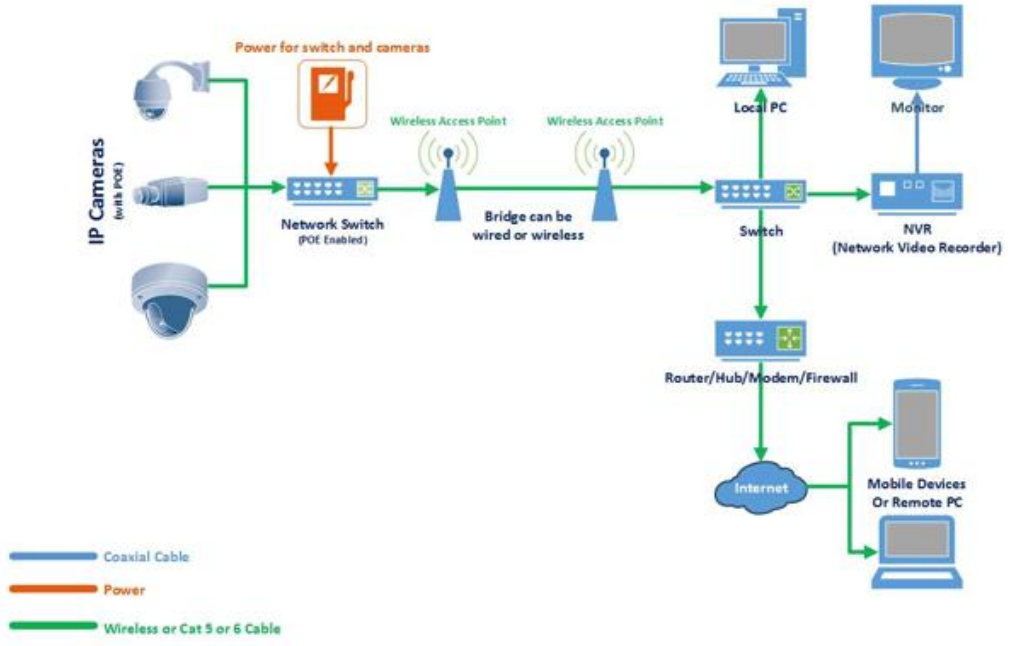


Obrázek 28 Analogový kamerový systém [32]

2.3 Digitální CCTV

Digitální systém nebo také IP (Internet Protocol), jsou kamery, které nepotřebují DVR, ale namísto toho používají NVR (network video recorder). Jedná se o software, který běží na počítači nebo serveru, případně je to samostatné zařízení. Videosignál, který je již v digitální podobě, není potřeba převádět na analogový a obrazy jsou uloženy na novém nebo existujícím síťovém RAIDu (redundant array of independent disks), tak jak je směrováno pomocí softwaru NVR.

Protože je každá kamera samostatným malým počítačem dokáže provádět i pokročilejší funkce jako detekce pohybu, nebo automatické spuštění záznamu. Podle nastavení systému mohou být obrazy také poslány e-mailem, uloženy na interní paměťovou kartu nebo poslána do externího paměťového zařízení. [32]



Obrázek 29 Digitální kamerový systém [32]

2.4 Druhy kamer podle konstrukce

Analogové i digitální kamery jsou vyráběny v různých konstrukčních provedeních, aby bylo možné je využít v různých aplikacích. Budete mít například rozdílné požadavky na kameru, pokud chcete chránit venkovní prostory, kde bude kamera odolávat vlivům počasí, jiné požadavky budete mít pro střežení zboží uvnitř obchodu.

2.4.1.1 Kamery typu Dome

Dome kamery jsou převážně pro vnitřní použití pro montáž na strop nebo stěnu. Jejich jméno pochází z anglického dome = kopule, ve které je kamera uložena. Tato pouzdra jsou dělána, aby kamera nebyla tak nápadná, mohou mít také zesílenou konstrukci, která dokáže odolat útoku na kameru. Navíc přes tuto kopuli není tak lehké odhadnout kam kamera směřuje. Tyto kamery je možné manuálně natáčet, také obsahují funkci automatického pohybu kamery v daných intervalech, což umožňuje pokrytí velkého prostoru pouze jednou kamerou, nebo k předejití špatných světelných podmínek v určitém času dne.

Obrázek 30 Dome kamera [34]

2.4.1.2 Bullet kamery

Tyto kamery mají dlouhý, válcový a zúžený tvar, který připomíná náboj do pušky, proto tedy anglický název bullet = střela. Často se používají na aplikace, které potřebují zobrazení velkých vzdáleností. Mnoho bullet kamer je voděodolná, protože jsou nainstalovány uvnitř ochranného pouzdra, které chrání před prachem, deštěm a nečistotami.

Obrázek 31 Bullet kamera [34]

2.4.1.3 C-mount kamery

Kamery mají vyměnitelné čočky a hodí se tedy pro rozdílné aplikace. Standardní CCTV čočky, dokáží pokrýt vzdálenosti 35 až 40 stop (10,7 až 12,2metru), proto je možnost vyměnit čočky pro pokrytí větších vzdáleností. Kamery jsou efektivní pro použití uvnitř budovy, ale jejich velké rozměry je činí velice nápadné, což ale může odradit případného narušitele.

Obrázek 32 C-mount kamera [34]

2.4.1.4 Termovizní/Infračervené kamery

Tyto kamery jsou časté na letištích nebo přístavech, kde poskytují kvalitní záznamy 24 hodin denně. Infračervené kamery mají malé LED obklopující objektiv, které pomáhají zachytit pohybující se postavy i v naprosté tmě. Termokamery dokáží pracovat na velké vzdálenosti a to 250–300 metrů.

Obrázek 33 Termovizní/Infračervená kamera [34]

2.4.1.5 Denní/noční kamera

Tento druh kamer dokáže pracovat jak v dobře, tak i špatně osvětleném prostředí. Jsou ideální pro venkovní aplikace, kde využití infračervených kamer není optimální. Denní/noční kamery nemají infračervené iluminátory, protože dokáží zachytit čistý obraz i v šeru pomocí svých velmi citlivých obrazových senzorů. Mohou pracovat nepřetržitě jak při silném slunečním světle, jsou odolné proti oslnění a nevadí jim ani silné zadní světlo.

Obrázek 34 Denní/noční kamera [34]

2.4.1.6 Síťové/IP kamery

Kamery mohou mít jak drátové, tak bezdrátové provedení. Obraz přenáší přes internet, záznamy mohou být tedy jednoduše zobrazeny i z velké vzdálenosti od střeženého objektu.

Využití mají jak pro společnosti, tak i pro domácí použití. Výhodou je i méně kabeláže, než je tomu u analogových kamer, nevýhodou je nárok na síť, protože přenášená data mohou mýt velké objemy.

Obrázek 35 IP kamera [34]

2.4.1.7 HD kamery

Kamery s vysokým rozlišením jsou použity v rizikových zařízeních jako jsou banky nebo kasina. Zachytí kvalitní obraz každého, kdo vstoupí a odejde, aby byla zajištěna vysoká bezpečnost a maximální ochrana. Umožňují přiblížení při zachování velice dobré kvality obrazu, což zajišťuje nezpochybnitelnost, pokud by záznamy měli být použity u soudu.

2.4.1.8 Varifokální kamery

Varifokální kamery umožňují upravit ohniskovou vzdálenost, úhel nebo zmenšit zoom bez ztráty ostrosti, což je ideální pro čtvercovou místnost. Kde by za normálních okolností kamery s pevnou čočkou měli „mrtvou zónu“.

2.4.1.9 Kamery PTZ

PTZ tedy pan, tilt and zoom, jsou kamery, které se dokáží otáčet doprava a doleva (panning = posouvání), nahoru a dolů (tilting = naklápění), také mají přiblížení/oddálení (zoom). Kamery jsou použity v případě, že je v budově strážný u kamer, který si upraví kameru podle potřeby.

Obrázek 36 PTZ kamera [34]

2.4.1.10 Skryté kamery

Jedná se o miniaturní kamery, které umožňují diskrétní pořízení záznamu. mohou být maskovány jako běžné předměty a dokáží pořídit záběr z krádeže, aniž by to tom narušitel věděl. To také snižuje možnost poškození kamery během krádeže. [34], [35]

2.5 Přenos signálu

Pro přenos videosignálu k zobrazovacímu, případně záznamovému zařízení se existuje několik variant. Analogový přenos pomocí koaxiálního kabelu, datového kabelu po krouceném páru, použitím optického kabelu nebo bezdrátovým přenosem. Pro digitální datový přenos se využívá protokol TCP/IP po síti LAN nebo bezdrátové síti.

Analogové kamerové systémy využívají hvězdicové instalace kabeláže, mají tedy vždy jeden kabel pro přenos videosignálu od každé kamery k rekordéru. Každá kamera také potřebuje napájení 12 V, které může být přivedeno společně s videosignálem pomocí speciálních kabelů a redukcí. Druhá možnost, jak zajistit napájení je použití samostatného zdroje, připojeného na 230 V pro každou kameru samostatně. Toto řešení se ale příliš nedoporučuje, protože výpadek proudu může způsobit vyřazení kamerového systému z provozu, navíc vyžaduje volnou zásuvku u každé kamery a znemožňuje případnou instalaci centrálního napájení pro celý kamerový systém.

Systémy IP kamer používají pro komunikaci síťové kabely používané v počítačových sítích, tedy kabely označené jako Cat.5, Cat.5E nebo Cat.6. Napájení kamer je podobné jako u analogových systémů, každou kameru je možné napájet samostatně napájecím zdrojem v místě instalace, nebo pomocí redukcí vzdáleně po kabelu. Mohou ale také využívat Power over Ethernet, tedy být napájeny po datovém kabelu. [36], [37]

2.5.1 Koaxiální kabely

Koaxiální kabely se dělí podle impedance na dvě hlavní skupiny 75Ω a 50Ω. Impedance vyjadřuje odpor, který klade kabel střídavému elektrickému proudu. Kabely 75Ω se používají pro přenos videosignálu, zatímco 50Ω se používají na přenos dat a pro bezdrátovou komunikaci.

Koaxiální kabel je nejčastěji složen ze čtyř různých vrstev. Střed kabelu obsahuje vodič, obvykle měděný drát, který přenáší data. Ten je obalen dielektrickým izolantem s přesně definovanou elektrickou charakteristikou. Kolem izolantu je pletená síť nebo kovová fólie typicky z mědi nebo hliníku, která chrání před elektromagnetickým rušením. Poslední vrstvou je venkovní izolace.

Obrázek 37 Koaxiální kabel [38] (přeložil autor)

2.5.1.1 Koaxiální kabel RG-6

Tyto kabely mají širší vodič, to zajišťuje lepší kvalitu signálu, vrstva dielektrika je silnější a obalena rozdílnými druhy stínění, pro lepší zvládnutí frekvencích v řádech GHz. Kabely jsou tenké a mohou být instalovány do zdí nebo stropů. Jsou lepší volbou než RG-59 pro digitální video a pokud frekvence přesahuje 50MHz.

Obrázek 38 Koaxiální kabel RG-6 [39]

2.5.1.2 Koaxiální kabel RG-59

Jedná se o běžný kabel pro domácí použití, který je dobrou volbou pro nízkofrekvenční přenosy, je podobný RG-6, ale centrální vodič je tenčí. Přestože RG-6 dokáže přenášet video signál beze ztrát na delší vzdálenosti, jeho pevnější konstrukce a tloušťka nedovoluje, aby se s ním pracovalo tak dobře jako s RG-59. Proto je pro kamerové systémy a analogové video lepší volbou RG-59. [38], [39]

Obrázek 39 Koaxiální kabel RG-59 [39]

2.5.1.3 Plug and play kabely

Jedná se o standardní Audio/Video kabel označený jako RCA. Konektory jsou barevně označené jako žlutý a bílý pro video a zvuk s RCA konektory, červený konektor je určen pro napájení. Pro přenos videosignálu z kamery je potřeba použití redukce na konektor BNC, případně je z výroby již tento konektor na nasazen. Tyto kabely, ale nejsou stíněné tak dobře jako RG-59 siamský kabel, proto se nedoporučuje je používat na vzdálenosti delší než 150 stop (45,75m).

