

**П Р И Р А Ч Н И К
ЗА ОСПОСОБУВАЊЕ И
ПОЛАГАЊЕ СТРУЧЕН ИСПИТ
ЗА ТЕХНИЧКО ОБЕЗБЕДУВАЊЕ**

Наслов:

Прирачник за осјособување и полагање на стручен испит за вршење на работи за техничко обезбедување

Издавач:

Комора на Република Македонија за приватно обезбедување

За издавачот:

Верица Милеска Стефановска, Претседател на Комора на Република Македонија за приватно обезбедување

Графички дизајн и подготовка за печатење:

ПОПЕ КОМПАНИ ДОО Скопје

Печати:

ПОПЕ КОМПАНИ ДОО Скопје

Тираж: 200

СОДРЖИНА

Вовед	v
-------------	---

ТЕОРЕТСКИ ДЕЛ

1. ОСНОВИ НА ЕЛЕКТРОТЕХНИКА И ТЕЛЕКОМУНИКАЦИИ.....	1
1.1. Типови на кабли, пресеци, правила за поставување на инсталација	3
1.2. Најони, сѐруи, оштоварувања, поларитет и симболи во електротехниката.....	20
1.3. Заштитата при работа во електротехниката	38
1.4. Видови на телекомуникации, општи поими	46
2. ВИДОВИ НА СИСТЕМИ ЗА ТЕХНИЧКО ОБЕЗБЕДУВАЊЕ.....	67
2.1. Видови системи за техничко обезбедување.....	69
2.2. Системи за детекција и дојава на најраник, кражба, напад и ѝаника	80
2.3. Системи за детекција, дојава и гасење на пожар.....	88
2.4. Системи за детекција и дојава на вода, токсични гасови и шечен нафтен гас (ѝлин).....	99
2.5. Системи за видео надзор CCTV.....	104
2.6. Системи за контрола на ѝрисѝай.....	121
2.7. Интегрирани системи.....	126
2.8. Мониторинг центри	129
3. СКИЦИРАЊЕ И ПЛАНИРАЊЕ НА ИЗВЕДБА И ИЗВЕДБА НА СИСТЕМИ ЗА ТЕХНИЧКО ОБЕЗБЕДУВАЊЕ.....	131
3.1. Стандарди.....	133
■ EN54 - Детекција на пожар и аларм на пожарен систем.....	133
■ EN50131 - Алармни системи, системи за најраници и задржување.....	137
■ EN50132 - CCTV системи за набљудување за употреба во сигурносни апликации.....	139
■ EN 50133 - Систем за контрола на ѝрисѝай и користење на сигурносни апликации.....	141

■ EN 50137 – Комбинирани односно интегрирани алармни системи	141
3.2. Читање на техничка спецификација:	151
4. ЗАКОН ЗА ПРИВАТНО ОБЕЗБЕДУВАЊЕ	153
4.1. Видови на приватно обезбедување	155
4.2. Општи услови за физичко лице за вршење на приватно обезбедување (лиценца и легитимација за обезбедување)	159
4.3. Вршење на техничко обезбедување	162
4.4. Заинтереси на приватноста и известување за вршење на видеонадзорот	163
4.5. Квалифет и исправност на техничките средства и уреди	164
4.6. Легитимирање на работникот за приватно обезбедување	165
4.7. Постапување по наредба	166
4.8. Работна облека и ознака на работниците за приватно обезбедување	166
4.9. Прекршочни одредби	167
5. ЗАКОН ЗА ЗАШТИТА НА ЛИЧНИ ПОДАТОЦИ	171
5.1. Правилник за техничките и организациските мерки за обезбедување тајност и заинтереси на обработката на личните податоци	173
5.2. Правилник за видео надзор	187

ПРАКТИЧЕН ДЕЛ

6. ПЛАНИРАЊЕ И ИНСТАЛИРАЊЕ НА СИСТЕМИ ЗА ТЕХНИЧКО ОБЕЗБЕДУВАЊЕ	195
6.1. Систем за детекција и дојава на најраник, кражба, напад и паника	197
6.2. Системи за детекција, дојава и гасење на пожар	205
6.3. CCTV практичен водич	213
6.4. Основен водич за планирање и изведба на систем за контрола на присутност	221

ВОВЕД

Техничко обезбедување, како обезбедување на лица и имот со примена на технички средства и уреди, нивно проектирање, инсталирање и одржување, прецизно е дефинирано и законски регулирано со Законот за приватно обезбедување (Сл. весник на РМ бр. 166/2012) и Правилникот за содржината на програмите и начинот на оспособувањето на физичките лица за физичко и техничко обезбедување; полагањето на стручните испити; формата и содржината на образецот на барањето за издавање на лиценца за приватно обезбедување и формата и содржината на обрасците на лиценците за приватно обезбедување (Сл. весник на РМ бр.79/13).

Иако во компаративните законодавства и практики дејноста техничко обезбедување, начинот на вршење на истата, нормите, стандардите, критериумите и други услови одамна се прецизно уредени, усвоени, применувани и усовршувани, Република Македонија со Законот за приватно обезбедување и под законските акти за прва пат пропишува дека техничко обезбедување може да се врши во вид на давање на услуги, од страна на правни лица кои имаат добиено дозвола од Министерството за внатрешни работи и кои имаат вработено работници за обезбедување кои имаат Лиценца за техничко обезбедување и легитимација за техничко обезбедување.

Законот за приватно обезбедување за добивање на Лиценца за техничко обезбедување го „пресликува“ концептот кој го пропишуваше и Законот за обезбедување на лица и имот (Сл. весник на РМ бр80/99; 66/2007....) за добивање на Лиценца за физичко обезбедување. Секој кандидат задолжително се оспособува и полага стручен испит за вршење техничко обезбедување, како неопходен услов за добивање Лиценца.

Имено, неопходен услов за добивање Лиценца за техничко обезбедување е оспособување во времетраење од 40 часови за 5 теоретски предмети (Основи на електротехника и телекомуникации , Видови на системи за техничко обезбедување , Скицирање и планирање на изведба и изведба на системи за техничко обезбедување , Закон за приватно обезбедување и Закон за заштита на лични податоци) и 1 практичен дел (Планирање и инсталирање на системи за техничко обезбедување), како и полагање на стручен испит за истите предмети.

Иако, организирањето на оспособувањето и полагањето на стручниот испит е законска обврска на Комората, треба да се истакне дека суштинска одговорност на Комората е унапредување на дејноста, па во тој смисол за Комората приоритет претставува придонесот за градење на стручна, професионална, современа дејност, пред се заради вршителите на истата, а секако и заради корисниците на услугите и генерално заради општата јавност.

Токму во правец на градење и создавање на квалитетен кадар кој ќе ја врши професијата приватно обезбедување, во случајов техничко обезбедување, Комората лоцираше неопходна потреба од креирање на стручно теоретско помагало – прирачник за оспособување и полагање на стручен испит за вршење на техничко обезбедување, кој ќе содржи сеопфатен, основен материјал за оспособување и полагање на стручен испит, за секој кандидат кој сака да се стекне со Лиценца за техничко обезбедување и да ја врши оваа дејност.

Овој прирачник го содржи комплетниот материјал пропишан со програмата, со реални примери, пракса и тематика, која веруваме дека ќе придонесе за полесно совладување на проблематиката, но истовремено се надеваме дека ќе ги мотивира кандидатите и понатаму да продолжат со стручно усовршување и унапредување на своите знаења, заради личен раст и развој и напредок на професијата и дејноста.

1

ТЕОРЕТСКИ ДЕЛ

Основи на електротехника и телекомуникации

- 1.1. Типови на кабли, пресеци, правила за поставување на инсталација **3**
- 1.2. Најони, сирани, оловарувања, поларитет и симболи во електротехника **20**
- 1.3. Заштити при работа во електротехника **38**
- 1.4. Видови на телекомуникации, оптички системи **46**

7 ЧАСА



1.1. ТИПОВИ НА КАБЛИ, ПРЕСЕЦИ, ПРАВИЛА ЗА ПОСТАВУВАЊЕ НА ИНСТАЛАЦИЈА

Вовед

Електричните и мрежните кабли денес претставуваат доминантен медиум за пренос на податоци. Постојат повеќе од 2200 различни видови на кабли кои во зависност од нивната намена се применуваат во енергетиката и телекомуникациите. Најголем дел од денешните мрежи користат четири основни видови на кабли и тоа:

- електроенергетски
- громобрански
- телекомуникациски
- сигнални

Електроенергетските инсталации претставуваат водови составени од еден или повеќе проводници кои се прекриени по целата своја должина со слој од изолационен материјал, а потоа сите заедно се опфатени со еден или повеќе заштитни слоеви. Еден од заштитните слоеви е внатрешниот плашт, којшто е најчесто метален и ги штити проводниците од продор на влага и другите штетни хемиски материи. Каблите најчесто имаат уште и механичка заштита (арматура) која овозможува тие да се користат за полагање (хоризонтално, косо или вертикално) во суви простории, во влажни простории, на отворено или директно во земјата (во т. н. кабелски ровови), под вода, во кабелски канали, во рудниците и на други места. Каблите служат за пренос и распределба на електричната енергија. Се произведуваат практично за сите напони, почнувајќи од нискиот напон ($U_n < 1 \text{ kV}$), за внатрешен развод, но и за среден напон (3, 6, 10, 20, 35 и 60 kV), за распределба (дистрибуција) на електричната енергија, за висок напон (110 и 220 kV) и за највисоките напони (над 220 kV), за пренесување на ел. енергија.

Громобранските инсталации се поставуваат со цел да ги заштитат луѓето и објектите од штетното делување на атмосферските електрични празнења.

Телекомуникациските инсталации овозможуваат пренос на податоци. Постојат неколку видови на телекомуникациски инсталации и тоа: телефонски инсталации, компјутерски инсталации, инсталации за интерфон, инсталации за интерна телевизија, инсталација за заеднички радио и ТВ состави, инсталации за разглас итн.

Сигнални инсталации се инсталации за електрични свона, инсталации за противпожарен систем и инсталациите за заштита од кражби - алармни системи.

Електроенергетските и громобранските инсталации спаѓаат во групата на груби инсталации со јака струја, додека телекомуникациските и сигналните инсталации се вбројуваат во инсталации со мала струја.

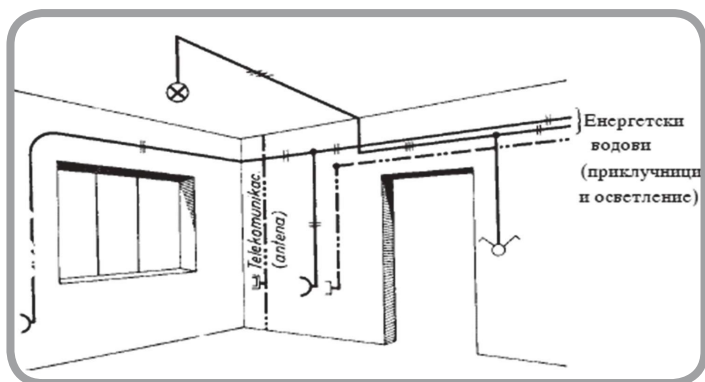
Изолирани водови и енергетски кабли

Енергетските водови се основни елементи на ЕЕС кои служат за пренос и распределба на електричната енергија. Според нивната конструкција и според местото на нивната употреба, енергетските водови се поделени во три основни групи:

- а) надземни водови (далеководи);
- б) изолирани водови
- в) кабелски водови (кабли).