Obrázek 40 Koaxiální plug and play kabel [40]

2.5.1.4 RG-59 siamský kabel

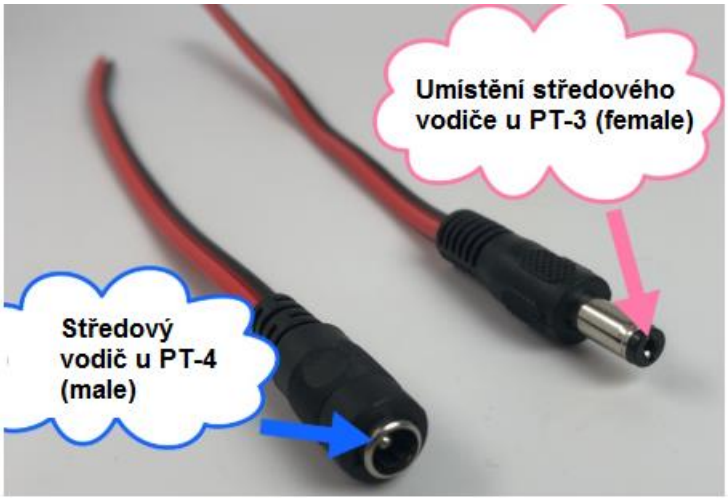
Stejně jako kabely Plug and play obsahuje siamský kabel jak koaxiální kabel, tak napájení. Jeho výhodou je, ale lepší stínění, a tedy možnost přenosu signálu na větší vzdálenosti. Jsou také odolnější než plug and play kabely. Jejich nevýhodou je složitější montáž, protože je potřeba je upravit na potřebnou vzdálenost a nasadit konektory, běžně používané konektory jsou BNC pro koaxiální kabel a PT-3 pro napájení. [41]

Obrázek 41 Siamský koaxiální kabel [42]

2.5.1.5 Napájecí konektory PT-3, PT-4

PT-3 napájecí kabely se používají k propojení siamského kabelu kamery, ke zdroji stejnosměrného napětí. Pracují s napětím 12 V a průměr konektoru je 2,1mm, což je standardní velikost používaná v nízkonapěťových aplikacích.

Na straně kamery bývá konektor PT-4, jedná se o samčí konektor (Male) do kterého, pasuje konektor PT-3 (Female). Proto může být matoucí, který konektor je samčí a který samičí, protože na první pohled by se to mohlo snadno zaměnit, nicméně označení není podle venkovního vzhledu, ale podle pozice středového, jak je znázorněno za následujícím obrázku.



Obrázek 42 Napájecí konektory PT-3, PT-4 [41] (přeložil autor)

2.5.1.6 BNC konektor

Konektory BNC (Bayonet Neill-Concelman) jsou malé konektory pro rádiové frekvence na rychlé připojení/odpojení koaxiálních kabelů. Konektor samice(Female) obsahuje dva malé výstupky a pro pojení stačí čtvrt otočky matice na samčím(Male) konektoru. Vyrábějí se ve verzích 75 Ω a 50 Ω stejně jako koaxiální kabely, pro které jsou použity.

Konektory 75 Ω používají frekvence až 2 GHz a jak již bylo zmíněno dříve, koaxiální kabel se u kamerových systémů se používají k přenosu Video signálu. [43]

Obrázek 43 BNC Konektor [43]

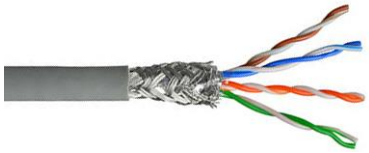
Obrázek 44 Rozdíl mezi 75 Ω a 50 Ω BNC konektory [43]

2.5.2 Síťové kabely

Síťové kabely, se kterými se běžně setkáme, využívají technologie krouceného páru. Jedná se o propletení dvou vodičů tak, že v jednom se proud pohybuje jedním směrem a druhým se pohybuje opačným. Toto způsobí, že pole, vznikající kolem vodičů se vyruší. Tímto způsobem je možné posílat data přes značné vzdálenosti, bez nutnosti použití dalších opatření. Protože jeden síťový kabel obsahuje několik kroucených párů, je počet křížení na jednotku délky odlišný pro každý pár. Počet je založen na prvočíslech, aby nemohlo dojít ke shodě, čímž se snižuje přeslech v kabelu.

Kabely mohou být stíněné nebo nestíněné, přidáním stínění uvnitř kabelu se snižuje vliv elektromagnetického rušení (EMI), radiofrekvenční rušení (RFI) a přeslech. U značení kabelů se používá písmen U, S, F a poslední dvě písmena jsou TP, což označuje křížený pár (Twisted pair). U znamená unshielded (nestíněný), S pro shielded (stíněný) a F je pro stínění pomocí folie. Například F/UTP tedy znamená, že kabel je stíněn pomocí fólie a kroucené páry nemají stínění žádné. Přehled používaných značení kabelů je v následující tabulce. [44], [45], [46]

Tabulka 1 Druhy stínění síťových kabelů [44]

Název	**Typ stínění kabelu**	**Typ stínění krouceného páru**	**Příklad**
U/UTP	Žádné	Žádné	
F/UTP	Fólie	Žádné	
S/UTP	Opletení	Žádné	
SF/UTP	Opletení i fólie	Žádné	
U/FTP	Žádné	Fólie	
F/FTP	Fólie	Fólie	
S/FTP	Opletení	Fólie	
SF/FTP	Opletení i fólie	Fólie	

Síťové kabely se dále dělí do jednotlivých kategorií, které mohou být v lankovém nebo pevném provedení vodičů. Lankové provedení má pro každý vodič několik měděných vláken zkroucených dohromady, jsou tedy ohebnější a jsou vhodnější tam kde se očekává časté přesouvání kabelu. Pevné provedení není tak pružné, ale je odolnější a je tedy lepší pro trvalé instalace jako umístění do zní nebo pod podlahu.

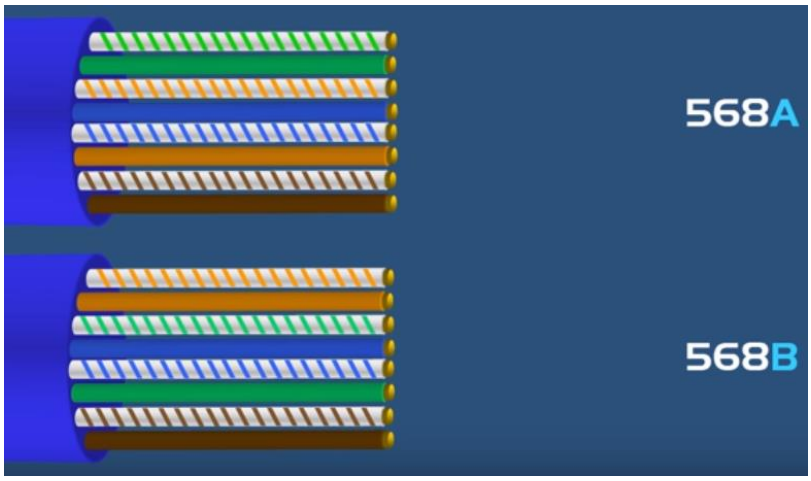
Kategorie 5 nahradila dříve používané Cat 3, ale nyní už je zastaralá a nepodporuje dnes běžné přenosové rychlosti, proto se budování nových instalací s touto kategorií se nedoporučuje. Konektorem u většiny kategorií je RJ45, nicméně vyšší kategorie jako Cat 7 mohou mít konektor GG45 (GigaGate45), ten je ale zpětně kompatibilní s Rj45, není tedy nutné měnit celou instalaci, při přechodu na Cat 7. [46]

Tabulka 2 Dělení síťových kabelů podle kategorie [46], [47]

Kategorie	Stínění	Maximální přenosová rychlost	Maximální šířka pásma (bandwidth)
Cat 3	Nestíněný	10 Mbps	1 MHz
Cat 5	Nestíněný	100 Mbps	100 MHz
Cat 5e	Nestíněný	1 Gbps	100 MHz
Cat 6	Stíněný / nestíněný	10 Gbps	250 MHz
Cat 6a	Stíněný	10 Gbps	600 MHz
Cat 7	Stíněný	10 Gbps	1000 MHz
Cat 8	Stíněný	40 Gbps	2000 MHz

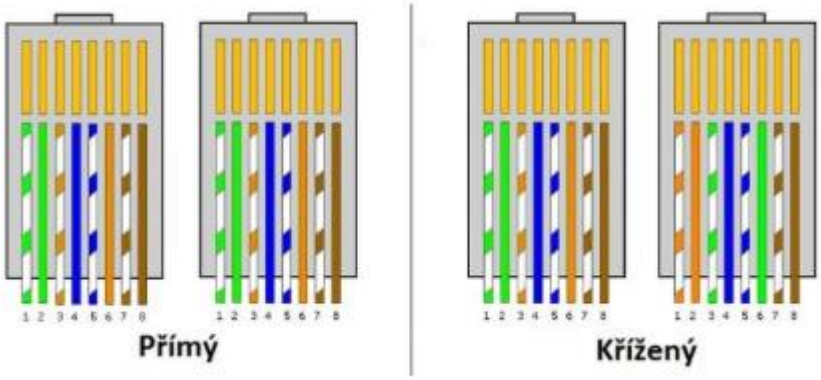
2.5.2.1 Konektor RJ45

Konektor RJ45 (Registered Jack 45) je v podstatě standardem pro síťové kabely. Jedná se o osmi pinové plastové konektory, u kterých rozlišujeme dva druhy zapojení 568A a 568B, jejich rozdílem je prohození vodičů zelené a oranžové barvy, což je znázorněno na následujícím obrázku.



Obrázek 45 Rozdíl mezi 568A a 568B [48]

Tímto získáme dva druhy kabelů, kabel přímý, který má na obou koncích stejné zapojení (nezáleží na tom, zda typ A nebo B). Kabel křížený má na jednom konci zapojení 568A a druhý konec 568B.



Obrázek 46 Zapojení přímého a kříženého kabelu [45]

Přímé kabely se používají pro propojení rozdílných zařízení jako například počítač a switch. Kabely křížené jsou na propojení stejných zařízení (PC-PC, Switch-Switch). Dnešní síťové karty a routery dokáží rozpoznat, druh připojeného kabelu a dokáží si signály vnitřně upravit. Nicméně je lepší používat správný druh kabelu, protože může nastat situace, kdy je potřeba vyměnit některou komponentu sítě za starší a ta by potom nemusela fungovat. [45], [46], [48]

2.5.2.2 Power over Ethernet

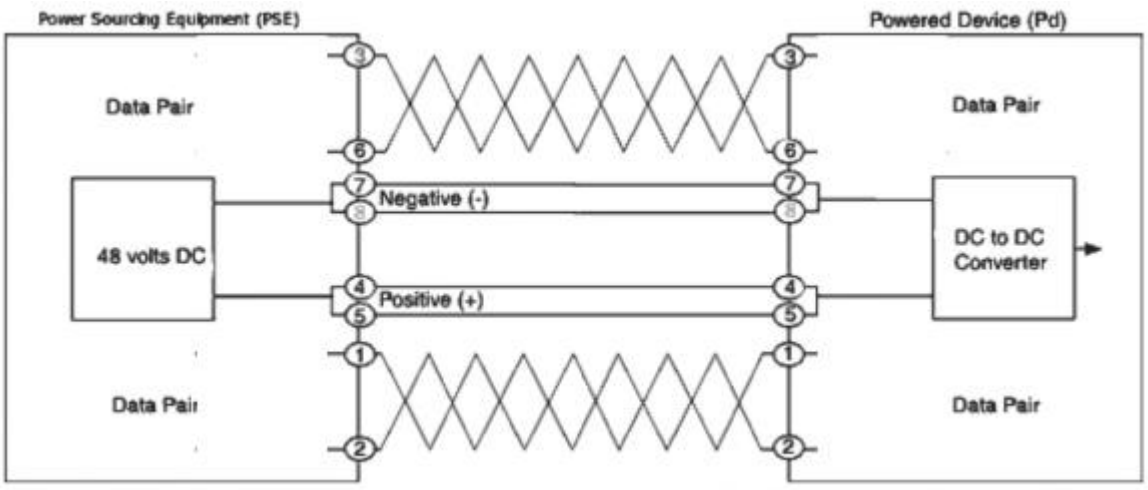
Power over Ethernet ve zkratce (PoE), je schopnost síťového kabelu, přenášet s daty i napájení. Na rozdíl od siamského kabelu, který je použit u analogových kamer, zde není nutné mít v jednom pouzdře dva kabely, ale dá se použít klasický síťový kabel, obvykle Cat 5e.

U Power over Ethernet rozlišujeme dva druhy zařízení, zařízení, která dodávají napájení (Power Sourcing Device – PSE) a zařízení, které je napájeno (Powered Device – PD). Napájení je přenášeno po datových vodičích (Mód A) nebo po volných vodičích (Mód B). Napájená zařízení jsou konstruována tak, aby dokázala přijmout napájení jak módem A, tak i B. Zařízení dodávající mají povoleno používat pouze jeden mód, to zajišťuje, že napájené zařízení není zničeno, pokud je připojeno ke špatnému napájecímu zařízení.

Tenké dlouhé vodiče, které obsahuje síťový kabel, budou mít značný odpor (například pro 100m 10Ω), proto není možné poslat pouze napětí, které je vyžadováno zařízením, ale musí být zvýšeno, a to na 40-57 voltů, aby byli pokryty ztráty. Toto napětí je přivedeno na oba vodiče v krouceném páru. Na napájeném zařízení je potom převodník, který zajistí snížení tohoto napětí na potřebnou hodnotu.