Надземните водови т.е. (далеководи) денес се основен елемент за пренос на големо количество електрична енергија. Нивна основна одлика е, како што тоа го кажува и самиот поим, фактот што проводниците кај нив се водат над земјата и се одржуваат во просторот на определено меѓусебно растојание. Проводниците кај надземните водови се голи (т.е. неизолирани) бидејќи како изолација се користи самиот воздух, додека изолаторите служат само за механичко зацврстување и поставување на проводниците за самата конструкцијата на електричните столбови.

За разлика од надземните водови, кај изолираните водови и кај каблите кои се користат за спроведување на електрична енергија во станбени објекти самите проводници се изолирани со сопствена изолација и тие се поставуваат во специјални заштитни обвивки кои се инсталираат во самата заштитна изолација на самиот објект или пак директно во земјата.



Слика 1.1. Изолирани водови (електроенергетски и телекомуникациони) положени во стамбени простории

Помеѓу изолираните водови и кабли постојат одредени разлики, како во поглед на намената и конструкцијата, така и во поглед на начинот на полагање. Основната разлика се состои во тоа што изолираните водови никогаш не се поставуваат директно во земјата, поради што тие имаат едноставна и поекономична конструкција. Исто така, изолираните водови се применуваат главно за напони до 1 kV (освен во некои исклучителни случаи, како на пример кај електричните инсталации кои се со намена за пренос на електрична енергија за осветлување), воедно каблите се изработуваат за сите номинални напони, почнувајќи од нискиот напон 220/380 V, па сè до 220 kV и повеќе.

Изолираните електроенергетски водови можат да се поделат во четири групи:

- инсталациони водови;
- изолирани водови
- каблови во зависност од нивната намена (електрични и мрежни)
- изолирани водови за посебна намена.

Инсталационите водови служат за трајно поставување во индустриските, јавните и земјоделските објекти, во стамбените и деловните простории (слика 1.1 и 1.2) и на други места каде што постојат нормални услови за поставување. Со други зборови, тие се поставуваат на места каде што не постои можност од механички напрегања и оштетувања на водовите како и можности за хемиско оштетување (присуство на агресивни хемиски материи) или термичко разорување (значително повишување на амбиентната температура) на водовите.

Изолирани проводници и кабли

I група - посебно подрачје на примена

A - автомобилски,	S - за светилки,
B - бродски,	Z - за заварување,
D - за дигалки,	Z - железнички.

II група - ознака за изолациониот материјал

P - поливинил хлорид,	Pu - полиуретан,
E - термопластичен полиетилен,	IP - импрегнирана хартија,
X - умрежен полиетилен,	NP - особено импрегнирана хартија,
G - гума,	H - слабоспроводлив слој,
Ev - етилен винилацетат,	h - слабоспроводлив плашт,
Ep - етилен - пропилен гума,	T - текстилен оплет.
N - полихлоропрен (неопрен),	

III група - ознака која дава информација за особините на конструкцијата, значајни за примената на изолираниот спроводник (се одвојува од втората група со коса црта)

A - отпорен на атмосфер. влијанија,
F - финожичен,
J - зајакнат плашт,
K - калаисан спроводник,
L - полесен плашт,
M - многужичен,
N - не поддржува горење,

O - самоносив,
R - со раздвоени жили,
S - особено погоден за свиткување,
T - отпорен на топлина
U - со невпредени (паралелни) жици,
V - високонапонски,
Z - со електрична заштита од метал,

IV група ако изолираниот спроводник содржи и жила со зелена и жолта боја на изолацијата, во неговата ознака ќе постои оваа група на симболи. Оваа група се состои само од буквата Y, која со цртичка е одделена од претходната група.

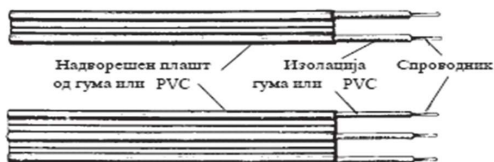
V група има ознака која дава информација за материјалот од кој е направен спроводниот дел, но и за обликот на неговиот напречен пресек.

A - за проводници од алуминиум,
S - за повеќежични проводници со секторски пресек,
SJ - за едножични проводници со секторски пресек.

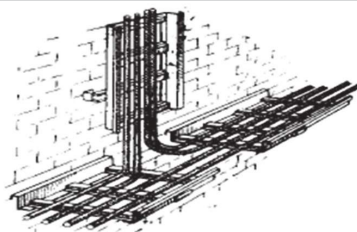
Ако материјалот е од бакар не се користи ознака во петтата група на симболи. Ако напречниот пресек е кружен не се користи никаква ознака.

VI група дава информација за бројот на жилите и нивниот номинален пресек (mm²). Се пишува зад претходната со оставање празнина чија ширина е еднаква на ширината за пишување на една буква.

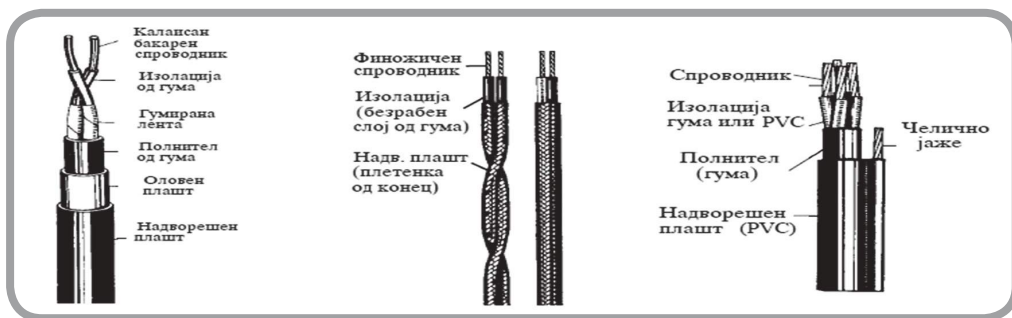
VII група дава информација за зависината на номиналниот напон во V група, за кој е изграден изолираниот спроводник.



Слика 1.3. Инсталациони водови, прицврстени на сид и поставени на специјални конструкции



Слика 1.2. Инсталациони водови тип PP/R или тип PG/R за полагање под малтер



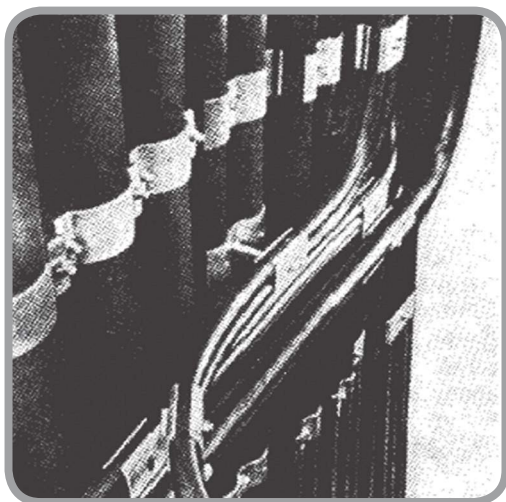
а) Изолиран вод сличен на кабел, тип GO

б) Гајтани од типот GT/P и GT

в) Самоносечки изолиран вод тип PP 00/0

Слика 1.4. Разни видови изолирани водови

Инсталационите водови во станбените и деловните простории, па и во индустриските погони, најчесто се поставуваат директно под самата заштитна изолација на објектот, или пак се поставуваат во инсталациони цевки. Цевките можат да бидат поставени под заштитната изолација, или над заштитната изолација - на самите сидови. Во последно време, електричните инсталации се поставуваат и во самиот под. Меѓутоа, во индустриските погони инсталирањето на самите водови се поставуваат на челични конструкции, или пак на специјални метални носачи (сл.1.3), но често пати инсталациите се поставуваат во сидани канали или пак во специјални бетонски блокови.



Слика 1.5. Енергетски кабли, водени паралелно

За разлика од нив, изолираните водови слични на кабел (сл. 1.4 а) кои што претставуваат извесен премин од изолираните водови кон каблите, се полагаат онаму каде што постојат можности за поблаги механички или хемиски оштетувања.

Проводниците прикажани на (слика. 1.4 б), кои служат за напојување на подвижните приемници (потрошувачи) на електричната енергија, поради што тие мора да бидат флексибилни. Затоа, проводниците кај нив се изведуваат како финожични (лицнести), а изолацијата е најчесто гума.

Енергетските кабли претставуваат водови составени од еден или повеќе проводници кои се прекриени по целата своја должина со слој од изолационен материјал, а потоа сите заедно се опфатени со еден или повеќе заштитни слоеви. Еден од заштитните слоеви е внатрешниот плашт, којшто е најчесто метален и ги штити проводниците од продор на влагата и другите штетни хемиски материи. Каблите најчесто имаат уште и механичка заштита (арматура) која овозможува тие да се користат за поставување (хоризонтално, косо или вертикално) во суви простории, во влажни простории, на отворено или директно во земјата (во т. н. кабелски ровови), во кабелски канали, во рудниците и на други места. Енергетскиот кабел се состои од следните елементи: спроводник (проводници), изолација, електрична заштита (екран), пополнување, внатрешен плашт, внатрешна заштита од корозија, арматура и надворешна заштита од корозија (надворешен плашт) (слика 1.6). Некои типови кабли ги немаат сите наведени елементи во својата конструкција.

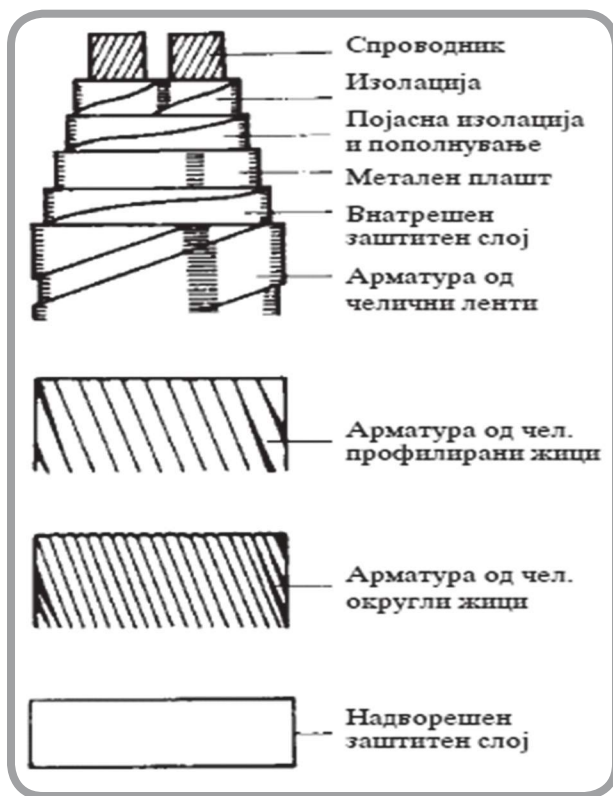
Основен и единствено активен елемент на кабелот кој ја спроведува електричната струја е спроводникот (проводниците). Спроводникот се состои од една или повеќе жици, изработени од бакар или алуминиум кои се впредуваат во форма на јаже. Околу спроводникот се поставува слој од изолационен материјал изработен од поливинил-хлорид (PVC), полиетилен (PE), импрегнирана хартија (IP), гума и др., наречен изолација на кабелот. Изолацијата има определена дебелина и определена диелектрична цврстина, во склад со номиналниот напон на кабелот.

Спроводникот заедно со изолацијата се нарекува жила. Кабелот може да има една жила (едножилен кабел) или повеќе жили (повеќежилен кабел).

Пополнување (полнител, испуна) е соодветен материјал кој се вметнува во празниот простор од кабелската конструкција и служи за постигнување кружен облик на попречниот пресек на кабелот.

Јадрото на кабелот е конструктивна целина што ја сочинуваат сите жили на кабелот, материјалот за пополнување и изолацијата што ги опфаќа сите жили (појасна изолација), доколку ја има. Жилите од кабелот во јадрото се меѓусебно впредени одлево надесно.





Слика 1.6. Градба на енергетски кабли

Каблите со повеќе жили и со заедничка изолација обвиеана околу сите жили се нарекуваат уште и појасни кабли или кабли со нерадијално електрично поле. За разлика од нив, постојат и кабли со радијално електрично поле кои уште се нарекуваат и заштитени кабли или Н-кабли. Заштитените кабли имаат т.н. електрична заштита.

Електричната заштита се состои од тенок слој слабспроводен материјал (н. п. карбонизирана харија) поставен преку спроводникот и слој спроводен материјал кој што се поставува над изолацијата.

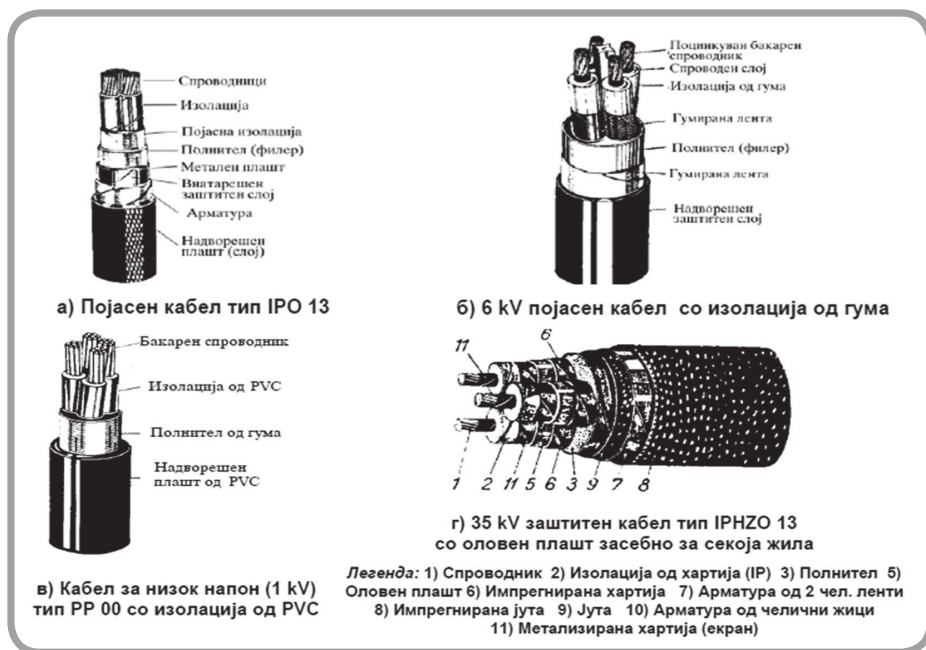
Внатрешниот плашт претставува безрабна цевка изработена од метал (олово, алуминиум, бакар или челик) или од термопластична маса (PVC, PE) односно еластомер (гума). Плаштот цврсто налегнува врз јадрото од кабелот и има задача да ја заштити изолацијата на кабелот од продор на влага и други штетни материји, а истовремено го штити кабелот и од поблаги механички повреди.

Внатрешниот заштитен слој се поставува преку металниот плашт и има задача да го спречи можното триење помеѓу плаштот и арматурата на кабелот, а воедно служи и како хемиска и термичка заштита на самиот плашт.

Арматурата е елемент од кабелската контрукција кој служи за заштита на кабелот од механички оштетувања и повреди до кои може да дојде поради надворешни удари, истегнување, свиткување на кабелот и слично. Има форма на оклоп, обвиткан околу кабелот, а се изработува од челични ленти или поцинкувани челични жици, а понекогаш се изработува од легиран бакар или легиран алуминиум.

Надворешната заштита од корозија (надворешниот плашт) е елемент на кабелот кој има задача да го штити внатрешниот плашт и арматурата на кабелот од корозија и механички оштетувања. Кај неармираните кабли (кабли кои немаат челична арматура) тој се поставува директно преку металниот плашт, додека пак кај армираните кабли тој се поставува преку самата арматура на кабелот. Надворешниот плашт е последниот, завршен слој на кабелот.

На сликата 1.7 се прикажани конструкциите на некои почесто употребувани типови кабли. Во понатамошниот дел од текстот, ќе стане збор за секој елемент од конструкцијата на кабелот - одделно.



Слика 1.7. Конструкција на разни типови кабли

Типови на кабли

Кабли со изолација од импрегирана хартија и метален влакно

Овие кабли се произведуваат за напони од 1 до 60 kV. Во зависност од применетиот тип на механичка заштита и во зависност од начинот на изработката, се применуваат за хоризонтално, косо и вертикално полагање. Се положуваат на отворен простор, во затворени простории, директно во земјата, во кабелски канали, под вода, во рудници и на други места. Според конструкцијата и начинот на изработката се делат на:

- појасни кабли (за напони до 10 kV);
- заштитени Н-кабли (за напони до 20 kV);
- заштитени кабли со 3 метални плашта (за напони до 60 kV);
- едножилни кабли (за напони до 60 kV).

Појасни кабли

Жилите кај овие кабли се изведени од бакарни или алуминиумови проводници, изолирани со импрегирана хартија. Жилите, заедно со пополнувањето (жили од хартија или јута) меѓусебно се впредуваат. Над впредените жили се намотува заедничка изолација од импрегирана хартија, која се нарекува појасна изолација. Врз така формираното „јадро“ од кабелот, се поставуваат: металниот плашт, внатрешната заштита од корозија, челичната арматура и надворешната заштита од корозија. Се изработуваат за напони до 10 kV.

Заштитени (екранизирани) кабли

Поради нерадијалниот карактер на електричното поле, појасните кабли не се произведуваат за напони над 10 kV. Кај заштитените Н-кабли, со помош на слабоспроводниот слој под и над изолацијата и со помош на екранот (метализирана хартија) кој се поставува преку изолацијата од IP, се постигнува симетричност, т.е. радијалност на електричното поле, а со тоа и повишување на пробојниот напон на кабелот. Екранизираните жили се впредуваат, заедно со пополнувањето, а потоа се обмотуваат со метална фолија или пак со памучна лента која е проткаена со тенки бакарни жички. Имаат ознака IPHO или NPHO и се произведуваат за напони до 20 kV.



Заштитени кабли со шри метални влашша

Кај овие кабли секоја жила има засебен метален плашт. На тој начин радијалната структура на електричното поле во изолацијата од секоја жила на кабелот се постигнува со помош на самиот метален плашт. Над металниот плашт се нанесува слој импрегнирана хартија. Така формираните жили се впредуваат и се добива јадрото на кабелот. Над јадрото се поставува заедничка механичка заштита (челична арматура) и надворешна заштита од корозија. Се изработуваат за напони до 60 kV.

Едножилни кабли

И кај едножилните кабли електричното поле во изолацијата има чисто радијална структура. Тоа овозможува овие кабли исто така да се произведуваат за напони до 60 kV.

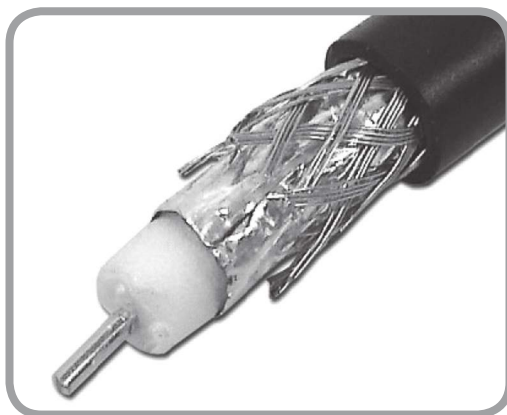


Мрежни кабли

Каблите денес претставуваат доминантен медиум за пренос на податоци. Постојат многу различни типови на кабли кои можат да се применат во различни ситуации (спрема каталог на една водечка фирма во таа област постојат повеќе од 2200 различни типови). Најголем дел од денешните телекомуникациски мрежи користат три основни видови на кабли и тоа:

- Коаксијални кабли
- Оптички кабли
- Кабли со упредена метална парица

Коаксијален (соосен) кабел е кабел што се состои од заштитна надворешна обвивка направена од изолатор под кој е поставена метална мрежа обвиена околу изолирани проводни жици. Сите овие делови се наоѓаат на истата заедничка оска од каде и потекнува името на овој вид кабел. Коаксијалниот кабел е откриен од страна на англискиот инженер и математичар Оливер Хевајсајд, патентирајќи го дизајнот за првпат во 1880 година.



Коаксијалниот кабел се употребува за пренесување на телефонски, телеграфски, телевизиски, а во поново време и пренос на интернет сигнали со висока фреквенција, под земја, над земја или под море, за пренос на податоци во компјутерски системи. Една од предностите на коаксијалниот кабел во однос на останатите радио преносни кабли е во тоа што електромагнетното поле коешто се создава во самиот кабел се грижи сигналот да е активен само во просторот помеѓу внатрешните и надворешните проводници. Оваа предност овозможува инсталација на коаксијален кабел во близина на метални објекти обезбедувајќи заштита на сигналот од надворешни електромагнетни интерференци (попречувања).

Коаксијалниот кабел се разликува од другите заштитни (изолирани) кабли коишто се користат за пренос на пониски фреквентни сигнали како што се аудио сигналите, во тоа што опсегот на кабелот е контролиран да обезбеди прецизно константно т.н спроводливо растојание, коешто е потребно за да функционира ефикасно како што се радио фреквенциските трансмисиони (преносни) кабли.

За избор на дизајн на коаксијалниот кабел влијае физичката големина, фреквентните перформанси, ослабувањето, способноста за регулирање на енергијата, флексибилноста, јачината и цената. Внатрешниот спроводник може да биде полн или лиснаст, лиснастиот е пофлексибилен. За да се добие подобри високо фреквентни перформанси, внатрешниот спроводник може да биде сребрен.

Изолаторот којшто го опкружува внатрешниот спроводник може да биде цврста пластика, пенлива пластика, или можеби само воздух придружувајќи го внатрешниот жица (спроводник). Својствата на изолаторот контролираат некои електрични својства на кабелот. Вообичаено се избира цврст полиетиленски (PE) изолатор, употребуван во кабли со помала загуба. Цврст тефлон (PTFE) е исто така користен како изолатор. Некои коаксијални жици користат воздух (или некој друг гас) и содржат одредени т.н делови (места) за да спречат внатрешниот спроводник да дојде во допир со металната мрежа-обвивката.

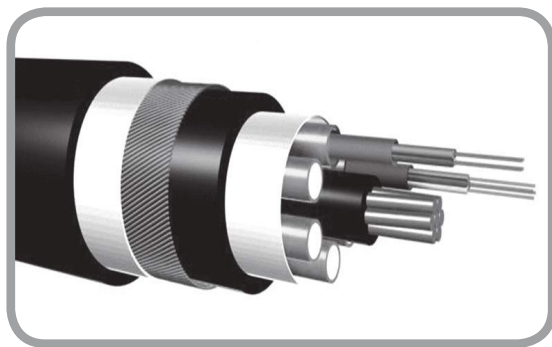
Вообичаено многу од коаксијалните кабли користат бакарни жици испреплетени, формирајќи ја металната мрежа-обвивката. Ова му овозможува на кабелот да биде флексибилен, но исто така има и празнини во обвивката, па така внатрешната димензија на обвивката варира речиси незначајно бидејќи плетеницата неможе да биде рамна-сплесната. Понекогаш плетеницата е сребреникава. За подобри перформанси на металната заштитна мрежа, некои кабли имаат двослојна обвивка. Обвивката може да биде само од две плетенки, но сега е подобро да има тенка обвивка од фолија покриена со плетеницата. Некои кабли може да содржат повеќе од двослојни обвивки како што се “quad-shield” коишто користат четири наизменични слоеви од фолија и плетеница. Некои дизајни за обвивки ја жртвуваат флексибилноста за подобри перформанси, некои обвивки се цврсти метални цевчиња-проводници. Овие кабли не наоѓаат примена при инсталирање на кабел на места со остри кривини бидејќи обвивката ќе се засука што ќе предизвика загуба во кабелот.