Mód B

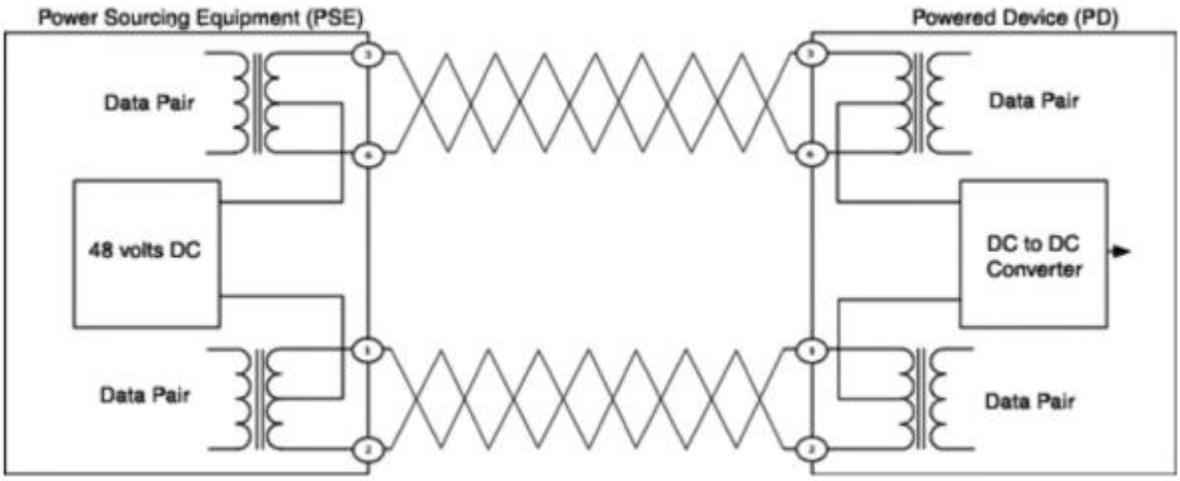
Standardy pro přenos dat 10BASE-T a 100BASE-TX (Fast ethernet) využívají pro komunikaci pouze dva kroucené páry, máme tedy druhé dva páry volné a můžeme je využít pro napájení.



Obrázek 47 Power over Ethernet Mód B [49]

Mód A

Standard 1000BASE-T (Gigabit ethernet) a jeho následníci využívají pro přenos dat všechny čtyři kroucené páry. Napětí je zde přeneseno na vodičích společně s daty. Aby bylo odděleno, jsou na obou koncích datového páru transformátory, které přenášejí střídavý proud, lze je tedy využít k oddělení signálu a stejnosměrného proudu. [49]



Obrázek 48 Power over Ethernet Mód A [49]

2.5.2.3 Wi-Fi přenos

Digitální bezdrátové kamery využívají pro přenos standardu IEEE 802.11x, tedy Wi-Fi. Standard využívá několik šifrovacích metod, pro větší bezpečnost přenášených dat. Během přenosu jsou data zašifrována a přijímač je poté pomocí bezpečnostního klíče dešifruje.

IEEE 802.11x pracuje ve dvou frekvencích 2,4GHz a 5GHz. Frekvence elektromagnetických vln určuje šířku pásma a vzdálenost pokrytí. Pro vyšší frekvenci je dosah kratší. Frekvence 2,4GHz má tedy větší dosah, ale je používána například mobilními telefony nebo mikrovlnnými troubami, a to může způsobovat rušení. Z tohoto důvodu je preferována frekvence 5Ghz, přestože je dražší. [50]

IEEE 802.11x nebo jen IEEE 802.11 není jednotným standardem, ale spíše souborem standardů a pro Wi-Fi typy jsou standardy následující.

802.11a

Přenáší až 54 megabitů dat za sekundu frekvencí 5 GHz. Také používá OFDM (orthogonal frequency-division multiplexing), efektivní kódovací techniku, která rozdělí rádiový signál do několika dílčích signálů předtím, než se dostanou k přijímači, to výrazně snižuje rušení.

802.11b

Jedná se o nejméně nákladný a nejpomalejší ze standardů. Díky nízké ceně byl dříve populární, ale protože cena rychlejších standardů klesá, tak již nebývá tak běžný. 802.11b vysílá ve frekvenčním pásmu 2,4GHz rádiového spektra. Přenosová rychlost je až 11 megabitů za sekundu a ke zvýšení rychlosti používá modulaci doplňkového klíčování kódu (CCK).

802.11g

Přenáší na 2,4GHz stejně jako 802.11b, ale je mnohem rychlejší. Zvládá přenos 54 megabitů dat za sekundu. Rychlejší je proto, že používá stejné kódování jako 802.11a.

802.11n (Wi-Fi 4)

Je zpětně kompatibilní a rychlost je vyšší než jeho předchůdců, dokáže přenášet až čtyři proudy dat každý maximálně 150 megabitů za vteřinu. Nicméně většina routerů dovoluje pouze dva až tři proudy.

802.11ac (Wi-Fi 5)

Standard je z počátku roku 2013 a je zpětně kompatibilní se standardem n. Není tak náchylný k rušení jako jeho předchůdci a přenáší až 450 megabitů za sekundu na jeden proud. S využitím až osmi proudů, může překročit rychlost gigabitu za sekundu, proto se mu občas přezdívá gigabit Wi-Fi.

802.11ax (Wi-Fi 6)

Jedná se o nejnovější standard, u kterého připojení budou rychlejší a stabilnější než Wi-Fi 5. Umožní připojit více zařízení a přenosová rychlost bude 10 až 12 gigabajtů za vteřinu. [51], [52], [53]

3 OCHRANA SÍTĚ

Zabezpečení sítě zahrnuje protokoly, technologie, zařízení, nástroje a techniky pro zabezpečení dat a zmírnění hrozeb. Ochrana sítě je snaha být o krok napřed před hackery, protože prolomení zabezpečení může narušit elektronický obchod, umožnit přístup k soukromým údajům nebo způsobit ztrátu obchodních údajů. To může mít za následek ztrátu příjmů společnosti, krádeže duševního vlastnictví nebo dokonce ohrozit veřejnou bezpečnost. [54]

3.1 Druhy sítí podle rozlohy

Máme různé druhy sítí a kategorizovat je můžeme podle jejich velikosti a jejich účelu. Velikost sítě je vyjádřena jejím geografickým pokrytím a počtem počítačů, které jsou součástí této sítě. Nejznámější typy sítí jsou PAN, LAN, MAN a WAN.

3.1.1 Osobní síť (Personal Area Network – PAN)

PAN je počítačová síť vytvořená v osobním dosahu. Obecně se skládá z počítače, mobilního telefonu nebo digitálního asistenta. Pan lze použít k navázání komunikace mezi těmito osobními zařízeními, nebo pro připojení k internetu.

Zařízení, která běžně používají síť PAN jsou bezdrátové myši, klávesnice nebo systém bluetooth. PAN může být také připojen bezdrátově k internetu a potom je označován jako WPAN. Nejznámější drátová verze sítě PAN je USB.

Výhodou PAN je že jsou relativně bezpečné a nabízí možnost přenosu na krátké vzdálenosti. Nevýhodou je jejich dosah, který je jen do deseti metrů a to, že mohou navázat nekvalitní připojení k jiným sítím ve stejných rádiových pásmech.

3.1.2 Místní síť (Local Area Network – LAN)

LAN je skupina počítačů a periferních zařízení, která jsou připojena v omezeném prostoru obvykle jedna budova. Ale může se jednat i o síť propojenou několika budovami, která má, ale méně než 5000 připojených zařízení. Nejjednodušším typem sítě LAN je propojení tiskáren a počítačů v domácnosti nebo kanceláři, a to může být jak drátově klasickou kroucenou dvojlinkou, tak i bezdrátově s využitím Wi-Fi.

Výhodou LAN je snížení finančních nároků na hardware, protože pevné disky, DVD-ROM i tiskárny mohou být lokálně sdíleny. Také stejný software může být použit pro každého klienta v síti a také nabízí sdílení jednoho internetového připojení mezi všemi uživateli LAN. Další výhodou je jednoduché sdílení dat v síti a možnost uložení dat všech uživatelů sítě na jednom pevném disku počítačového serveru. Spravování dat pouze na jednom místě zvyšuje jejich bezpečnost.

Nevýhodou jsou počáteční náklady, které jsou poměrně vysoké. LAN neposkytuje příliš velké soukromí, protože správce sítě má možnost prohlížet soubory každého uživatele. Dalším problémem je, že neautorizovaní uživatelé mohou mít přístup k důležitým datům, pokud správce LAN nezabezpečil centralizované uložiště dat.

3.1.3 Rozlehlá síť (Wide Area Network – WAN)

Síť WAN, která je další důležitá počítačová síť se rozkládá po velké geografické oblasti. Většinou je omezena na podnik nebo organizaci a k propojení se používají optické kabely, nebo bezdrátové mikrovlnné, infračervené nebo satelitní přenosy. Nejznámější sítí WAN je internet, který je kolekce propojení jiných LAN a WAN.

Nevýhodou sítí WAN jsou vysoké počáteční náklady a její udržování není snadné, proto potřebuje kvalifikované techniky a správce sítě. Vzhledem k širokému pokrytí a používání různých technologií se také může vyskytovat více chyb a problémů, které vyžadují více času na opravy, protože je zapojeno více kabelových a bezdrátových technologií. Posledním nedostatkem je zabezpečení, které je nižší ve srovnání s jinými typy sítí.

3.1.4 Metropolitní síť (Metropolitan Area Network – MAN)

Metropolitní síť se skládá z počítačové sítě, která je napříč městem, univerzitním kampusem, nebo malou oblastí. Tento typ sítě je větší než LAN, která je obvykle omezena jednou budovou. Podle konfigurace může síť MAN pokrýt oblast několika mil po několik desítek mil (1míle = 1,6km), obvykle ale v okruhu max 50km. Přenosovým médiem bývají kabely s optickými vlákny nebo mikrovlnný bezdrátový přenos.

Pomocí optických vláken poskytuje rychlou komunikaci, vynikající podporu pro rozsáhlou síť a lepší přístup k WAN. Duální sběrnice v síti MAN poskytují podporu pro současný přenos dat v obou směrech.

Nevýhodou MAN je nutnost více kabelů k navázání spojení z jednoho místa na druhé. Také zabezpečit tuto síť proti hackerům je velice náročné. [55], [56]

3.1.5 Virtuální privátní síť(Virtual Private Network – VPN)

VPN je privátní síť, která používá veřejnou síť, obvykle internet, k připojení uživatelů. Virtuální je proto, že přenáší informace uvnitř soukromé sítě, ale ta informace je vlastně přenášen přes veřejnou síť. Privátní vyjadřuje to, že je provoz šifrován, aby data zůstala soukromá při přenosu přes veřejnou síť. Virtuální připojení může být z podnikové soukromé sítě nebo služby VPN třetích stran, která je bezplatná nebo placená. [54], [55]

Hlavní výhody VPN jsou:

1) Rozšiřitelnost – VPN umožňuje organizaci použití internetu k jednoduchému přidání nových uživatelů, bez nutnosti rozšiřování infrastruktury
2) Redukce nákladů – S příchodem nových technologií s velkou šířkou pásma o přijatelné ceně, mohou společnosti využít síť VPN na snížení nákladů na připojení a současně zvýšit šířku pásma vzdáleného připojení.
3) kompatibilita – VPN lze implementovat přes celou řadu technologií, včetně širokopásmových technologií.
4) bezpečnost – VPN zajišťuje nejvyšší úroveň zabezpečení, použitím pokročilého šifrování a ověřovacích protokolů, aby byla data ochráněna před neautorizovaným přístupem.

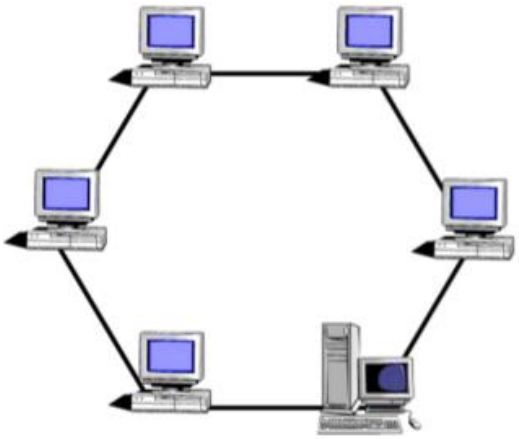
VPN existují dva základní typy, VPN vzdáleného přístupu(remote-access) a site-to-site VPN. VPN vzdáleného přístupu se automaticky vytvoří, pokud není VPN informace staticky nastavena, místo je umožněno, aby se informace o připojení dynamicky měnila. Site-to-site je vytvořena, pokud obě strany ví o VPN připojení, VPN pak zůstává statická a interní zařízení nemusí vědět, že VPN existuje, protože dostávají normální TCP/IP provoz přes bránu VPN, což může být například router, firewall nebo Cisco VPN concentrator. Tato VPN brána má za úkol zapouzdření a šifrování provozu, který ho pošle VPN tunelem přes internet na vzdálenou VPN bránu, ta odstraní hlavničky, dešifruje obsah a předá paket cílovému hostiteli. [54]

3.2 Rozdělení sítí podle topologie

Topologie počítačové sítě vyjadřuje, jak jsou prvky v této síti uspořádány. Těmito prvky mohou být jak počítače, tak i různé propojovací prvky.