За пренос на високи радио фреквенции повеќе од 1 GHz, коаксијален кабел со цврст бакарен надворешен спроводник е достапен во димензии од 0.25 инчи па нагоре.

Коаксијалниот кабел има потреба од внатрешна структура на некаков вид изолаторен материјал, со цел да може да го одржи просторот

пomeѓу централниот спроводник и обвивката. Изолаторските загуби растат по овој редослед: идеален изолатор (без загуба), вакум, воздух, политетрафлуоретилен (PTFE), полиетиленска пена, и цврст полиетилен. Пониска релативна допустливост овозможува поголема фреквентна искористеност. Еден нехомоген изолатор треба да биде надоместен со некружен спроводник за да се избегнат моменталните т.н жаришта (анг. hot-spots).

Оптички кабел е кабел кои содржи едно или повеќе оптички влакна. Оптичките влакна се обвивени со пластична обвивка заради заштита и полесна употребливост во средините каде што треба кабелот да биде спроведен. Во пракса, обвивката на влакното е премачкана со слој од смола, кој може да биде понатаму опкружен со заштитен слој од стакло. Овие слоеви му даваат цврстина на влакното, но не допринесуваат за подобрување на неговите карактеристики. Понекогаш помеѓу влакната кои се врзани во сноп се поставува стакло кое ја апсорбира светлината таканаречено темно стакло. За да се спречи светлината која може да излезе од едно влакно и да влезе во друго. Ова го спречува вкрстувањето на сигналите помеѓу влакната или го намалува одблесокот во снопот од влакна наменет за апликациите со слики.



Модерните оптички кабли доаѓаат со голема разновидност на обвивки наменети за различни потреби како изолација од висок напон, двојно користење за линии кои пренесуваат моќност, антени за телефон, инсталации за подморници или асвалтирани улици.

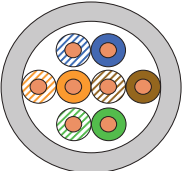
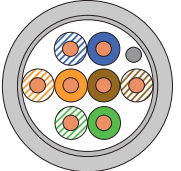
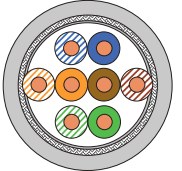
Оптичките кабли можат да бидат многу флексибилни, но нормалната загуба во голема мера порасна кај влакната со радиус помал од 30 мм. Ова создава проблем кога кабелот е свиткан околу аглите или замотан правејќи FTTX инсталации. Каблите кои можат да се вијат и лесно да се употребуваат за инсталации во домовите се стандардизирани како ITU-T G.657. Овој вид на оптички кабел може да биде свиткан во радиус од 7,5 mm, без негативни последици. Исто така овие кабли се отпорни на хаڪери зошто сигналот во влакното е неприметно мониториран од истекување.

Друга важна функција на кабелот е издржливоста од хоризонтално применетата сила. Технички се нарекува затегнувачка цврстина дефинирајќи колку сила може да се примени врз кабелот додека трае процесот на инсталација.

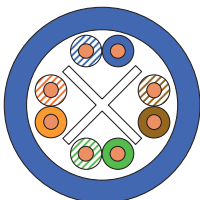
Кабли со уѝредена метална ѝарица

Типот (генерацијата) на кабелот воглавно генерално го дефинира капацитетот и намената на кабелот. Cat.5е е димензиониран за изведба на мрежи до 1000 Mbps. Cat.6 каблите се димензионирани за чисто гигабитни мрежи. Имаат поголем капацитет на пренос на податоци и на кратки растојанија можат да се постигнат и брзини до 10 Gbps. За пренос со брзини од 10 Gbps се димензионирани Cat.6а каблите и кај нив ваков пренос може да се сертифицира. Кај поновите типови на кабли Cat.7/7а капацитетот на пренос расте, па се во можност за пренос дури и на Broadband Video.

Накратко се опишани повеќе различни конструкции на кабли од повеќе генерации.

Cat.5e		
		
UC300 24 Cat5e U_ UTP AWG 24 U/UTP кабел категорија 5E DRAKA изолација PVC или LSZH; тестиран до 300MHz, сертификати DELTA & 3P - 'Wall', 4 парици со полн пресек; пакуван во кутија 305m; останати сертификати ISO9001, ISO14001, RoHS..... Апликации: Инст. на места со мало EMI поле Primary (Campus), Secondary (Riser), Tertiary (Horizontal) IEEE 802.3: 10Base-T; 100Base-T; 1000Base-T; IEEE 802.5 16 MB; ISDN; TPDDI; ATM	UC300 S24 Cat5e F_ UTP AWG 24 F/UTP кабел категорија 5E DRAKA изолација PVC или LSZH; тестиран до 300MHz, сертификати DELTA & 3P - 'Wall', 4 парици со полн пресек и заштитна метална фолија околу нив; пакуван во кутија 305m; останати сертификати ISO9001, ISO14001, RoHS..... Апликации: Инст. на места со големо EMI поле Primary (Campus), Secondary (Riser), Tertiary (Horizontal) IEEE 802.3: 10Base-T; 100Base-T; 1000Base-T; IEEE 802.5 16 MB; ISDN; TPDDI; ATM	UC300 HS24 Cat5e U_ UTP AWG 24 SF/UTP кабел категорија 5E DRAKA изолација PVC или LSZH; тестиран до 300MHz, сертификати DELTA & 3P - 'Wall', 4 парици со полн пресек и заштитна метална фолија и ширм околу нив; пакуван во кутија 305m; останати сертификати ISO9001, ISO14001, RoHS..... Апликации: Инст. на места со многу големо EMI поле Primary (Campus), Secondary (Riser), Tertiary (Horizontal) IEEE 802.3: 10Base-T; 100Base-T; 1000Base- T; IEEE 802.5 16 MB; ISDN; TPDDI; ATM

Cat.6



UC400 23 Cat6 U_UTP AWG 23

U/UTP кабел категорија 6 DRAKA изолација PVC или LSZH; тестиран до 400MHz, сертификати DELTA & 3P - 'Wall', 4 парици со полн пресек и **крстаст елемент помеѓу париците** за нивно раздвојување; пакуван во кутија 305m и котур од 500m; останати сертификати ISO9001, ISO14001, RoHS.....

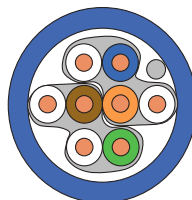
Апликации:

Инстал.на места со мало EMI поле

Primary (Campus), Secondary (Riser), Tertiary (Horizontal)

IEEE 802.3: 10Base-T; 100Base-T; 1000Base-T;

IEEE 802.5 16 MB; ISDN; TPDDI; ATM



UC400 S23 Cat6 U_FTP AWG 23

U/FTP кабел категорија 6 DRAKA изолација PVC или LSZH; тестиран до 400MHz, сертификати DELTA & 3P - 'Wall', 4 парици со полн пресек и **наместо крстаст елемент има заштитна метална фолија помеѓу нив** што резултира со помало преслушување; пакуван во котур 500m; останати сертификати ISO9001, ISO14001, RoHS.....

Апликации:

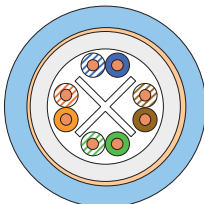
Инст. на места со големо EMI поле

Primary (Campus), Secondary (Riser), Tertiary (Horizontal)

IEEE 802.3: 10Base-T; 100Base-T; 1000Base-T;

IEEE 802.5 16 MB; ISDN; TPDDI; ATM

Cat. 6a



UC500 23 Cat6a U_UTP AWG 23

U/UTP кабел категорија 6a DRAKA изолација PVC или LSZH; тестиран до 500MHz за 10GbE, сертификати DELTA & 3P - 'Wall', 4 парици со полн пресек, **крстаст елемент помеѓу париците и патентирана 10G фолија**; пакуван во котур 500m; останати сертификати ISO9001, ISO14001, RoHS.....

Апликации:

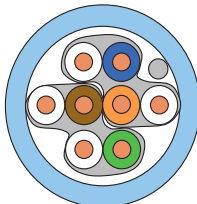
Инстал.на места со мало EMI поле

Primary (Campus), Secondary (Riser), Tertiary (Horizontal)

IEEE 802.3: 10Base-T; 100Base-T;

1000Base-T; 10GbBase-T

IEEE 802.5 16 MB; ISDN; FDDI; ATM



UC500 S23 Cat6a U_FTP AWG 23

U/FTP кабел категорија 6a DRAKA изолација PVC или LSZH; тестиран до 500MHz, сертификати DELTA & 3P - 'Wall', 4 парици со полн пресек и **наместо крстаст елемент има заштитна метална фолија помеѓу нив**; пакуван во котур 500m; останати сертификати ISO9001, ISO14001, RoHS.....

Апликации:

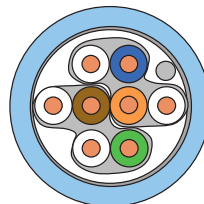
Инстал.на места со големо EMI поле

Primary (Campus), Secondary (Riser), Tertiary (Horizontal)

IEEE 802.3: 10Base-T; 100Base-T;

1000Base-T; 10GbBase-T

IEEE 802.5 16 MB; ISDN; FDDI; ATM



UC500 AS23 Cat6a F_FTP AWG 23

F/FTP кабел категорија 6a DRAKA изолација PVC или LSZH; тестиран до 500MHz, сертификати DELTA & 3P - 'Wall', 4 парици со полн пресек, **метална фолија околу две парици и заедничка метална фолија околу сите парици**; пакуван во котур 500m; останати сертификати ISO9001, ISO14001, RoHS.....

Апликации:

Инстал.на места со многу големо EMI поле

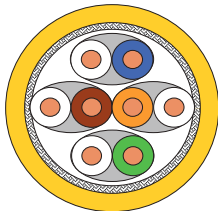
Primary (Campus), Secondary (Riser), Tertiary (Horizontal)

IEEE 802.3: 10Base-T; 100Base-T; 1000Base-T;

10GbBase-T

IEEE 802.5 16 MB; ISDN; FDDI; ATM

Cat. 7, 7a



UC900 HS23 Cat7 S FTP AWG 23

S/FTP кабел категорија 7 DRAKA изолација LSZH; тестиран до 900MHz за 10GbE, сертификати DELTA, 3P & GHMT, 4 парици со полн пресек, **алуминиумска фолија околу секоја парица и бакарна фолија околу сите парици (40% покриеност)**; пакуван во котур 500m; останати сертификати ISO9001, ISO14001, RoHS.....

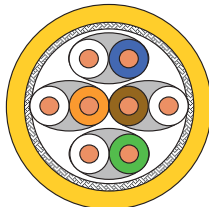
Апликации:

Инстал.на места со многу големо EMI поле

Primary (Campus), Secondary (Riser), Tertiary (Horizontal)

IEEE 802.3: 10Base-T; 100Base-T; 1000Base-T; 10GBase-T

IEEE 802.5 16 MB; ISDN; FDDI; ATM



UC900 SS23 Cat7 S FTP AWG 23

U/UTP кабел категорија 7 DRAKA изолација LSZH; тестиран до 900MHz за 10GbE, сертификати DELTA, 3P & GHMT, 4 парици со полн пресек, **алуминиумска фолија околу секоја парица и бакарна фолија околу сите парици**; пакуван во котур 500m; останати сертификати ISO9001, ISO14001, RoHS.....