3.2.1 Topologie kruhová (RING)

Každý počítač je přímo propojen s následujícím i předchozím prvkem v kruhu. Využívá se v síti MAN, v LAN jen velmi zřídka. Výhodou této topologie je lehká rozšiřitelnost, malé množství spojů a snadné vyslání zprávy. Nevýhodou je, ale že výpadek v libovolném místě způsobí výpadek celé sítě. Další nevýhodou je velké nebezpečí odposlechu síťové komunikace, procházející přes spojovací počítače.

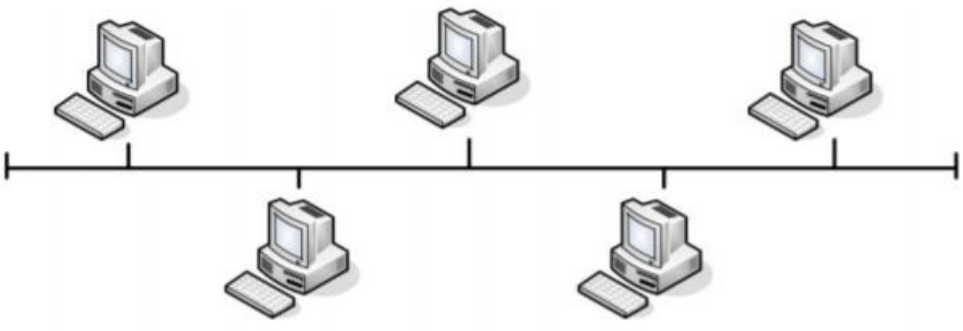


Obrázek 49 Kruhová topologie [57]

3.2.2 Topologie sběrnicová (BUS)

Tato topologie byla používaná na začátku devadesátých let, ale dnes se příliš nepoužívá. Všechny počítače jsou zde připojeny na pasivní společné médium, které sdílejí, býval to koaxiální kabel, pomocí kterého se jednotlivé počítače připojily do sítě.

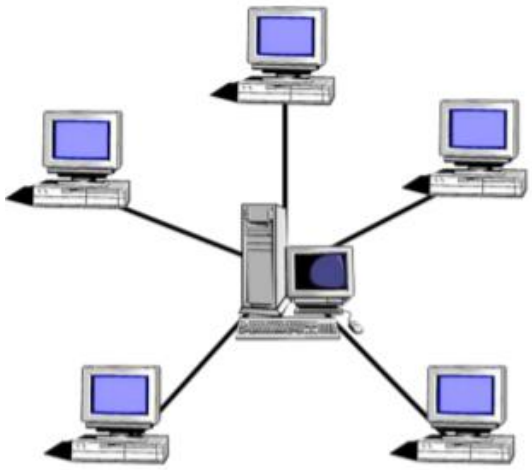
Výhodou takového uspořádání bylo snadné všesměrové vysílání, neexistence aktivních prvků a cena. Jednotlivé stanice také nebyli závislé na výpadku jiné. Nevýhodou bylo určení, kdo bude mít přístup ke společnému médiu (kdo bude vysílat), také výpadek tohoto média, vyřadil celou síť.



Obrázek 50 Sběrnicová topologie [57]

3.2.3 Topologie hvězda (STAR)

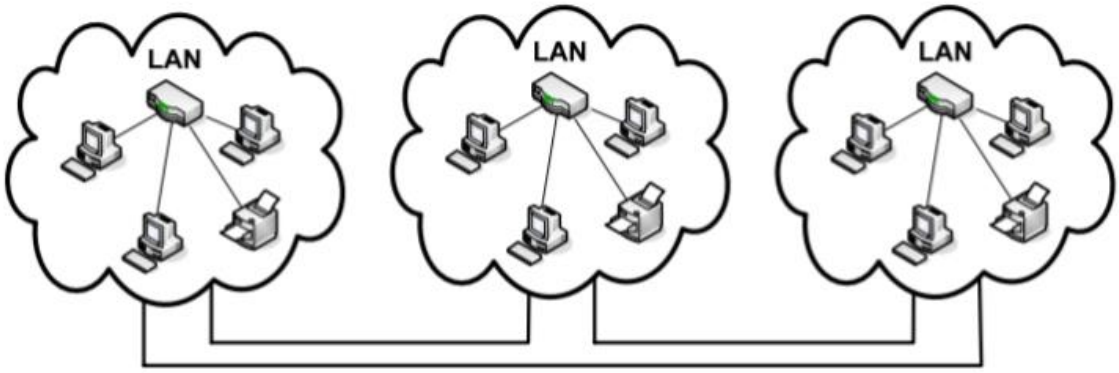
Jedná se o nejpoužívanější topologii v sítích LAN. Existuje zde centrální prvek (HUB, SWITCH), který spojuje všechny prvky. Výhodou je lehké rozšiřitelní struktury a výpadek libovolné stanice nevyřadí celou síť. Při použití aktivních prvků typu SWITCH je většina síťové komunikace skryta před ostatními účastníky sítě, a to zvyšuje bezpečnost. Nevýhodou je větší množství kabeláže, náročnější montáž a nutnost použití hubu nebo switche.



Obrázek 51 Hvězdicová topologie [57]

3.2.4 Páteřní topologie

Páteřní topologie vyjadřuje situaci, kdy celé sítě LAN propojujeme pomocí určité topologie. Může být zapojena jako kruh, sběrnice nebo hvězda, nejčastěji se ale používá kruh. Jejím základem je hlavní nezávislá část, která propojuje důležité celky a na ni se naopak připojují různé subsítě nebo segmenty. Páteř může mít vyšší přenosovou rychlost a při výpadku libovolného segmentu není provoz na páteři ovlivněn. [57]



Obrázek 52 Páteřní topologie [57]

3.3 Druhy útoků na sítě

Útoky na síť dělíme do dvou kategorií útoky z venku (External threats) a útoky zevnitř (Internal threats). Externí útok může být například, když hacker chce prolomit síť přes internet ve snaze narušit síťové operace a vytvořit DoS útok (Denial of Service). Ten má za následek, že síť není schopná podporovat požadavky uživatelů. Útok zevnitř má na svědomí například zaměstnanec, který ukradne a zkopíruje důvěrná data, odpojí kritické síťové připojení a způsobí výpadek sítě, nebo připojí zavirovanou jednotku přes USB, k podnikovému počítačovému systému. Interní hrozby mají tedy potenciál způsobit mnohem větší škody, protože interní uživatelé mají přímý přístup do budovy a znají podnikovou síť.

3.3.1 Průzkumové útoky (Reconnaissance Attacks)

Jde o shromažďování informací, podobně jako když zloděj obhlíží dům, který chce vykrást. Hacker tento útok používá k neoprávněnému mapování systémů, služeb nebo zranitelných míst. Útoky často předcházejí útokům na přístup nebo útokům DoS a často využívají široce dostupné nástroje.

Postup útoku může být následující

1) Informační dotaz – Na zjištění základních informací o cíli se dá použít mnoho nástrojů včetně vyhledávání Google, webových stránek organizací, whois a dalších.
2) Ping sweep – Informační dotaz obvykle odhalí síťovou adresu cíle, hacker poté může zahájit ping sweep, kterým určí, které IP adresy jsou aktivní
3) Skenování portů (Port scan) – Určení, které porty nebo služby jsou k dispozici. Pro tyto účely se dá použít například Nmap, SuperScan, Angry IP Scanner nebo NetScan Tools.
4) Zahájit sken zranitelnosti (Vulnerability Scan) – Snahou je určit typ a verzi aplikace a operačního systému, který běží na cílovém hostiteli. Nástroje k tomu jsou Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT a Open VAS.
5) Zneužití zranitelnosti (Exploitation tools) – Hacker hledá zranitelné služby, které lze využít, nástrojů je celá řada, například Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit nebo Netsparker.

3.3.2 Přístupové útoky (Access Attacks)

Přístupové útoky využívají známé slabiny v zabezpečení v ověřovacích službách, FTP (File transport protocol) a webových službách k získání přístupu k webovým účtům, důvěrným databázím a dalším citlivým informacím.

Existuje šest běžných typů přístupových útoků

1) Útok na heslo – Hacker se pokouší objevit kritická systémová hesla pomocí různých metod, jako je sociální inženýrství, slovníkový útok (dictionary attack), útok hrubou silou (brute force attack) nebo odposlouchávání (sniffing). Útoky hrubou silou zahrnují opakované pokusy s použitím nástrojů jako Ophcrack, L0phtCrack, THC Hydra, RainbowCrack a Medusa.
2) Zneužití důvěry (Trust exploitation) – Hacker používá neautorizovaná oprávnění k získání přístupu k systému.
3) Přesměrování portů – Hacker používá nabouraný systém jako základnu pro útoky proti jiným cílům
4) Útoky typu člověk uprostřed (man-in-the-middle) – Hacker se nachází mezi dvěma legitimními entitami, aby mohl číst nebo upravovat data, která prochází mezi oběma stranami.
5) Přetečení vyrovnávací paměti (Buffer overflow) – V tomto případě se hacker snaží přeplnit vyrovnávací paměť neočekávanými hodnotami, to obvykle způsobí nefunkčnost systému a vytvoří útok DoS.
6) IP, MAC,DHCP Spoofing - Při spoofing útoku se jedno zařízení snaží tvářit jako jiné, falšováním dat. K falšování MAC adres například dochází, když jeden počítač přijímá datové pakety založené na MAC adrese jiného počítače. [54]

3.3.2.1 Sociální inženýrství

Sociální inženýrství je přístupový útok, který se snaží zmanipulovat jednotlivce, aby provedli akce, které by hackerovi pomohli, nebo mu sdělili důvěrné informace. Často spoléhají na ochotu lidí pomoci, nebo cílí na jejich slabé stránky. Příkladem nástrojů sociálního inženýrství jsou:

1) Pretexting – V tomto případě hacker zavolá zaměstnanci ve snaze získat přístup k privilegovaným datům. Například předstírá, že potřebuje osobní nebo finanční údaje, aby potvrdil totožnost příjemce.
2) Phishing – Je poslání podvodného e-mail, který je maskován jako z legitimního zdroje. Záměrem je přimět příjemce k instalaci malwaru do zařízení, nebo ke sdílení osobních nebo finančních informací.
3) Spear phishing – Jedná se o cílený phishingový útok přizpůsobený konkrétní osobě nebo organizaci.
4) Spam – Pomocí spamového e-mailu, chce hacker přimět uživatele ke kliknutí na infikovaný odkaz nebo ke stažení infikovaného souboru.
5) Tailgating – Hacker zde následuje autorizovanou osobu do zabezpečené oblasti, kam by se jinak nedostal.
6) Něco za něco (Something for Something) – Hacker požádá o osobní informace výměnou za něco jiného, například dárek zdarma.
7) Baiting – Toto je situace, kdy hacker nechá fyzické zařízení napadené malwarem, například USB flash, na veřejném místě. Nálezce jej připojí do svého počítače a tím neúmyslně nainstaluje malware. [54]

3.3.3 Odepření služby (Denial of Service – DoS)

Útoky typu DoS jsou velice časté, jejich následkem je přerušení služby uživatelům, zařízením nebo aplikacím. Jsou velkým rizikem, protože mohou snadno přerušit obchodní proces a způsobit značné ztráty. Tyto útoky jsou také relativně jednoduché provádět i nekvalifikovaným útočníkem. Existují dva hlavní zdroje útoků DoS:

1) Škodlivě formátované pakety(Maliciously Formatted Packets) – Jedná se o případ, kdy je škodlivý paket předán hostiteli nebo aplikaci a příjemce nemůže zvládnout neočekávaný stav. Například hacker předává pakety obsahující chyby, které aplikace nemůže identifikovat, nebo předává pakety nesprávně formátované. To způsobí selhání nebo zpomalení přijímacího zařízení.

2) Ohromující množství provozu (Overwhelming Quantity of Traffic) – To je situace, kdy síťový hostitel nebo aplikace nedokáže zpracovat obrovské množství dat, což způsobí zhroucení systému nebo jeho extrémní zpomalení.

3.3.3.1 Útoky DDoS

Distribuovaný útok DoS je podobný útoku DoS, rozdílem je to, že DDoS pochází z více koordinovaných zdrojů. U DDoS se používají termíny botnet, manipulační systémy (handler system) a zombie počítače. Botnet je síť infikovaných počítačů, kterou vytvořil hacker. Infikované počítače se nazývají zombie počítače a jsou ovládány manipulačním systémem. Zombie počítače pokračují ve skenování a infikování dalších cílů a vytvářejí tak nové zombie. Když je hacker připraven, dá příkaz botnetu, pomocí manipulačního systému a zahájí útok DDoS. [54]

3.4 Malware

Malware je prostředek, který hackeři používají k nalezení a rozšíření bezpečnostních slabin. Hlavní druhy malware jsou viry, trojské koně a červy.

3.4.1 Viry

Virus je škodlivý software, který v počítači provede určitou nežádoucí, většinou škodlivou činnost nebo funkci. Je to škodlivý kód, který bývá připojen ke spustitelným souborům obvykle legitimních programů a většina virů tak vyžaduje aktivaci koncovým uživatelem. Nejběžnější šíření virů je pomocí e-mailů, další možností šíření jsou paměťová zařízení USB, CD a DVD.