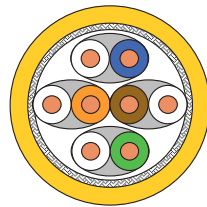
Апликации:

Инстал.на места со многу големо EMI поле

Primary (Campus), Secondary (Riser), Tertiary (Horizontal)

IEEE 802.3: 10Base-T; 100Base-T; 1000Base-T; 10GBase-T

IEEE 802.5 16 MB; ISDN; FDDI; ATM



UC1000 SS23 Cat7a S FTP AWG 23

S/FTP кабел категорија 7a DRAKA изолација LSZH; тестиран до 1000MHz за 10GbE, сертификати DELTA, 3P & GHMT, 4 парици со полн пресек, **алуминиумска фолија околу секоја парица и дебела бакарна фолија околу сите парици**; пакуван во котур 500m; останати сертификати ISO9001, ISO14001, RoHS.....

Апликации:

Инстал.на места со многу големо EMI поле

Primary (Campus), Secondary (Riser), Tertiary (Horizontal)

IEEE 802.3: 10Base-T; 100Base-T; 1000Base-T; 10GBase-T

IEEE 802.5 16 MB; ISDN; FDDI; ATM

Правила на поставување на електрична инсталација

Уредите и опремата за електрични инсталации (во натамошниот текст: електричната опрема) мораат да бидат погодни за работа при номиналниот напон на електричната инсталација, односно при ефективната вредност на напонот за наизменична струја. Ако во ИТ систем се води неутрален спроводник, електричната опрема се приклучува помеѓу фазниот и неутралниот спроводник и мора да биде изолирана за меѓуфазен напон.

Електричната опрема мора да и одговара на проектираната струја односно на ефективната вредност на струјата за наизменична струја која ќе протекува во текот на нормалната работа. Електричната опрема мора да поднесе струи кои протекуваат во вонредни услови, во текот на временските периоди што ги допуштаат карактеристиките на уредите за заштита.

Ако фреквенцијата влијае врз карактеристиките на електричната опрема, номиналната фреквенција на таа опрема мора да и одговара на фреквенцијата на соодветното напојно струјно коло.

Електричната опрема определена според карактеристиките на моќноста на електричната опрема што се вградува мора да биде погодна за нормална работа, земајќи ги предвид факторите на оптоварување и интермитенција.

Електричната опрема, при нормална работа и при вклучување и исклучување, не смее штетно да дејствува врз друга опрема. Електричната опрема, вклучувајќи ги проводниците и каблите, мора да се постави така што да може лесно да се проверува, одржува и до се приоѓа до нејзините приклучоци и лесно да се ракува со неа.

Натписите, плочките и другите средства што служат за распознавање мораат да се постават на расклопните апарати заради означување на нивната намена. Управувачките елементи и елементите за сигнализација (тастери, сигнални светилки и др.) мораат да се поставуваат на лесно пристапни и видливи места.

Изолираните проводници и кабли мораат да се положат и означат така што да можат лесно да се распознаат при испитување, поправање или заменување.

Заштитниот спроводник (PE спроводник) и заштитно - неутралниот спроводник (PEN спроводник) се означуваат со комбинација на зелена и жолта боја, а неутралниот спроводник (N спроводник) се означува со светлосина боја. Комбинацијата на зелена и жолта боја и светлосината боја не смее да се употреби за кое и да било друго означување.

Означување може да се врши и на крајот на спроводникот, близу спојот, особено кога проводниците не се изолирани.

Уредот за заштита мора да се постави и означи така што лесно да може да се распознае неговото припаѓачко струјно коло. Уредот за заштита мора да се постави во расклопен блок (разводен орман, разводна табла, команден пулт и др.).

Шемите, дијаграмите или табелите на електричните инсталации за низок напон мораат да се постават на места на кои има повеќе струјни кола, така што да ја означуваат природата (типот) и составот на струјните кола (точките на напојување и бројот и пресекот на изолираните проводници и кабли) и карактеристиките за распознавање на уредите за заштита, вклучување и исклучување, како и нивното место за поставување и изолација.

Во расклопниот блок (разводната табла, разводниот, орман, командниот пулт или разводната кутија) мора да се постави и да се групира електричната опрема од ист вид на струја и/или напон и да се раздели од електричната опрема од друг вид на струја и/или напон, така што да не може да дојде до меѓусебно штетни влијанија.

1.2. НАПОНИ, СТРУИ, ОПТОВАРУВАЊА, ПОЛАРИТЕТ И СИМБОЛИ ВО ЕЛЕКТРОТЕХНИКАТА

Електротехниката, електрицитет

Уште многу одамна, луѓето ги забележале електричните појави. Така, уште во стара Грција, пред нашата ера е забележано дека килибарот кога ќе се протрие со волнена крпа ги менува особините и може да привлекува некои предмети. Подоцна е утврдено дека и други материјали смола, порцелан, стакло со триење може да стекнат со слични својства.

Со взаемното дејство на наелектризираните тела и фактот дека некои од нив се привлекуваат, а некои се одбиваат, се дошло до заклучокот дека постојат две електрични состојби. Утврдено е дека овие две состојби настануваат едновременно. Ако го протриеме стаклото со амалгамова кожа, едната состојба се јавува на стаклото, а истовремено на кожата се јавува другата состојба. Исто така меѓусебното дејство може да биде појако или послабо, од што следи заклучокот дека електричните состојби на телата може да се разликуваат и по интензитет.

Електричната состојба на телата во минатото се објаснувала дека на телата постои „нешто“ кое ги предизвикува овие состојби. Тоа „нешто“ е наречено **електрицитет**.

Електротехниката е наука која ги проучува појавите што се последица на електрицитетот. Своеето име, електротехниката го има добиено според грчкото име на килибар - електрон.

Долго време електрицитетот е сметан за некој вид гас или многу подвижна течност – флуид. Врз основа на таквото толкување, биле создадени таканаречените флуидни теории за електрицитетот. Според едната од овие теории, се сметало дека постојат два вида на флуиди. На секое не наелектризирано тело постојат двата вида флуиди во еднакви количества. Ако на некое тело преовладее едниот вид флуид, телото станува наелектризирано. Според другата флуидна теорија, постои еден вид флуид, кој е рамномерно распореден по сите тела. Ако на некое тело има повеќе или помалку флуид отколку што е нормално, тоа тело станува наелектризирано. Телата што имале повеќе електрицитет биле наречени позитивно наелектризирани тела, а пак телата што имале помалку електрицитет биле наречени негативно наелектризирани тела.

Преку хипотезите за електричните флуиди воведен е поимот за количество на електрицитет, како карактеристика на наелектризираните тела. Како физичка величина, количеството електрицитет (количеството

полнеж) е дефинирана со помош на Кулоновиот закон. Со истиот закон дефинирана е и единицата за мерење на количество електрицитет е Кулон [1 C].

Кулон во 1785 година го објавил законот со кој се дефинира одредена сила F на меѓусебното дејство на две наелектризирани тела чии димензии се многу мали во однос на нивното меѓусебно растојание r . Законот гласи:

$$F = k \frac{Q_1 Q_2}{r^2}$$

односно:

$$F = k \frac{Q^2}{r^2}$$

во случај кога количеството електрицитет на телата Q_1 и Q_2 се еднакви и означени со Q . Коефициентот k е коефициент на сразмерност и има вредност еден за тела кои се наоѓаат во вакуум.

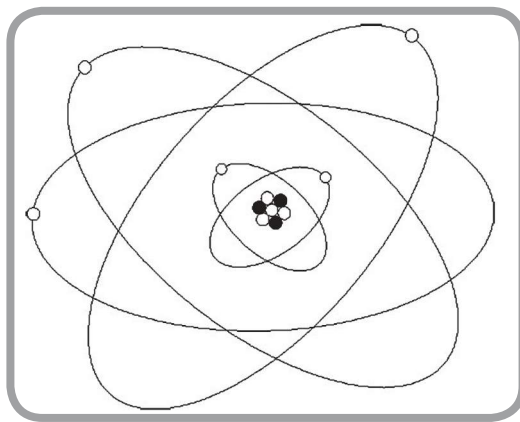
Вистинскиот развиток на електротехниката започнува во текот на XIX век. Во тоа време откриени се законите, кои претставуваат основа на современата електротехника. Врз основа на тие откритија, доаѓа и до меѓусебно поврзување на одделни делови од физиката, кои дотогаш се развивале независно една од друга. Со таквото поврзување, оформена е денешната електротехника. За оформување на современата електротехника значајни се откритијата на францускиот физичар Ампер (Ampere). Имено, во периодот од 1820-1825 година, тој утврдил дека постои цврста врска меѓу електричните струи и магнетните појави. Неговите откритија го отвориле патот кон сознанието дека природниот магнетизам е последица на одредени електрични струи кои се создаваат во некои материи.

Во 1864 година, физичарот Максвел (Maxwell) утврдил дека електричното и магнетното поле претставуваат само посебна форма на едно единствено поле. Таквото поле тој го нарекол **електромагнетно поле**. Своите заклучоци Максвел ги темелел на резултатите од одредени експерименти, извршени од Фарадеј (Faraday) во 1831 година. Ваквото гледање на појавите претставува основа на современата електротехника. Интересно е да се спомене дека во 1864 година Максвел по теоретски пат го утврдил постоењето на електромагнетни бранови. Нивното постоење е потврдено по експериментален пат од Херц, дури во 1888 година. Експериментите на Фарадеј, со кои во 1834 година ја проучувал електролизата, ја побиле флуидната теорија на електрицитетот. Тие експерименти покажале дека во природата мора да постои најмало можно количество електрицитет. Со откривањето на електронот, од страна на Џ. Џ. Томасон (J. J. Tomason) во 1897

година откриен е и носителот на најмалото количество електрицитет во природата.

Градба на материјата

За да може полесно да се разберат електричните појави, потребно е да се имаат некои основни познавања за градбата на материјата. Сите елементи и соединенија во природата се составени од атоми и молекули. Во суштина, молекулите претставуваат група на атоми кои меѓу себе се поврзани во една целина. Поради тоа, може да се смета дека атомот е основен елемент од кој е составена материјата (зборот атом доаѓа од зборот атомос, што значи неделив). Овој поим го вовел грчкиот филозоф Демокрит, уште во V век пред н.е. Тој сметал дека материјата е составена од мали, неделиви, непроменливи и неуништливи честици. Во однос на појавите кои ќе ги разгледуваме, молекулите се однесуваат на ист начин како и атомите. Поради тоа, ќе се задржиме на разгледување на основните особини на атомите. Секој хемиски елемент е составен од атоми кои се карактеристични само за него. Но, во основа, сите имаат иста градба. За објаснување на некои појави кои ќе не интересираат, ќе го користиме моделот на атом даден од Н. Бор (N. Bor) (сл. 1.8).



Слика 1.8.

Овој модел, во извесна мерка, потсетува на Сончевиот систем, поради што се нарекува планетарен модел на атом. Атомите се составени од таканаречени елементарни честици. Елементарните честици од кои се составени атомите се: електрони, протони и неутрони. Протоните и неутроните со еден збор се нарекуваат нуклеони.

Наелектризираноста се создава заради преминувањето на **електроните** од еден материјал во друг. Електроните носат негативен електричен полнеж. Притоа, материјалот што губи електрони станува позитивен, додека материјалот што прима електрони станува негативно наелектризиран. Наелектризираните предмети привлекуваат мали предмети како што се парчиња хартија.