Jednoduchý virus se může nainstalovat na první řádek kódu a když je aktivován tak zkontroluje disk na jiné spustitelné soubory, aby mohl infikovat všechny soubory, které ještě nebyli infikovány.

Viry mohou být jak neškodné, že například zobrazí obrázek na obrazovce, nebo mohou být destruktivní, které odstraňují nebo upravují soubory pevného disku. Aby se zabránilo detekci tak můžou viry i mutovat.

3.4.2 Trojský kůň

Trojský kůň obvykle obsahuje škodlivý kód, který se tváří jako něco jiného, jako aplikace nebo soubor. Trojský kůň, přichází se skrytým škodlivým kódem a provádí škodlivé operace, zatímco se tváří, že probíhají požadované funkce. Trojské koně využívají oprávnění uživatelů, kteří je spouští. Často jsou trojské koně připojeny k online hrám, ale pokud jsou trojské koně napsány na míru se specifickým cílem, je obtížné je odhalit.

Při hraní hry si uživatel nevšimne žádného problému. Zatímco na pozadí se trojský kůň nainstaluje na uživatelův systém. Škodlivý kód poté pokračuje v činnosti i po ukončení hry.

Trojské koně mohou mít různý charakter, mohou způsobit okamžité poškození, poskytnout vzdálený přístup do systému, nebo provádět instrukce, které jsou mu na dálku předány, jako například „každý týden mi odešli soubor s heslem“.

Trojské koně dělíme podle způsobeného poškození nebo podle způsobu, kterým narušují systém:

- Trojský kůň se vzdáleným přístupem (Remote-access Trojan horse) – Jak název napovídá, tento typ umožňuje neoprávněný vzdálený přístup.
- Trojský kůň odesílající data (Data-sending Trojan horse) – Posílá citlivá data jako jsou hesla.
- Destruktivní trojský kůň (Destructive Trojan horse) – Poškozuje nebo odstraňuje soubory.
- Proxy trojský kůň – Tento typ využije napadený počítač jako základnu k zahájení dalších útoků a ilegálních aktivit.
- FTP Trojský kůň – Umožní nepovolený přenos souborů mezi koncovými zařízeními.
- Trojský kůň deaktivující bezpečnostní software (Security software disabler) – Zastavuje antivirové programy a vypíná firewall.
- DoS Trojský kůň – Zpomaluje nebo zastavuje síťové aktivity.

3.4.3 Červ

Červ provede zadaný kód a nainstaluje jeho kopie do paměti infikovaného počítače. Sám se replikuje a šíří po síti ze systému na systém, napadené sítě potom většinou zpomaluje. Na internetu se nikdy nezastaví, jak jsou vypuštěny, tak pokračují v šíření, dokud nejsou opraveny všechny možné zdroje infekce.

Zatímco virus vyžaduje spuštění hostitelského programu, červi mohou běžet sami. Uživatele potřebují jen k počáteční fázi infekce, dokáží se potom velmi rychle šířit po síti. Proto jsou červi zodpovědné za některé z nejničivějších útoků internetu, například v roce 2003 byl vypuštěn virus SQL Slammer, který dokázal nakazit více jak 250 000 hostitelů za 30minut.

Většina útoků červů se skládá ze tří složek:

1) Umožnění zranitelnosti (Enabling vulnerability) – Červ se nainstaluje do systému pomocí zranitelného mechanizmu, jako je e-mailová příloha, spustitelný soubor nebo trojský kůň.
2) Propagační mechanismus (Propagation mechanism) – Po získání přístupu k zařízení se červ replikuje a hledá nové cíle.
3) Datový obsah (Payload) – Jedná se o škodlivý kód, který má za následek nějakou akci, nejčastěji se snaží vytvořit zadní dvířka do systému, aby je mohl využít pro DoS útok. [54]

3.4.4 Další druhy malware

Malware se neustále vyvíjí, zde je několik příkladů moderního malwaru:

- Ransomware – Tento malware zakáže přístup k infikovanému počítači. Ransomware pak požaduje, aby uživatel zaplatil za to, aby byl odstraněn.
- Spyware – Používá se ke shromažďování informací o uživateli a zasílání těchto informací někomu jinému, bez vědomí uživatele. Spyware se dělí na monitorování systému, trojské koně, Adware, sledovací cookies a key loggery.
- Adware – Tento malware obvykle zobrazuje otravná vyskakující okna, aby získal peníze pro svého autora. Malware může také analyzovat zájmy uživatelů, sledováním navštívených webových stránek a vytvářet vyskakovací okna s reklamou na ně. [54]
- Scareware – Malware tohoto typu zahrnuje podvodný software, který pomocí sociálního inženýrství chce přinutit uživatele k návštěvě malwarem infikovaných stránek. Může se tvářit jako zpráva od antiviru, že byl počítač infikován, uživatel si pak ve strachu z této hrozby zakoupí podvodný malware, který se tváří jako antivir. [54], [58]
- Phishing – Tento typ se snaží přiměn uživatele, aby mu vyzradit citlivé informace. Příkladem může být podvodný e-mail od banky s požadavkem na zadání čísla účtu a PIN kódu.
- Rootkit – Tento malware je nainstalován na napadeném systému, kde se skrývá a udržuje privilegovaný přístup pro hackera.

Tento seznam se nesjpíše dále bude rozšiřovat, protože s růstem internetu se neustále vyvíjejí nové druhy malware. [54]

3.5 Zabezpečení sítě

Pro zabezpečení sítě je důležité průběžné vzdělávání a neustálá ostražitost. Je potřeba zabezpečit celou síťovou infrastrukturu, ta zahrnuje směrovače (router), přepínače (switch), koncové body (endpoints) a další zařízení.

Doporučené postupy pro zabezpečení sítě jsou následující:

- Písemné vypracování bezpečnostní politiky společnosti
- Vzdělávání zaměstnanců o rizicích sociálního inženýrství a používání dalších úrovní zabezpečení jako telefonické nebo e-mailové ověření
- Zabezpečit fyzický přístup k systémům
- Použití silných hesel a jejich častá obměna
- Šifrovat a chránit citlivá data
- Implementovat bezpečnostního hardware a software, jako jsou brány firewall, IPS, VPN, antivirový software a použít filtrování obsahu
- Zálohovat a pravidelně kontrolovat zálohované soubory
- Vypnout nepotřebné služby a porty
- Udržovat systémy aktualizované
- Provádět bezpečnostní audit, který otestuje síť proti útoku

3.5.1 Zmírnění dopadu malware

Tyto techniky jsou často označovány jako protiopatření, primárním prostředkem ke zmírnění útoků je antivirový software. Ten pomáhá snížit riziko napadení a zabraňuje šíření škodlivého kódu. Přičemž je mnohem méně časově náročné udržovat antivirus aktuální než čistit infikovaný počítač. Antivirus běží na počítačích a serverech, kde detekují a odstraňují viry, nezabrání ale vniknutí virů do sítě, proto je potřeba, aby odborník na zabezpečení sítě měl přehled běžných virových útocích a sledoval aktualizace týkající se nově vzniklých virů.

3.5.2 Zmírnění dopadu červů

Červi jsou více síťově založené než viry, zmírnění jejich dopadu vyžaduje pečlivost a koordinaci s odborníky v oblasti zabezpečení sítě. Reakce na útok se dá rozdělit do čtyř částí:

1) Containment (Zadržení) – Fáze zahrnuje omezení šíření infekce v místech, která byla napadena. To vyžaduje rozčlenění (compartmentalization) a segmentaci sítě ke zpomalení nebo zastavení šíření červa a zabránění napadeným hostitelům v infikování dalších systémů. Vyžaduje použití příchozích i odchozích seznamů ACL (Access control list) na routerech a firewallech v kontrolních bodech sítě.
2) Inoculation (Očkování) – Fáze očkování běží paralelně se zadržovací. Všechny systémy, které dosud nebyli infikovány dostanou příslušný patch, tím červ přijde o možné cíle.
3) Quarantine (Karanténa) – Karanténa zahrnuje nalezení a identifikování infikovaných stanic, které odpojí, zablokuje nebo odstraní. To izoluje tyto systémy pro fázi léčby.
4) Treatment (Léčba) – Léčba zahrnuje aktivní odstranění infekce ze systémů. To může zahrnovat zastavení procesu červa, odstranění modifikovaných souborů nebo systémových nastavení, která červ upravil. Také je potřeba opravit slabinu v systému, kterou červ využil. Ve vážnějších případech je nutné systém reinstalovat, aby bylo zajištěno, že byl červ a všechny jeho vedlejší produkty odstraněny.

3.5.3 Zmírnění průzkumových útoků

Průzkumové útoky obvykle předcházejí útokům k získání neoprávněného přístupu nebo narušení síťových funkcí. Pro zjištění probíhajícího útoku se dají nakonfigurovat alarmy, které se spouštějí při překročení určitých parametrů například počet požadavků ICMP (Internet Control Message Protocol) za sekundu. K monitorování tohoto typu činnosti lze použít celou řadu technologií a zařízení, například adaptivní bezpečnostní zařízení (Adaptive Security Appliance – ASA), kterou poskytuje společnost Cisco.

Techniky zmírnění průzkumných útoků zahrnují:

1) Implementace ověření identity (autentizace), aby byl zajištěn pouze řádný přístup
2) Použití šifrování, zachycená data nejdou číst a paketový sniffing je nepoužitelný
3) Použití detekčních nástrojů, které odhalí sniffing útoky (anti-sniffer)
4) Implementace přepínané infrastruktury (switched infrastructure)
5) Použití firewall a systém prevence průniku IPS (Intrusion Prevention Systems)

Softwarové a hardwarové nástroje proti sniffing útokům detekují změny v době odezvy hostitelů a dokáží tak určit, zda zpracovávají více provozu, než je jejich vlastní.

Proti skenování portů lze použít systémy prevence průniku (IPS) a bránu firewall, to může omezit informace získané ze skenování portů. Ping sweep může být zastaven, pokud ICMP echo a echo-reply jsou vypnuté na okrajových routerech. Nicméně pokud jsou tyto služby vypnuty, jsou ztracena diagnostická data. Navíc skenování portů lze udělat i bez použití ping sweep, pouze to zabere více času, protože se skenují i neaktivní IP adresy.

3.5.4 Zmírnění přístupových útoků

Velké množství přístupových útoků se provádí jednoduchým hádáním hesla slovníkovým útokem (dictionary attack) nebo útokem hrubou silou (brute force attack). Obranou proti těmto útokům je použití silných hesel a zakázání přihlášení k účtu, po určitém množství neúspěšných přihlášení. Silné heslo obsahuje velká a malá písmena, čísla, speciální znaky a má minimálně osm znaků.

Síť by také měla být navržena tak, aby používala princip minimální důvěry (minimum trust principle). To znamená, že pokud například společnost používá důvěryhodný server (trusted server), který využívají nedůvěryhodná zařízení, například webové servery. Pak tento důvěryhodný server nemá věřit nedůvěryhodným zařízením.

Kryptografie je kritickou součástí každé bezpečné moderní sítě. Je doporučeno, aby byl šifrovaný vzdálený přístup, provoz směrovacího protokolu (routing protocol) by měl být také šifrován. Čím více je provoz šifrován, tím méně možností má útočník na zachycení dat útokem člověk uprostřed (man-in-the-middle). Použití šifrovaných nebo hashovaných ověřovacích protokolů v kombinaci se silnými hesly výrazně snižuje pravděpodobnost úspěšných přístupových útoků.

Nakonec, aby nemohl útočník využít neznalosti zaměstnance, tak je důležitá podpora vzdělání a poučení zaměstnanců o možných rizicích sociálních inženýrství a vyvíjení dodatečných strategií pro ověření totožnosti například telefonické nebo e-mailové.

Obecně lze přístupové útoky odhalit prohlížením log souborů, záznamů o vytížení procesů a využití šířky pásma. Podle zásad zabezpečení by měl být tvořen log pro všechna síťová zařízení a servery.

3.5.5 Zmírnění útoku DoS

Jedním z prvních znaků DoS útoku jsou stížnosti od mnoha uživatelů na nedostupnost zdrojů. Aby se minimalizoval počet útoků, měl by být vždy spuštěn software na kontrolu využití sítě, pokud jeho graf ukazuje neobvyklou aktivitu, může to naznačovat DoS útok.