Ако два наелектризирани предмета се постават еден до друг, врз нив ќе влијае сила. Предметите може да се привлечат еден кон друг или да се одбијат еден од друг. Предметите со ист електричен полнеж ќе се одбиваат, додека предметите со спротивен електричен полнеж ќе се привлекуваат.

Предмет со електричен полнеж ќе привлекува предмет без електричен полнеж. Предмет со електричен полнеж може да биде неутрализиран со негово поврзување со земјата преку проводник. Ако кај предметот се собере голем електростатички полнеж, тој може да биде опасен. Колку што е поголем полнежот, толку е поголем напонот меѓу предметот и Земјата. Ако напонот е доволно голем, електрицитетот може да прескокне од предметот до најблискиот **заземјен проводник**.

Високите згради имаат заземјени громобрани, со што се намалува опасноста од пожари.

Електричниот полнеж може да биде со различен **поларитет**:

- *Позитивен*, чијшто носители се протоните
- *Негативен*, чијшто носители се електроните

Електричен напон, електрична струја и електрична отпорност

Електричен напон претставува разлика на електрични потенцијали помеѓу две точки на електрично или електронско коло, изразен во волти. Тој ја мери потенцијалната енергија на електрично поле кое предизвикува електрична струја низ проводник. Единица мерка за електричен напон е Волт [V].

Електрична струја претставува ток (движење) на електричен полнеж. Во системот SI (System International), единица мерка за електрична струја е Амперот [A], кој е еднаков на тек од еден кулон електрицитет во секунда.

Количество на електрична струја (мерено во амperi) низ некоја површина (на пр. пресек на бакарен проводник) е дефинирано како количество на електричен полнеж (мерено во кулони) кој поминува низ таа површина во единица време. Ако Q е количество на полнеж кој поминува низ површина во единица време t , тогаш просечна струја изнесува:

$$I = \frac{Q}{t}$$

Доколку времето t оставиме да тежнее кон 0, тогаш ја добиваме моменталната струја $i(t)$:

$$i(t) = \frac{dQ}{dt}$$

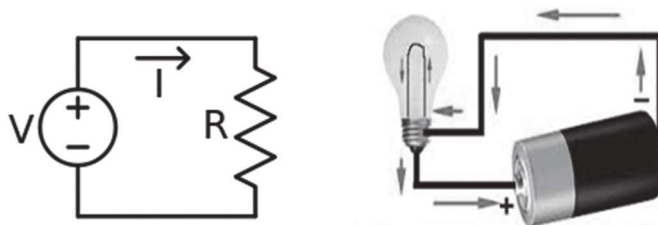
Да претпоставиме дека имаме проводник со пресек A - даден во метри квадратни, должина ℓ - даден во метри m и специфичен електричен отпор на материјалот од кој е изработен проводникот ρ - изразена во ом метри - Ωm . Неговиот отпор ќе биде :

$$R = \frac{\ell \cdot \rho}{A}$$

Спротивставувањето на електричната струја од страна на елементите на колото се нарекува **електрична отпорност**. Отпорноста зависи од:

- типот на материјалот
- површината на напречниот пресек
- неговата должина
- неговата температура

Единица мерка за електрична отпорност е Ом [1Ω]. На слика 1.9 се прикажани основни електрични кола низ кои тече **еднонасочна струја DC** (Direct Current). Кај оваа струја треба да се внимава на **поларитетот** на приклучоците - постои позитивен „+“ и негативен „-“ приклучок.



Слика 1.9.

Напонскиот извор V , предизвикува електрична струја I , низ отпорникот R , тоа се трите величини на кои се однесува Омовиот закон. **Омовиот закон** се однесува на електрични кола и тој вели дека:

Струјата помеѓу две точки е директно пропорционална со **напонот** (потенцијалната разлика) и обратно пропорционална со **отпорот** помеѓу нив. Математички, тоа се изразува како:

$$I = \frac{U}{R}$$

Каде што I е струјата во ампери, U е потенцијалната разлика во волти, и R е електричната отпорност изразена во оми. Потенцијалната разлика е позната и како пад на напонот, и може да се означува и со V , E или EMC (електромоторна сила).

Оваа законитост ја открил германскиот физичар Георг Ом, и ја објавил во 1827 година како резултат на лабораториски мерења, и во малку посложена форма.

Покрај еднонасочната струја, постои и **наизменична струја AC** (Alternating Current). Кај оваа струја нема поларитет, туку „фаза“ и „нула“ соодветно.

Отпорноста на повеќето отпорнички материјали (отпорници) е константна за широк спектар на струи и напони. Кога отпорникот се употребува во вакви околности, неговата отпорност се нарекува „омска“. Покрај омската отпорност, постои и капацитивна и индуктивна, кои се јавуваат кај променливите и наизменичните струи.

Омовиот закон, во презентираната форма, е мошне корисен за електротехниката, затоа што опишува како напонот, струјата и отпорот се поврзани на „макроскопско“ ниво, односно како елементи на електричното коло. Физичарите кои ги проучуваат електричните својства на материјалите на микроскопско ниво ја употребуваат равенка:

$$J = \sigma E$$

каде што J е густина на струјата (струја по единична површина), σ е електричната спроводливост, а E е електричното поле.

Во однос на електричната спроводливост што ја имаат, материјалите ги делиме на **проводници и изолатори**. Во проводниците, надворешните електрони во секој атом можат лесно да одат или дојдат и се нарекуваат слободни електрони. Во изолаторите, надворешните електрони не можат слободно да се движат. Проводници се металите како што се: сребро, бакар, злато, алуминиум и др. Најчесто употребувани изолатори се следните материјали: стакло, гума, масло, асфалт, порцелан и др. Затоа велíme дека проводниците имаат мала отпорност, а изолаторите имаат многу голема отпорност.

Постојат и материјали кои се изолатори, но во одредени случаи може да станат проводници. Овие материјали се нарекуваат **полупроводници**,

а најпознати полупроводници се: силициум, германиум и галиум арсенид, од кои се изработуваат различни полупроводнички елементи: диоди, транзистори, интегрални кола.

Електромагнетна индукција

Индуцирана струја

Магнетните полиња се користат за производство на електрични струи. Оваа идеја е искористена во генераторите за производство на електрична струја и во трансформаторите за зголемување или намалување на електричниот напон. Ако магнет се вметне во намотка што претставува составен елемент на струен круг, во намотката се создава (се индуцира) електрична струја.

Ако магнетот се повлече надвор од намотката или во намотката се вметне спротивниот пол на магнетот, тогаш насоката на струјата ќе се промени. Меѓу двата краја на намотката се создава напон кога намотката ги пресекува магнетните силиви линии. Создадениот напон предизвикува проток на електрична струја низ намотката.

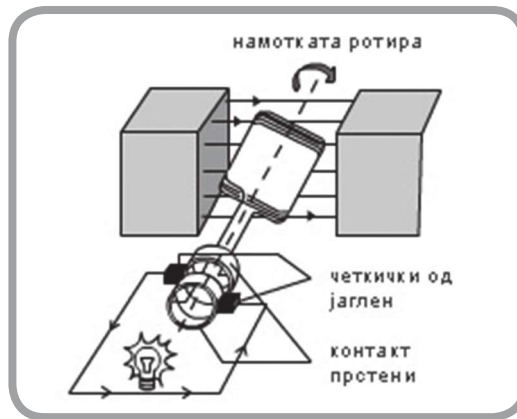
Големината на индуцираниот напон зависи од:

- Брзината на движењето низ магнетното поле
- Јачината на магнетното поле
- Бројот на навоите во намотката
- Големината на површината на намотката

Генератори

Генераторите ја користат идејата на електромагнетна индукција за да произведат електрична енергија. Во ротирачко магнетно поле се сместува намотка или пак, самиот магнет ротира во жичена намотка. Намотката е поддржана од посебни прстени што се вртат заедно со неа. Четките од јаглен го одржуваат контактот.

Кога намотката ротира, индуцираната струја се пренесува преку четките до надворешниот струен круг. Како што намотката ротира, една нејзина страна патува нагоре низ магнетното поле, додека другата страна патува надолу низ магнетното поле. Одовде, индуцираната струја првин патува во една насока, потоа во друга насока. Оваа струја е наречена **наизменична струја**.

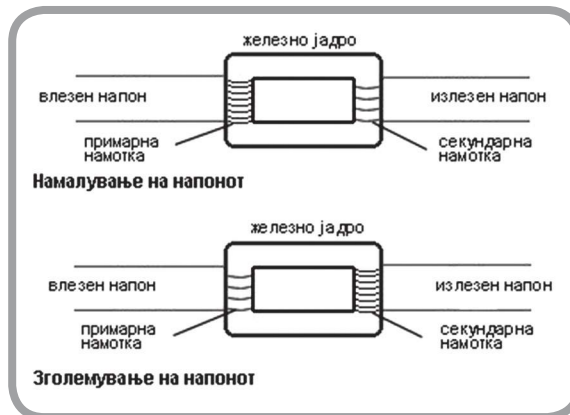


Слика 1.10.

Ако намотката се движи во насока во која таа не пресекува магнетни силиви линии, тогаш во неа не се индуцира струја.

Трансформатори

Трансформаторите се употребуваат за промена на напонот на наизменичната струја.



Слика 1.11.

Како што наизменичната струја тече низ примарната намотка на трансформаторот, така таа индуцира променливо магнетно поле во железното јадро. Натаму, ова предизвикува индуцирање на струја во секундарната намотка.

Ако примарната намотка содржи поголем број навои од секундарната, напонот на излезот од секундарната намотка ќе биде помал од напонот на влезот на примарната намотка. Ако примарната намотка содржи помал број навои од секундарната, напонот на излезот од секундарната намотка ќе биде поголем од напонот на влезот на примарната намотка. Напоните на примарната и секундарната намотка се во следниот сооднос:

$$\frac{\text{напон на примарна намотка}}{\text{напон на секундарна намотка}} = \frac{\text{број на навивки во примарна намотка}}{\text{број на навивки во секундарна намотка}}$$

Во електраните, **трансформаторите** го зголемуваат напонот пред електричната енергија да биде ослободена во националната електрична мрежа. Ова значи дека е потребна помала струја за пренос на електрична енергија при зачувување на соодносот на преносот. При тоа, каблите за пренос помалку се греат, што значи дека има помали загуби во енергијата. Освен тоа, каблите може да бидат потенки и полесни. Во трафостаниците, напонот се намалува пред испораката на електричната енергија до потрошувачите.

Трофазна струја е систем од три назименични струи меѓу кои има фазно поместување. Фазното поместување помеѓу напоните на одделните фази во симетричен трофазен систем изнесува 120°. Трофазниот систем е најчесто користен повеќефазен систем и на него се заснива денешниот глобален електроенергетски систем.

Проводниците во трофазниот систем вообичаено се идентификуваат според бојата на нивните изолатори. Боите би требало да соодветствуваат на меѓународниот стандард IEC 60446, но во пракса се среќаваат и имплементации на постари стандарди или не се практикуваат никакви стандарди и можно е да има различни имплементации и во една иста инсталација. Пример во Канада и САД се користат различни бои за заземјени и незаземјени системи. На слика 1.12 се прикажани различни стандарди за обележување на трифазните инсталации.

Old fixed cables colors in european countries (CENELEC - feb. 1996)																		
	Austria	Belgium	Czech Republic	Denmark	Finland	France	Germany	Hungary	Ireland	Italy	Norway	Portugal	Slovak Republic	Sweden	Switzerland	United Kingdom		
PE																		
N																		
L1				no requirements						IEC 445	no requirements			no requirements				
L2									any exsept above									
L3																		
Prohibited	 	 		 					 				 					
G-Y and Blue G-Y with Blue marking Black or brown																		

Слика 1.12.