Pro zmírnění počtu DoS útoků se využívá kombinace systému prevence průniku (IPS) a firewallu. Dalším důležitým krokem je také kvalitně navržené hlídání provozu a dostatečně velká paměť se kterou může router pracovat. Historicky mnoho DoS útoků pocházelo z falešných zdrojových IP adres (spoofed address). Antispoofingové technologie zahrnují zabezpečení portů, DHCP (Dynamic Host Configuration Protocol), IP Source Guard, ARP (Dynamic Address Resolution Protocol) nebo ACL(Access Control List). [54]

3.5.6 Systém prevence průniku (Intrusion Prevention Systems – IPS)

Jedná se o technologii, která zkoumá provoz na síti ve snaze nalézt a zabránit zneužití zranitelných míst. Obvykle se IPS nachází hned za firewallem a poskytuje tak další kontrolní vrstvu k zadržení nebezpečného obsahu. Narozdíl od jeho předchůdce IDS (Intrusion Detection System), který jen pasivně skenoval síťový provoz a hlásil nalezené hrozby. IPS nejen informuje administrátora o nalezené hrozbě, ale také aktivně analyzuje provoz a provádí automatizované akce, jako zahození paketu, blokování provozu ze zdrojové adresy nebo resetování připojení. [59]

Detekce podle vzoru (Pattern-Based)

Jedná se o nejjednodušší mechanismus, který hledá konkrétní předdefinovaný vzor. IPS nebo IDS zde porovnává síťový provoz s databází známých útoků a v případě shody provede příslušné akce. Spouštěč může být textový, binární nebo je to série volání funkcí a může být detekován v jednom paketu, nebo jako sekvence paketů. Ve většině případů, je vzor přiřazen pouze tehdy je-li podezřelý paket spojen s konkrétní službou nebo směřován z konkrétních portů, to snižuje množství potřebných kontrol na paketu, ale ztěžuje systémům vypořádat se s protokoly a útoky, které nepoužívají přesně definované porty.

Detekce anomálií (Anomaly-Based)

Detekce založená na anomáliích, nebo tako detekce založená na profilech, nejdříve vyžaduje definování toho, co je pro síť nebo hostitele považováno za normální. Tento stav lze zjistit sledováním aktivity v síti nebo spuštěním aplikací k tomu určených na hostiteli. Po definování normální aktivity, je zahájena akce, pokud aktivita překračuje prahovou hodnotu, zahrnutou v normálním profilu.

Výhodou detekce anomálií je možnost detekovat nové útoky, bez toho, aby se muselo definovat množství vzorů, pro scénář útoku. Správce jednoduše definuje profil normální aktivity a každá aktivita, která se odchyluje je považována za neobvyklou a vyvolá příslušnou akci.

Nevýhodou, ale je, že poplach vyvolaný neznámou aktivitou nemusí hned znamenat hrozbu, může jít jen o odchylku od normálního provozu. Jak se síť vyvíjí, je také nutné opětovně definovat co je normální aktivita, během zjišťovací fáze také musí být také zaručeno, že síť není pod útokem, protože jinak by byl útok považován za běžný stav.

Detekce založená na zásadách (Policy-Based)

Tento typ detekce je podobný detekci založené na vzorech, místo snahy definovat specifické vzory, se zde definuje chování, které je považováno za podezřelé. Tímto způsobem je možné pokrýt celou řadu činností, bez nutnosti specifikovat každou jednotlivou situaci. Například pokud správce definoval akci, která se provede, pokud e-mailový klient volá cmd.exe, dá se tato akce aplikovat k jakékoli aplikaci, jejíž chování napodobuje charakteristiky e-mailového klienta, nezáleží tedy na tom, jakou e-mailovou aplikaci uživatel používá.

Detekce hrncem medu (Honey Pot-Based)

Detekce Honey Pot využívá fiktivního serveru, aby přilákala útoky. Účelem je odvrátit útoky od skutečných zařízení. Nastavením různých slabých míst na „medových" serverech, můžou administrátoři analyzovat příchozí typy útoků a jejich průběh. Tuto analýzu lze potom použít k zabezpečení skutečných zařízení. Tento typ detekce se používá zřídka, většinou antivirovými společnosti, které ho používají k výzkumu. [54]

3.5.7 Seznam pro řízení přístupu – ACL (Access Control List)

Seznam pro řízení přístupu je sada pravidel, která se obvykle používají k filtrování síťového provozu. ACL se používají na kontrolu přicházejících a odcházejících paketů z interface a lze je nakonfigurovat na síťových zařízeních jako jsou routery nebo brány firewall. Obsahují seznam podmínek, které kategorizují pakety a určují, zda provoz projde nebo bude zakázán.

Cisco zařízení mají k dispozici dva typy ACL, standardní a rozšířené. Standardní umožňují vyhodnotit pouze zdrojovou IP adresu paketu. Nejsou tak výkonné jako rozšířené ACL, ale méně zatěžují procesor. Rozšířené ACL umožňují vyhodnotit zdrojovou a cílovou adresu, zdrojový a cílový port a další parametry. Jsou složitější na konfiguraci a vyžadují více času procesoru, ale poskytují větší flexibilitu a kontrolu nad přístupem do sítě než standardní ACL.

Pomocí ACL lze například zajistit, aby k serveru, který obsahuje důležité dokumenty měl přístup pouze administrátor. To lze zařídit tak, že v ACL povolíme pouze provoz z administrátorova počítače, provoz z jakéhokoli jiného zdroje bude blokován. [54], [60]

3.5.8 Firewall

Původní firewally nebyly samostatná zařízení, ale byly to routery nebo servery se softwarem, který zajišťoval funkce firewallu. Firewall je systém nebo skupina systémů, které uplatňují zásady kontroly přístupu mezi sítěmi, jsou odolné vůči útokům a jsou jediným průchozím bodem mezi sítěmi, tedy všechen provoz přes ně musí projít. Může zahrnovat možnosti routeru s filtrováním paketů, switche s dvěma VlANy (Virtual LAN) a několik hostitelů se softwarem firewall.

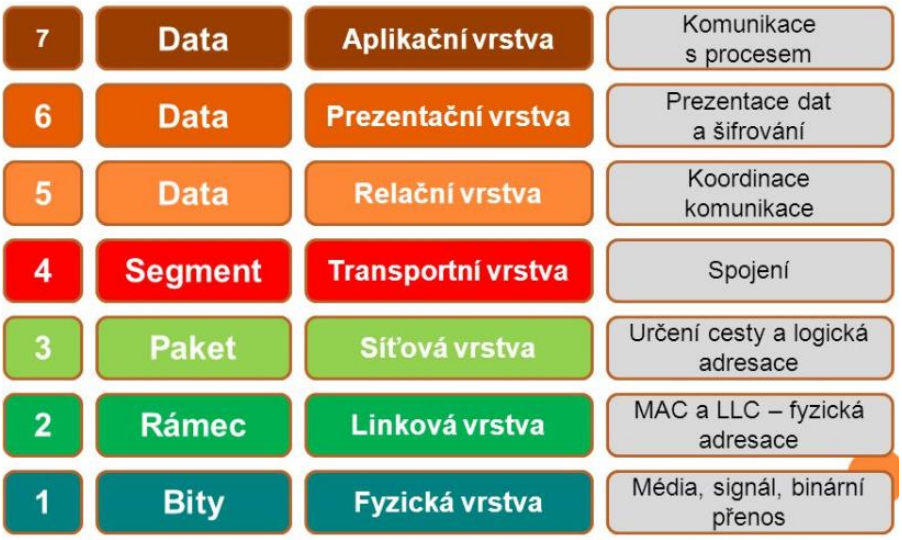
Firewall pro filtrování paketů (Packet filtering) –Firewall pro filtrování paketů jsou obvykle součástí firewallu routeru, který povoluje nebo zakazuje provoz třetí a čtvrté vrstvy ISO/OSI modelu (Obrázek 53 ISO/OSI model). Mají tabulku, ve které mají specifická kritéria, podle kterých filtrují provoz. Například servery SMTP (Simple Mail Transfer Protocol) využívají ve výchozím nastavení portu 25, administrátor může tento port zakázat, aby zabránil broadcastu e-mailového viru.

Výhody použití firewallu pro filtrování paketů jsou:

- Pro povolení nebo zákaz mají jednoduchou sadu pravidel
- Mají malý dopad na výkon sítě
- Jsou jednoduché na implementaci a většina routerů je podporuje
- Poskytují první stupeň v zabezpečení na síťové vrstvě
- Zvládá většinu úkolů brány firewall vyšší třídy

Přestože filtry paketů nepředstavují kompletní řešení, jsou důležitým prvkem v bezpečnosti sítě. Jejich nevýhodou jsou:

- Podléhají spoofing útokům (falešné IP adresy)
- Nefiltrují spolehlivě fragmentované pakety, protože ty mají TCP (Transmission Control Protocol) hlavičku v prvním fragmentu a fragmenty po prvním projdou.
- Paketové filtry používají komplexní ACL, které se obtížně implementují a udržují
- Nemohou dynamicky filtrovat určité služby, například filtrování relací, které využívají dynamického vyjednávání portů je obtížné filtrovat bez otevření přístupu k velkému množství portů
- Zkoumají každý paket jednotlivě, nikoli v závislosti na stav připojení



Obrázek 53 ISO/OSI model [61]

Stavový firewall (Stateful) –Stavový firewall je nejvšestrannější a nejběžnějším typem brány firewall. Pracuje na síťové vrstvě, ale analyzuje také provoz na vrstvě 4. a 5. ISO/OSI modelu. Sleduje každé připojení, kontroluje, zda je validní a ukládá jeho informace do tabulky stavů. Například prozkoumává TCP hlavičku, aby našla kontrolní kódy jako dokončení (FIN), synchronizaci (SYN), potvrzení (ACK) nebo jiné a podle nich určí stav připojení.

Výhody stavového firewallu jsou:

- Používají se k filtrování nežádoucího, zbytečného nebo nechtěného provozu
- Poskytují lepší filtrování paketů, protože mají přísnější kontrolu bezpečnosti
- Jsou výkonnější než filtrování paketů nebo proxy servery
- Dokáží zabránit spoofing nebo DoS útokům, určením, zda pakety náleží k existujícímu připojení nebo jsou z neautorizovaného zdroje
- Poskytují lepší informace v log souboru

Stavové firewally mají, ale také omezení:

- Nedokáží zabránit útokům aplikační vrstvy, protože nezkoumají skutečný obsah připojení HTTP
- Ne všechny protokoly jsou stavové, například UDP nebo ICMP negenerují informace o připojení pro stavovou tabulku, mají tedy jen limitovanou podporu filtrování
- Připojení využívající dynamické vyjednávání portů je obtížné sledovat
- Nepodporují ověření uživatelů

Firewall aplikační brány (Application gateway/ proxy firewall) – Filtruje informaci na vrstvách 3,4,5 a 7 ISO/OSI modelu. Většina ovládání a filtrování je prováděna softwarem, pokud klient potřebuje přístup ke vzdálenému serveru, připojí se k proxy serveru. Proxy server se připojuje ke vzdálenému serveru jménem klienta, tak vzdálený server vidí pouze připojení k proxy serveru.

Další metody implementace zahrnují hostitelský, transparentní nebo hybridní firewall. hostitelský to je server nebo počítač se spuštěným softwarem brány firewall. Transparentní filtruje přenos mezi dvojicí přemostěných rozhraní (bridged interfaces). A hybridní firewall je kombinací různých typů firewallů.

Výhody použití firewall:

- Zabránění vystavení citlivých zdrojů hostitele nedůvěryhodným aplikacím a uživatelům
- Zabraňuje zneužití chyb protokolu
- Blokuje škodlivá data ze serverů a klientů
- Snižuje složitost ve správě zabezpečení, přesunutím většiny řízení přístupu do sítě na několik bran firewall

Nevýhody firewall:

- Chybně nakonfigurovaný firewall může mít velký dopad na funkčnost sítě
- Data z mnoha aplikací nemohou bezpečně projít přes brány firewall
- Uživatelé mohou hledat cestu kolem firewallu, aby se dostali k blokovanému obsahu
- Síť může mít nižší výkon
- Neautorizovaný provoz může být skryt jako legitimní a projít přes firewall

3.5.9 Okrajový router (edge router)

Implementace okrajového routeru záleží na velikosti organizace a složitosti požadovaného návrhu sítě. Může zahrnovat jeden router, který chrání celou vnitřní síť nebo router, který funguje jako první obranná linie v hloubkové ochraně.

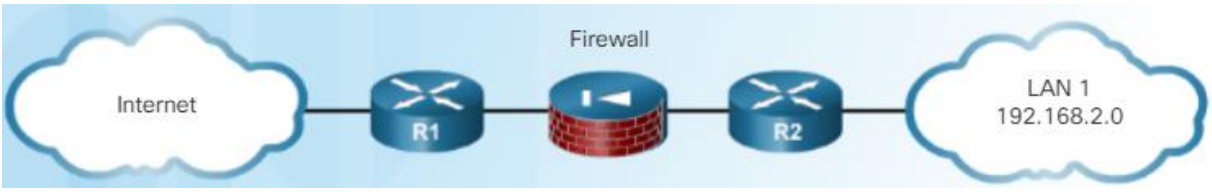
3.5.9.1 Přístup jednoho routeru (Single router approach)

Okrajový router propojuje interní místní síť k internetu. Všechny bezpečnostní zásady jsou nakonfigurovány v tomto zařízení. Tento přístup je běžný v pobočkách, malých kancelářích nebo domácích pracovnách. V menších sítích také můžou požadované bezpečnostní funkce být podporovány IRS routery (Integrated Services Router), bez ztráty jejich výkonu.