Електротехнички елементи, електротехнички симболи

Електѝричен оѝѝорник

Поспецифично, Омовиот закон вели дека отпорот R во релацијата е константен, без разлика на струјата I . Електричната отпорност е еднаква на падот на напонот низ отпорникот поделена со струјата низ него при константна температура. Отпорниците се употребуваат во електрични и електронски кола. Електричната отпорност се мери во Оми (Ω). Бидејќи отпорниците се произведени со голем опсег на отпорности, се користат и милиоми ($1\text{ m}\Omega = 10^{-3}\Omega$), киломи ($1\text{ k}\Omega = 10^3\Omega$) како и мегаоми ($1\text{ M}\Omega = 10^6\Omega$).

На слика 1.13 се прикажани симболи на отпорник. Симболите со стрелка означуваат променлив отпорник (потенциометар):



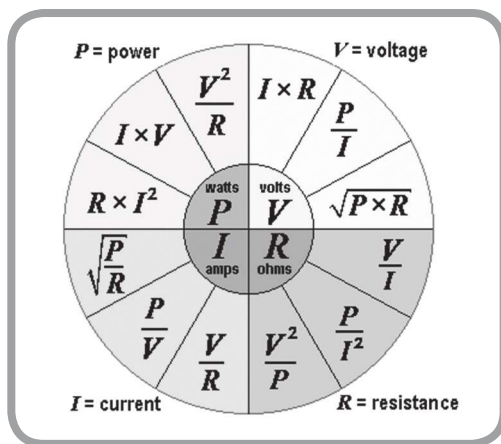
Слика 1.13.

Електрично оптоварување претставува онаа снага со која одреден отпорник може да ја прими, а да не се оштетат неговите витални функции. Електричната снага или моќност во електричните кола се означува со P , а единица мерка за електрична моќност е ват [1 W] и генерално се одредува со формулата:

$$P=UI=I^2R=\frac{U^2}{R}$$

Каде U е електричниот напон, I е електричната струја, а R е електричната отпорност.

На слика 1.14 се прикажани меѓусебните зависности на основните електрични величини:



Слика 1.14.

Иако на некои отпорници е напишана вредноста на нивната електрична отпорност, најчесто означување е со четири обоени прстени околу телото на отпорникот. Кодирањето е едноставно: првите две бои ја означуваат вредноста, третиот е мултипликатор (бројот на нули - 10^n), а четвртиот прстен ја означува прецизноста односно толеранцијата. На слика 1.15 е покажано означување на отпорник со 4 прстени:



Слика 1.15.

Овој отпорник означен со четири прстени (син, сив, црн, златен) има отпорност од 68 ома и толеранција од $\pm 5\%$. На слика 1.16 се прикажани значењето на боите на отпорници обележани со четири прстени.

Боја на прстенот	1.	2.	3.(мултипликатор)	4.(толеранѝија)
Црна	0	0	$\times 10^0 (=1)$	
Кафена	1	1	$\times 10^1$	$\pm 1\% (F)$
Црвена	2	2	$\times 10^2$	$\pm 2\% (G)$
Портокалова	3	3	$\times 10^3$	
Жолта	4	4	$\times 10^4$	
Зелена	5	5	$\times 10^5$	$\pm 0,5\% (D)$
Сина	6	6	$\times 10^6$	$\pm 0,25\% (C)$
Виолетова	7	7	$\times 10^7$	$\pm 0,1\% (B)$
Сива	8	8	$\times 10^8$	$\pm 0,05\% (A)$
Бела	9	9	$\times 10^9$	
Златна			$\times 10^{-1}$	$\pm 5\% (J)$
Сребрена			$\times 10^{-2}$	$\pm 10\% (K)$
Без боја				$\pm 20\% (M)$

Слика 1.16.

Елекѝричен кондензаѝор

Кондензаторот е електротехнички елемент, кој може да ја сочува енергијата во облик на електрично поле. Комбинаѝија на две тела проводници кои се наелектризирани со исти, но по знак спротивни количества електриѝетет и кои меѓусебно се добро изолирани електрично, се викаат електричен кондензатор, прикажан на слика 1.17. Металните тела од кои е составен кондензаторот се викаат електроди на кондензаторот.



Слика 1.17.

Во електрониката, кондензаторот е пасивен електронски елемент, па поради потребата за поголем капаѝитет и други работни својства се произведуваат технолошки различни видови кондензатори: повеќеслоен керамички, диск керамички, повеќеслоен фолијски, цвѝчест керамички, полистиролски (аксијален и радијален), електролитски.

Нека едната електрода на еден кондензатор е наелектризирана со количество електрицитет Q , а другата со $-Q$, при што напонот меѓу нив е U . Со помош на низа мерења (наелектризирајќи го кондензаторот со различни количини електрицитет и мерејќи го напонот) или со помош на теоретски испитувања, се заклучува дека напонот меѓу електродите е правопрпорционален со количина електрицитет. Според тоа, количникот:

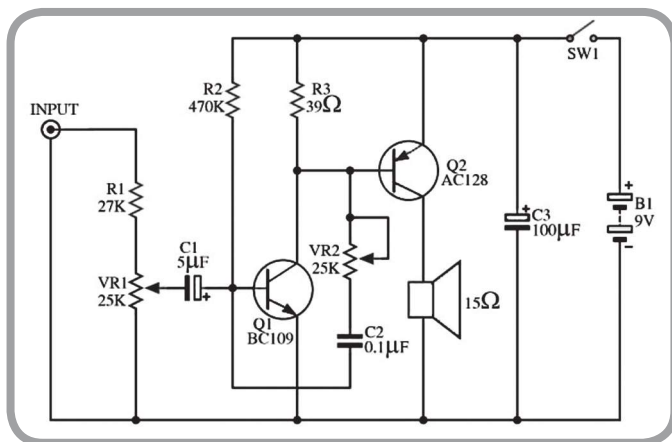
$$C = \frac{Q}{U} [F]$$

е карактеристичен за дадениот кондензатор. Оваа величина се вика капацитет на кондензаторот, а единицата во која се мери се вика фарад (F), во чест на Фарадеј.

Електричниот кондензатор е, всушност направа во која при определен потенцијал може да се собере (кондензира, натрупа) големо количество електричество.

Електйройшехнички симболи

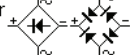
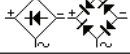
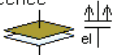
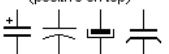
Електротехничките елементи имаат соодветни електротехнички симболи. Овие елетротехнички симболи се користат за прикажување на електротехничките елементи на електрични шеми. На слика 1.18 е прикажан пример на електрична шема.



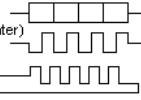
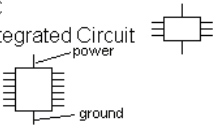
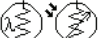
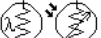
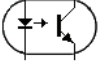
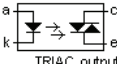
Слика 1.18.

Електротехничките симболи се разликуваат во некои земји, а постојат и разлики во самиот начин на поврзување во електричните шеми.

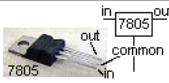
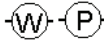
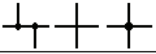
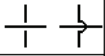
1. Сите симболи се елементи (електронски компоненти) освен линиите;
2. Сите елементи се означени со буква + реден број и вредност или тип под неа. Буквата зависи од типот на елементот и тоа: R - Отпорници, VR - Променливи отпорници, C - Кондензатори, Q - Транзистори, D - Диоди, L - Калеми, U - интегрирани кола, V - електронски цевки и т.н;
3. Сите линии се „жици“ или каде што поврзува линијата значи има електричен контакт помеѓу елементите;
4. Каде што се сечат линиите, а има црна точка во спојот значи дека има електричен контакт помеѓу нив. Каде што линиите се сечат, а нема црна точка значи дека се разминуваат и нема електричен контакт помеѓу нив;
5. Во некои американски шеми се употребува „прескок“ на шемата што означува дека нема контакт. Во таквите шеми значи секаде има контакт и без да има точка освен на местата како што е нацртан „прескок“;
6. Секој елемент има изводи (наречени исто и пинови или контакти);
7. Бројот на пинови на електронскиот елемент е во зависност од типот на елементот;
8. За изгледот на симболот на одреден елемент може да се види во соодветниот туторијал каде што се опишува тој елемент;
9. Постојат елементи кои се неполаризирани (на пример отпорниците, керамичките и блок кондензаторите) на кои двата изводи им се исти и можат да се поврзат и во двете насоки и елементи кои се поларизирани (електролитски кондензатори, транзистори, диоди, интегрирани кола) на кои мора точно да се знае кој пин каде треба да се поврзе;
10. Постојат многу симболи кои означуваат елементи кои и не се електронски туку електрични, како на пример: прекинувачи, приклучоци, преклопници, батерии и слично. Изгледот на некои од електротехничките симболи кои претставуваат одредени електротехнички елементи е прикажан слика 1.19:

ЕЛЕКТРОТЕХНИЧКИ СИМБОЛИ			
AC current:  voltage: 	ALTERNISTOR TRIAC A TRIAC and 33 - 43v DIAC  Main Terminal 1 Gate Main Terminal 2	Ammeter (amp meter) 	
AND Gate 	AND Gate 	Antenna balanced 	
Antenna Loop, Shielded 	Antenna Loop, Unshielded 	Antenna unbalanced 	
Attenuator, fixed (see Resistor) 	Attenuator, variable (see Resistor) 	Battery 	
Bilateral Switch (DIAC) 	Bridge Rectifier (Diode Bridge) 	BUFFER (Amplifier Gate) 	
BUFFER (Amplifier Gate) 	Buzzer 	Capacitor feedthrough 	
Capacitor non-polarised 	Capacitor polarised (see electrolytic) 	Capacitor Variable 	
Cavity Resonator 	Cell 	Circuit Breaker 	
Coaxial Cable 	CRO - Cathode Ray Oscilloscope 	Crystal Microphone (Piezoelectric) 	
Connectors Plug (male)  Jack (female)  connected  Plug (male)  (female) 	Crystal Piezoelectric  Darlington Transistor  collector base emitter DIAC (Bilateral Switch) 	DC current:  voltage:  Delay Line 	
Diode - Gunn 	Diode - Light Emitting (LED) 	Diode Photo Sensitive 	
Diode Photovoltaic 	Diode Bridge (Bridge Rectifier) 	Diode - Pin 	
Diode - Varactor 	Diode - Zener 	Earth Ground 	
Earpiece (earphone, crystal earpiece)  	Electroluminescence  el	Electret Microphone (Condenser mic) 	
Electrolytic (Polarised Capacitor)  alternate symbols: (positive on top) 	Electrolytic - Tanatalum positive end black band or chamfer  10u tantalum	Exclusive-OR Gate (XOR Gate) 	
Field Effect Transistor (FET) n-channel also: N-Channel J FET  Gate Drain Source	Field Effect Transistor (FET) p-channel also: P-Channel J FET  Gate Drain Source	Exclusive-OR Gate (XOR Gate) 	
		Flashing LED (Light Emitting Diode) (Indicates chip inside LED) 	