3.5.9.2 Přístup hloubkové obrany (Defence-in-depth approach)

Tento přístup je bezpečnější, protože používá více vrstev zabezpečení, než povolí přístup do chráněné LAN. Jedná se o dva routery, mezi kterými je firewall. Okrajový router je připojen k internetu a vnitřní router je připojen k chráněné LAN. Okrajový router slouží jako první obranná linie, který vyfiltruje provoz a předá ho firewallu. Ta provede další filtrování, ve výchozím nastavení zamezí připojení z vnějších (nedůvěryhodných) sítí do vnitřní sítě. Nicméně dovoluje uživatelům vnitřní sítě připojit se k vnějším sítím a umožňuje, aby se jejich odpověď vrátila. Firewall také může provádět ověřování uživatelů, ve kterém neověření uživatelé nedostanou přístup k síťovým prostředkům.

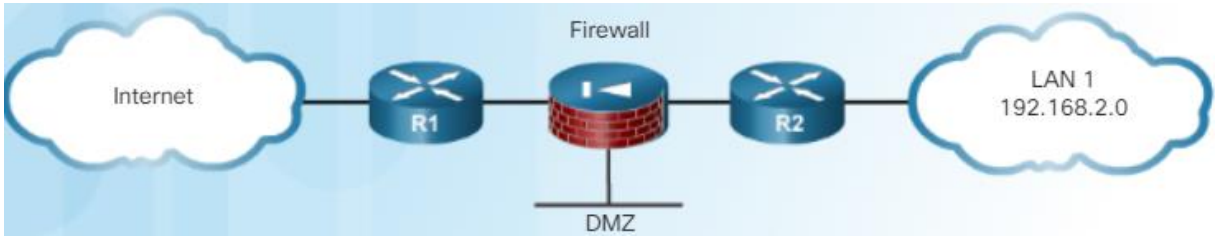
Pro hloubkovou obranu, lze použít i jiná zařízení než routery. Lze implementovat i další bezpečnostní nástroje, jako systémy IPS (Intrusion Prevention Systems), webové bezpečnostní aplikace (proxy servery) nebo e-mailová bezpečnostní zařízení (filtrování spamu)



Obrázek 54 Přístup hloubkové obrany [54]

3.5.9.3 Přístup DMZ

Jedná se o obměnu přístupu hloubkové obrany, zahrnuje mezilehlou oblast, která se nazývá demilitarizovaná zóna (DMZ). Přístup lze použít pro servery, které musí být přístupné z internetu nebo jiné externí sítě. Demilitarizovaná zóna lze nastavit mezi dvěma routery, okrajový router je připojen k externí síti a vnitřní je připojen k chráněné síti. Brána firewall je umístěna mezi chráněnými a nechráněnými sítěmi, je zde nastavena tak, aby umožňovala požadované připojení, například HTTP z vnějších sítí k veřejným serverům v demilitarizované zóně. Firewall zde souží jako primární ochrana pro všechna zařízení v DMZ.



Obrázek 55 Přístup DMZ [54]

3.5.9.4 Zabezpečení okrajového routeru

Zabezpečení okrajového routeru je kritický první krok v zabezpečení sítě. Zabezpečení routeru má tři hlavní oblasti, zabezpečení fyzické, zabezpečení operačního systému a router hardening. Pokud existují interní routery, tak i ty musí být bezpečně nakonfigurovány.

3.5.9.5 Fyzické zabezpečení routeru

Aby se k routeru a jiným zařízením k němu fyzicky připojeným nedostala neautorizovaná osoba je umístěn do uzamčené místnosti. Ta je bez elektrostatického nebo magnetického rušení, má protipožární systém a v místnosti je možnost regulovat teplotu a vlhkost vzduchu. Opatřením proti výpadku proudu je nepřerušitelný zdroj napájení (UPS) nebo záložní naftový generátor.

3.5.9.6 Zabezpečení operačního systému routeru

Je zde několik postupů, zahrnutých v zabezpečení funkcí a výkonu operačního systému routeru.

1) Nakonfigurování routeru s největším možným množstvím paměti. Dostupnost paměti pomůže zmírnit rizika způsobená DoS útoky a současně podporuje větší množství bezpečnostních služeb.
2) Použití nejnovější stabilní verze operačního systému nebo síťového zařízení. Udržování bezpečnostních a šifrovacích funkcí aktualizovaných.
3) Pořízení záložní kopie operačního systému a konfiguračních souborů routeru.

3.5.9.7 Router hardening

Zabránění možného zneužití nevyužitých portů a služeb:

1) Zabezpečení administrátorského přístupu – přístup mají pouze autorizované osoby a jejich úroveň přístupu je kontrolována.
2) Zakázání nepoužívaných portů a rozhraní – sníží se počet způsobů přístupu k zařízení.
3) Zakázání nepotřebných služeb – Stejně jako počítače, mají routery služby, které jsou defaultně aktivní. Některé tyto služby jsou pro nás nepotřebné a útočník je může použít ke shromažďování informací o routeru a síti.

Zabezpečení administrátorského přístupu

Jedná se o velmi důležitý krok v zabezpečení, protože pokud neoprávněná osoba získá administrátorská práva k routeru, může změnit nebo vypnout jeho funkce a může tak získat i přístup k jiným systémům v síti. Zabezpečení přístupu zahrnuje několik důležitých úkolů:

1) Omezení přístupu k zařízení – Omezení přístupných portů, povolených komunikátorů a omezení povolených způsobů přístupu.
2) Záznam všech přístupů – Zaznamená každého, kdo se připojí k zařízení, co se dělo během přístupu a kdy přístup proběhl.
3) Ověřený přístup – Zajištění, aby přístup byl povolen pouze ověřeným uživatelům, skupinám a službám. Omezení počtu neúspěšných pokusů o přihlášení a nastavení času pro opětovný pokus o přihlášení.
4) Schválení akcí – Omezení akcí, které může provádět konkrétní uživatel, skupina nebo služba.
5) Zobrazit právní oznámení – Zobrazení právního oznámení, vytvořeného ve spolupráci s právním zástupcem společnosti.
6) Zajištění důvěrnosti dat – Ochrana lokálně uložených citlivých dat před kopírováním a zobrazením. Je potřeba zvážit zranitelnost dat přenášených přes komunikační kanál, proti útokům sniffing, man-in-the-middle nebo únosům sezení (session hijacking).

Zabezpečení vzdáleného přístupu

K routeru lze přistupovat lokálně nebo vzdáleně. Lokální přístup, který se obvykle využívá pro počáteční konfiguraci zařízení většinou vyžaduje připojení na konzolový port, který je na routeru. Administrátor může příkazy zadávat na počítači se spuštěným softwarem emulátoru terminálu.

Správce může také přistupovat k zařízením infrastruktury vzdáleně z místní nebo vzdálené sítě. Nejběžněji pomocí Telnet, SSH, HTTP, HTTPS nebo SNMP. Některé protokoly vzdáleného přístupu posílají data, a to i uživatelská jména a hesla v prostém textu, pokud by tedy útočník odposlouchával komunikaci, tak by mohl jednoduše získat administrátorské údaje.

Z tohoto důvodu je lepší povolit pouze přístup k routeru v místní síti, pokud, ale je nutný přístup vzdálený, tak by měla být přijata následující opatření:

1) Zašifrování veškeré komunikace mezi routerem a administrátorem, například místo Telnetu použít SSH verzi 2, nebo místo HTTP použít HTTPS.
2) Vytvoření vyhrazené sítě pro správu. Ta zahrnuje pouze identifikované administrátory, připojené na vyhrazené rozhraní na routeru.
3) Nastavení filtru paketů tak, aby přístup k routeru umožnil pouze identifikovaným administrátorům a preferovaným protokolům. Například povolit pouze požadavky SSH z IP adresy administrátora.
4) Konfigurovat a vytvořit připojení VPN do lokální sítě, před připojením k administrátorskému rozhraní. [54]

ZÁVĚR

Cílem práce bylo projití možností zabezpečení budovy pomocí elektronických systémů. Práce úspěšně pokryla všechny tři části. Senzorová část seznámí čtenáře s detektory, které využívají elektromagnetické záření o různých vlnových délkách neboli detektory mikrovlnné a detektory využívající infračerveného světla. Jsou také zahrnuty senzory využívající ultrazvukových vln, senzory s detekcí narušitele využitím magnetizmu a detektory rozbití skla.

Kamerová část poskytuje informace o druzích kamer, jejich výhodách a možnostech. Je také rozebrána kabeláž, která je samozřejmě ke kamerám potřeba, protože každá kamera musí být z nějakého zdroje napájena a musí mít možnost přenést získaná data, aby je bylo možné zobrazit nebo uložit.

Poslední část věnovaná bezpečnosti sítě popisuje, jak se sítě dělí a ukazuje, jaké jsou běžné útoky na síť, jejich znaky, co mohou způsobit a prostředky pro zmírnění nebo zastavení těchto hrozeb. Informuje čtenáře, jaká protiopatření použít, aby byla síť bezpečnější.

Při tvorbě práce jsem se dozvěděl mnoho zajímavých informací, hlavně o senzorech, které osobně shledávám velice užitečné, a to nejen v zabezpečení, ale i například v automatizaci nebo výrobě, kde pomáhají ulehčit práci nebo předejít úrazům.

POUŽITÁ LITERATURA

[1] KRAHULÍK, Lukáš. *Poplachové zabezpečovací a tísňové systémy a návrh jejich funkčnosti* [online]. Zlín, 2012. Dostupné také z: https://digilib.k.utb.cz/bitstream/handle/10563/19152/krahul%C3%ADk_2012_dp.pdf?sequence=1. Diplomová práce. Univerzita Tomáše Bati.

[2] ElmgSpektrum. In: *Wikimedia Commons* [online]. 2019 [cit. 2020-01-25]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/e/e3/ElmgSpektrum.png

[3] MICHALEC, Libor. PIR detektor: skvělý sluha, ale zlý pán. *Vyvoj.hw.cz: profesionální elektronika* [online]. 2013. Dostupné z: https://vyvoj.hw.cz/automatizace/pir-cidlo-skvely-sluha-ale-zly-pan.html

[4] RŮČKA, Ondřej. *PIR detektory a jejich spolehlivost* [online]. Zlín, 2011. Dostupné také z: http://digilib.k.utb.cz/bitstream/handle/10563/18384/r%C5%AF%C4%8Dka_2011_bp.pdf?sequence=1&isAllowed=y. Bakalářská práce. Univerzita Tomáše Bati. Vedoucí práce Ing. Rudolf Drga.

[5] Fresnelova čočka pro PIR senzor - bílá. In: *Rasel spol. .s.r.o.: specialista na VF konektory* [online]. Praha: Rasel.cz, c2019 [cit. 2020-01-25]. Dostupné z: https://www.rasel.cz/fresnelova-cocka-pro-pir-senzor-bila-p20645/

[6] BOR, Michal. *Možnosti ověření vlastností PIR detektorů* [online]. Zlín, 2010. Dostupné také z: http://digilib.k.utb.cz/bitstream/handle/10563/13031/bor_2010_bp.pdf?sequence=1&isAllowed=y. Bakalářská práce. Univerzita Tomáše Bati. Vedoucí práce Ing. Petr Dostálek.

[7] Infračervené záření. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation. Dostupné z: https://cs.wikipedia.org/wiki/Infra%C4%8Derven%C3%A9_z%C3%A1%C5%99en%C3%AD

[8] Analýza a zpracování signálů: 2. Analogové a diskrétní signály. Sinusoidy a spojité signály [online]. Dostupné z: http://www.kiv.zcu.cz/~mautner/Azs/Azs2_Spojite_systemy_Vzorkovani.pdf

[9] Kvantování(signál). In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2020 [cit. 2020-01-25]. Dostupné z: https://cs.wikipedia.org/wiki/Kvantov%C3%A1n%C3%AD_(sign%C3%A1l)#/media/Soubor:Quantized.signal.svg

[10] KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Blatná: Blatenská tiskárna, 2006, 313 s. ISBN 80-902-9382-4.

[11] Technology. Occupancy sensors | Motion sensors PIR sensors [online]. Ecoamica Technologies LLP. Dostupné z: http://www.ecosirius.com/technology.html

[12] BARÁK, Petr. Metody detekce pohybu v ochraně objektu [online]. Zlín, 2010. Dostupné také z: http://digilib.k.utb.cz/bitstream/handle/10563/13139/bar%C3%A1k_2010_dp.pdf. Diplomová práce. Univerzita Tomáše Bati. Vedoucí práce Doc. Ing. Luděk Lukáš.

[13] Astabilní klopný obvod, multivibrátor. In: *Penguin: Neziskový server pro podporu Linuxu, UNIXu a free softwaru.* [online]. Penguin, c1998-2020 [cit. 2020-01-25]. Dostupné z: http://www.penguin.cz/~radek/book/electronic/ch21s01.html

[14] Snímače mechanického namáhaní: piezoelektrický jev. Elektronická učebnice [online]. Dostupné z: https://eluc.kr-olomoucky.cz/verejne/lekce/1590

[15] Multivibrátor: Blikač. Ok1ike: Web začínajících radioamatérů [online]. Dostupné z: http://ok1ike.nagano.cz/soubory/mult_blik.htm

[16] HITCHCOCK, R. Timothy. Radio-frequency and microwave radiation [online]. 3rd ed. Fairfax, Va.: American Industrial Hygiene Association, c2004. ISBN 19-315-0455-5. Dostupné také z: https://books.google.cz/books?id=0TUIQ9-Ap5cC&pg=PA1&dq=microwave&redir_esc=y#v=onepage&q=microwave&f=false

[17] FRADEN, Jacob. Handbook of modern sensors: physics, designs, and applications [online]. 4th ed. New York: Springer, c2010. ISBN 978-1-4419-6465-6. Dostupné také z: http://www.realtechsupport.org/UB/SR/sensors/Fraden_Sensors_2010.pdf

[18] Gunn diode basic. In: Youtube [online]. Dostupné z: https://www.youtube.com/watch?v=0FZyLiN3lQc. Kanál uživatele Electronics Physics and Spirituality.

[19] GUNN diode. *Electrical4U: Electrical and Electronics Engineering Basics & Principles* [online]. 31.07.2018. Dostupné z: https://www.electrical4u.com/gunn-diode/

[20] STRNAD, Jan. *Polovodiče a jejich využití a funkce v solární energetice* [online]. Olomouc, 2014. Dostupné také z: http://www.zshalkova.cz/dokumenty/ZP_Strnad_Polovodice-a-jejich-vyuziti-a-funkce-v-solarni-energetice_14.pdf. Závěrečná práce. Fakultní základní škola Olomouc. Vedoucí práce Mgr. Zdeněk Titz.

[21] Gunn Oscillator. *Electrical4U: Electrical and Electronics Engineering Basics & Principles* [online]. 4.09.2018. Dostupné z: https://www.electrical4u.com/gunn-oscillator/

[22] POLKHANOV, Alexei. Episode 7, Microwave Gunn diodes and Gunn diode oscillators. In: *Youtube.com* [online]. Dostupné z: https://www.youtube.com/watch?v=AsMgU2u1yYM. Kanál uživatele Alexei Polkhanov

[23] PUNČOCHÁŘ, Josef. *6. kapitola: Směšovače* [online]. Ostrava. Dostupné také z: http://fei1.vsb.cz/kat420/vyuka/FEI/AEO/sylaby/AEO_06.pdf

[24] Bezdrátový magnetický detektor na dveře a okna pro alarm,GSM alarm: Model: AS-D026. *Alarmsecurity.cz: Domácí zabezpečovací systémy* [online]. Dostupné z: https://www.alarmsecurity.cz/www-alarmsecurity-cz/eshop/4-1-MAGNETICKE-DETEKTORY/0/5/71-Bezdratovy-magneticky-detektor-na-dvere-a-okna-pro-alarm-GSM-alarm

[25] NORMAN, Thomas. Magnetic switches. NORMAN, Thomas. *Integrated Security Systems Design* [online]. 2. Edice. 2014. ISBN 978-0-12-800022-9. Dostupné z: https://www.sciencedirect.com/topics/computer-science/magnetic-switch

[26] WOODFORD, Chris. Reed switches. *ExplainThatStuff!* [online]. 2019. Dostupné z: https://www.explainthatstuff.com/howreedswitcheswork.html

[27] PAVLÍNEK, Radek. *Bezkontaktní detektory rozbití skla* [online]. Zlín, 2012 [cit. 2019-10-07]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/23248/pavl%C3%ADnek_2012_bp.pdf. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Doc. Ing. Luděk Lukáš CSc.

[28] What Is CCTV & How Does it Work? *State Systems Inc.: Protecting Life & Property* [online]. Memphis, c2019, 23. Července. 2019 [cit. 2019-12-27]. Dostupné z: https://www.statesystemsinc.com/blog/what-is-cctv

[29] WOODFORD, Chris. Webcams. *ExplainThatStuff!* [online]. c2000-2019, 8. Srpna 2019 [cit. 2019-11-20]. Dostupné z: https://www.explainthatstuff.com/webcams.html#ccds

[30] What Is a CMOS Image Sensor?: Semiconductor device that serves as an "electronic eye." *Nanotec Museum: Semiconductor Technologies* [online]. [cit. 2019-11-20]. Dostupné z: https://www.tel.com/museum/exhibition/principle/cmos.html

[31] Analog vs. digital ip security cameras & CCTV systems. Custormer1st communications [online]. Atlanta, c2019, 2016 [cit. 2019-12-27]. Dostupné z: https://www.c1c.net/blog/analog-vs-digital-security-cameras-cctv/

[32] A Basic Guide to CCTV: Analogue CCTV or Digital CCTV? Doyle Security [online]. Barnsley: Fortay Media, c2019 [cit. 2019-12-29]. Dostupné z: https://www.doylesecurity.co.uk/basic-guide-cctv-analogue-cctv-digital-cctv/

[33] NVR Vs. DVR: What's The Difference? *Swann Security: Security Made Smarter* [online]. Swann, c2018, 13 June 2018 [cit. 2019-12-29]. Dostupné z: https://www.swann.com/blog/dvr-vs-nvr-whats-the-difference/

[34] What Are the Different Types of CCTV Camera? *Caught on Camera* [online]. England, c2019 [cit. 2019-12-29]. Dostupné z: https://www.caughtoncamera.net/news/different-types-of-cctv/#question_1

[35] WILSON, Joe. What Type Of CCTV Camera Should I Buy? *Sonitrol Western Canada Inc: Verified electronic security* [online]. Canada: Brit Agency, c2019, 18 Jun 2015 [cit. 2019-12-29]. Dostupné z: https://www.sonitrolwesterncanada.com/blog/what-type-of-cctv-camera-should-i-buy

[36] Co potřebuji vědět před výběrem kamerového systému. *Doma v bezpečí: bezpečnostní kamerové systémy* [online]. Praha [cit. 2019-12-29]. Dostupné z: http://www.domavbezpeci.cz/jak-na-to.htm

[37] Složení bezpečnostního kamerového systému. *Hlídací kamery: zajistí Vám vyšší bezpečnost a přehled o Vašem okolí* [online]. bluecube.cz, c2011 [cit. 2019-12-29]. Dostupné z: http://www.hlidacikamery.cz/slozeni-kameroveho-systemu/

[38] ROUSE, Margaret. What is coaxial cable?: A definition from WhatIs.com. *SearchNetworking* [online]. TechTarget, c2000-2019 [cit. 2019-12-29]. Dostupné z: https://searchnetworking.techtarget.com/definition/coaxial-cable-illustrated

[39] Everything You Need To Know About Coaxial Cable. *RS Australia: World Leading Distributor of Electronic* [online]. Dublin [cit. 2019-12-29]. Dostupné z: https://au.rs-online.com/web/generalDisplay.html?id=ideas-and-advice/coaxial-cable-guide

[40] BNC 5M BNC Power Video Audio Plug and Play Extension Cable for CCTV Camera - Black. In: *GeekBuying* [online]. GeekBuying.com, c2012-2020 [cit. 2020-01-25]. Dostupné z: https://www.geekbuying.com/item/BNC-5M-BNC-Power-Video-Audio-Plug-and-Play-Extension-Cable-for-CCTV-Camera---Black-335969.html

[41] Security Camera Cable Information and Installation Instructions. *CCTV Camera Pros: Video Surveillance System for Home, Busines & Govemment* [online]. Florida (Lantana), c2019 [cit. 2019-12-29]. Dostupné z: https://www.cctvcamerapros.com/Security-Camera-Cable-s/58.htm

[42] 95% CCA Braid CCTV RG59 Coaxial Cable 20 AWG BC Conductor Foamed PE Siamese Cable. In: *Zion Communication: Cable Manufacturer & Cable Solutions Supplier* [online]. China: coaxialtvcables.com, c2015-2019 [cit. 2020-01-25]. Dostupné z: http://www.coaxialtvcables.com/sale-6132449-95-cca-braid-cctv-rg59-coaxial-cable-20-awg-bc-conductor-foamed-pe-siamese-cable.html

[43] Types of BNC Connectors. *IIT Kanpur: Indian Institute of Technology, Kanpur* [online]. Kanpur, c2019 [cit. 2019-12-29]. Dostupné z: https://www.iitk.ac.in/ibc/BNC.pdf

[44] What does UTP, S/UTP, FTP, STP and SFTP mean? *Universal Networks* [online]. United Kingdom (Hungerford) [cit. 2019-12-29]. Dostupné z: https://www.universal-networks.co.uk/faq/copper/what-does-utp-ftp-stp-or-sftp-mean

[45] Rozbor síťových kabelů, proč je znát? *PCage* [online]. Libešice: PCage, c2019, 12. 4. 2017 [cit. 2019-12-29]. Dostupné z: http://wiainternet.cz/rozbor-sitovych-kabelu-proc-je-znat/

[46] IAN, Poole. Ethernet Cable: Types, Performance & Pinout - Cat 5, 5e, 6, 6a, 7, 8 etc. *Electronics Notes* [online]. [cit. 2019-12-29]. Dostupné z: https://www.electronics-notes.com/articles/connectivity/ethernet-ieee-802-3/cables-types-pinout-cat-5-5e-6.php

[47] Cat6 vs Cat7 vs Cat8 Cable: What's the Difference? *Fiber Optic Network Products* [online]. 5 September 2018 [cit. 2019-12-30]. Dostupné z: http://www.fiberopticshare.com/cat6-vs-cat7-vs-cat8-whats-difference.html

[48] Ethernet Cables, UTP vs STP, Straight vs Crossover, CAT 5,5e,6,7,8 Network Cables. In: *Youtube* [online]. PowerCert Animated Videos [cit. 2019-12-30]. Dostupné z: https://www.youtube.com/watch?v=_NX99ad2FUA

[49] SPIESS, Andreas. #276 Power over Ethernet (PoE) Tutorial. In: *Youtube* [online]. Andreas Spiess [cit. 2019-12-30]. Dostupné z: https://www.youtube.com/watch?v=EUMIdhZXRWY

[50] SAILAJA, C. Wireless CCTV for Surveillance Monitoring. *Tech Speak: Tata Consulting Engineers Limited* [online]. Tech Speak, 13 March 2018 [cit. 2019-12-30]. Dostupné z: https://www.tce.co.in/blog/?p=221

[51] BRAIN, Marshall, Tracy WILSON a Bernadette JOHNSON. How WiFi Works. *HowStuffWorks: Learn How Everything Works!* [online]. HowStuffWorks, c2019 [cit. 2019-12-30]. Dostupné z: https://computer.howstuffworks.com/wireless-network1.htm

[52] MCFADDEN, Christopher. How Exactly Does Wi-Fi Work? *Interesting Engineering* [online]. c2019, 17 November 2019 [cit. 2019-12-30]. Dostupné z: https://interestingengineering.com/how-exactly-does-wi-fi-work

[53] LOEFFLER, John. How WiFi 6 is About to Revolutionize the Internet of Things. *Interesting Engineering* [online]. c2019, 6 July 2019 [cit. 2019-12-30]. Dostupné z: https://interestingengineering.com/how-wifi-6-is-about-to-revolutionize-the-internet-of-things

[54] CCNA Security: Implementing Network Security 2.0. *Cisco Networking Academy: Builds IT Skills & Education for Future Careers* [online]. [cit. 2020-01-08]. Dostupné z: https://1367347.netacad.com/courses/728179

[55] Types of Computer Networks: LAN, MAN, WAN, VPN. *Meet Guru99: Free Training Tutorials & Video for IT Courses* [online]. Wilmington (Delaware): Guru99, c2020 [cit. 2020-01-08]. Dostupné z: https://www.guru99.com/types-of-computer-network.html

[56] DELONY, David. LAN WAN PAN MAN: Learn the Differences Between These Network Types. *Techopedia: Where IT and Busines Meet* [online]. Techopedia, c2020, 10 May 2017 [cit. 2020-01-08]. Dostupné z: https://www.techopedia.com/2/29090/networks/lanwanman-an-overview-of-network-types

[57] Počítačové sítě: Rozdělení. *Střední škola technická Opava* [online]. Opava: Střední škola technická, c2011 [cit. 2020-01-08]. Dostupné z: https://sst.opava.cz/ict/site/ps_rozdeleni.pdf

[58] What is Scareware? *Expert Cyber Security Solutions for Home & Busines: Kaspersky* [online]. Switzerland: AO Kaspersky Lab, c2020 [cit. 2020-01-09]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/scareware

[59] What is an Intrusion Prevention System? *Global Cybersecurity Leader - Palo Alto Networks* [online]. Palo Alto Networks, c2020 [cit. 2020-01-17]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

[60] What is ACL (Access Control List)? *Geek University: Become a Geek* [online]. Geek University, 2019 [cit. 2020-01-19]. Dostupné z: https://geek-university.com/ccna/what-is-acl-access-control-list/

[61] Model ISO/OSI: vrstvy. In: *Maturitní Helpdesk* [online]. Brno [cit. 2020-01-25]. Dostupné z: http://matureplus.4fan.cz/pos/3-model-isoosi-vrstvy/