ОСНОВИ НА ЕЛЕКТРОТЕХНИКА И ТЕЛЕКОМУНИКАЦИИ

Ferrite Bead 	Fuse 	Galvanometer 
Globe 	Ground Chassis 	Ground Earth 
Heater (immersion heater) (cooker etc) 	IC Integrated Circuit 	Inductor Air Core 
Headphone 	Inductor Tapped 	Inductor Iron Core or ferrite core 
Inductor Tapped 	Inductor Variable 	Integrated Circuit 
Inverter (NOT Gate) 	INVERTER (NOT Gate) 	Jack Phone (Switched) 
Jack Co-axial 	Jack Phone (Phone Jack) 	Lamp Incandescent 
Jack Phone (3 conductor) 	Key Telegraph (Morse Key) 	LDR (Light Dependent Resistor) 
Lamp - Neon 	LASCR (Light Activated Silicon Controlled Rectifier) 	LDR (Light Dependent Resistor) 
LASER diode 	Light Emitting Diode (LED) 	Light Emitting Diode (LED - flashing) 
Mercury Switch 	Micro-amp meter (micro-ammeter) 	Microphone (see Electret Mic) 
Microphone (Crystal - piezoelectric) 	Milliamp meter (milli-ammeter) 	Motor 
NAND Gate 	NAND Gate 	Nitinol wire "Muscle wire" 
Negative Voltage Connection 	NOR Gate 	NOR Gate 
NOT Gate Inverter 	NOT Gate Inverter 	Ohm meter 
Operational Amplifier (Op Amp) 	Optocoupler (Transistor output) 	Opto Coupler (Opto-isolator) 
Optocoupler (Darlington output) 	Opto Coupler (Opto-isolator) 	OR Gate 
OR Gate 	Oscilloscope see CRO 	Outlet (Power Outlet) 
Piezo Diaphragm 	Photo Cell (photo sensitive resistor) 	Photo Diode 
Photo Darlington Transistor 	Photo FET (Field Effect Transistor) 	Photo Transistor 

Photovoltaic Cell (Solar Cell)		Piezo Tweeter (Piezo Speaker)		Positive Voltage Connection	
Potentiometer (variable resistor)		Programmable Unijunction Transistor PUT		Rectifier Silicon Controlled (SCR)	
Rectifier Semiconductor		Reed Switch		Relay - spst	
Relay - spdt		Relay - dpst		Relay - dpdt	
Resistor Fixed		Resistor Non Inductive		Resistor preset	
Resistor variable		Resonator 3-pin		RFC Radio Frequency Choke	
Rheostat (Variable Resistor)		Saturable Reactor		Schmitt Trigger (Inverter Gate)	
Schottky Diode (also Schottky) Low forward voltage 0.3v Fast switching also called Schottky Barrier Diode		Shielding		Shockley Diode 4-layer PNP device Remains off until forward current reaches the forward break-over voltage.	
Silicon Bilateral Switch (SBS)		Silicon Unilateral Switch (SUS)		Silicon Controlled Rectifier (SCR)	
Surface Mount		Switch - spst		Solar Cell	
Switch - push (Push Button)		Switch - spdt		Switch - process activated normally open: normally closed:	
Test Point		Switch - dpst		Flow	
Thermal Probe NTC: as temp rises, resistance decreases		Switch - dpdt		Level	
Transformer Air Core		Switch - mercury tilt switch		Pressure	
		Spark Gap		Temperature	
		Switch - push off (used in alarms etc)		Speaker	
		Thyristors: Main Terminal1		Switch - Rotary	
		Bilateral Switch		Thermocouple	
		DIAC		Tilt switch mercury	
		SCR		Touch Sensor	
		TRIAC		Transformer (Tapped Primary/Sec)	
		TRIAC			

Transistor Bipolar - NPN 	Transistor Bipolar - PNP 	Transistor n-channel Field Effect 
Transistor p-channel Field Effect 	Transistor Metal Oxide Single Gate 	Transistor Metal Oxide Dual Gate 
Transistor Photosensitive 	Transistor Schottky - NPN 	Transistor Unijunction - UJT 
TRIAC 	Transistor Unijunction - UJT 	Tunnel Diode 
Varactor varactor diode 	Voltage Regulator (7805 etc) 	Unijunction Transistor - UJT 
Voltmeter 	Wattmeter 	Wires Connected 
Wires Not Connected 	XOR Gate (exclusive OR) 	XOR Gate (exclusive OR) 
Zener Diode 		

Слика 1.19.

1.3. ЗАШТИТА ПРИ РАБОТА ВО ЕЛЕКТРОТЕХНИКАТА

Основни поими за заштита при работа

За да се доживее струен удар потребно е човекот да дојде во допир со напон во проводник или машина која по грешка добила напон на своето куќиште. За да се доживее струен удар потребно е низ човековото тело да протече струја, а тоа се случува кога стоиме на земја или пак со нашите екстремитети сме допрени до некој проведен елемент. При струен удар низ нашето тело протекува струја. Јачината на струјата зависи исклучиво од електричниот отпор што го има човековото тело. Овој отпор е различен од човек до човек, а и од условите во кои го доживеал струјниот удар. Исто така зависи од изолацијата на обувките што се носат во тој момент. При доживување на струен удар, протокот на струја предизвикува три основни дејствија кои што можат да го повредат или умртват човековото тело. Тие се: топлоотно дејство, механичко дејство и хемиско дејство.

Заштита од превисок напон при допир на предметите и деловите од опремата што во нормални работни услови не се под напон, се изведува на еден од следните начини:

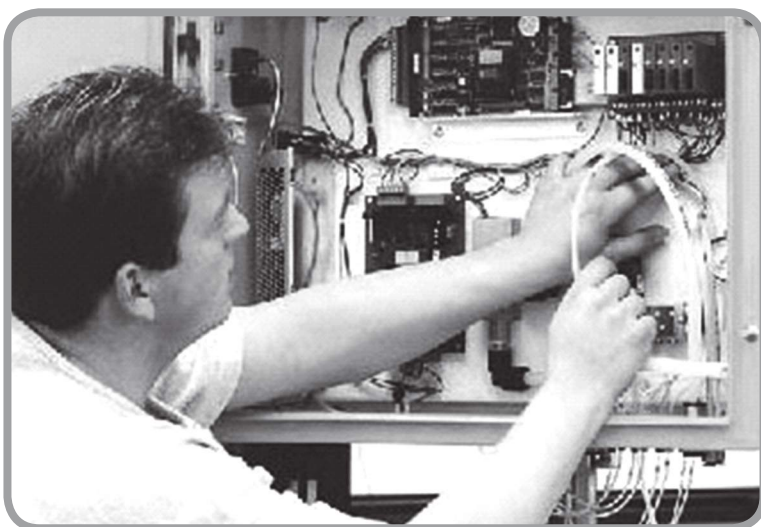
- Со заштитно изолирање
- Со мал напон
- Со нулување
- Со заштитен напонски прекинувач
- Со заштитен струен прекинувач
- Со заштитен трансформатор за галванско одвојување
- Со систем за заштитни водови

Заштитата од случаен допир на деловите од опремата и инсталациите што се под напон се изведува со изолирање или со поставување на активните делови надвор од дофат на рацете. Изолирање со помош на лак, смола или слични материјали не се смета за доволно сигурен материјал, па затоа се употребуваат посебни материјали како поливинилхлорид и гума.

Заштита на работници и други лица

За заштита на сите работници и други лица кои работат или се движат во близина на контактната мрежа пред исклучување на напонот во неа, работа на заземјувањето и изедначувањето на потенцијалот, при што не е дозволено да се врши:

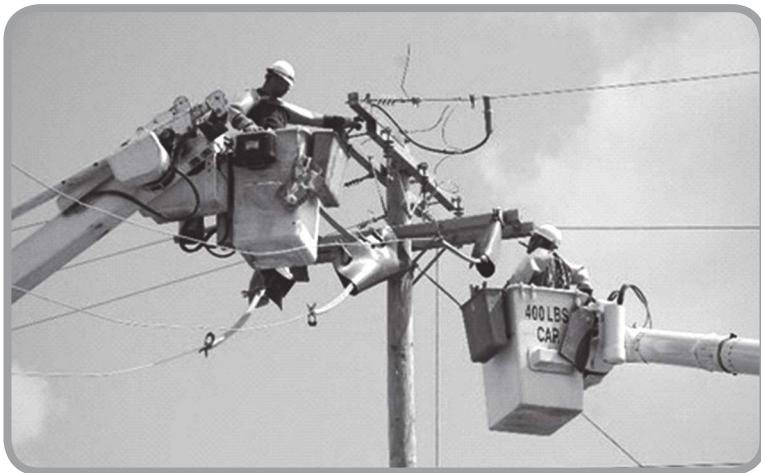
- допир со деловите на контактната мрежа
- допир со делови на контактната мрежа кои висат или проводник кој е откинат од напојните односно обиколните или возните водови како и со сите предмети кои се нафрлени и висат
- пристап на местото каде е паднат прекинатиот проводник на земја, внатре во кругот со полупречник 15 m, чиј центар претставува паднатиот проводник, или крајот на металниот дел кој е во допир со паднатиот проводник
- влегување со било кој дел од телото или со алат односно предмет во зоната на опасност



- качување на носечки конструкции од контактната мрежа и останатите метални конструкции
- качување на покривот од дизел или електровлечно возило и на покривите на патничките или товарните вагони, на отворени товарни вагони, вагон - цистерни, ладилници, градежни машини за одржување на колосеците и на дигалки со подвижни кранови кога се наоѓаат на електрифициран колосек
- полевање со вода во близина од 2 метра на било кој дел од контактната мрежа
- гасење на пожар со вода на товари, вагони, локомотиви, складови и други објекти во близина на деловите од стабилните постројки на електричната влека

Заштита при работа на висина

Работа на височина не може да се врши безбедно и според соодветните ергономски услови од соодветна површина, без да се одбере работна опрема најсоодветна за обезбедување и одржување безбедни услови за работа. Колективните заштитни мерки треба да добијат приоритет пред личните заштитни мерки.



Димензиите на работната опрема треба да бидат соодветни на природата на работата што треба да се врши и на предвидените стресови и да дозволуваат движење без опасност. Најсоодветните мерки на пристап до привремени работни места на височина треба да се одберат според зачестеноста на преминувањето, височината на која се преминува и времетраењето на употребата. Направениот избор треба да дозволува евакуација во случај на непосредна опасност. Преминувањето во која било насока меѓу средство за пристап и платформите, катови или мостови не смее да предизвикува дополнителни ризици од паѓање. Може да се користат скали како работни места за работа на височина единствено во околности кога, употребата на друга побезбедна работна опрема не е оправдана поради ниското ниво на ризик и краткото времетраење на употребата или постоечките карактеристики на местото што работодавачот не може да ги измени. Пристап со јаже и техники за позиционирање може да се користат единствено во околности каде што проценката на ризикот покажува дека работата може да се врши безбедно и каде што употребата на друга, побезбедна работна опрема не е оправдана. Земајќи ја предвид проценката на ризикот и во зависност особено од времетраењето на работата и ергономските ограничувања, треба да се обезбеди седиште со соодветна

додатна опрема. Во зависност од типот на одбраната работна опрема врз основа на претходно кажаното, треба да се определат соодветните мерки за минимизирање на ризиците по работниците што се вклучени кај овој тип опрема. По потреба, може да се предвиди инсталирање штитници за спречување падови. Тие треба да бидат со соодветна конфигурација и доволно силни за да спречат или ублажат падови од височина и, колку што е тоа можно, да оневозможат повредување на работниците. Колективните штитници за спречување падови може да бидат прекинати единствено на места на пристап на вертикална скала или скали. Кога вршењето одредена задача бара привремено отстранување на колективен штитник за спречување падови тогаш треба да се преземат ефективни компензирачки безбедносни мерки. Задачата не може да се изврши се додека не се преземат такви мерки. Штом се заврши конкретната задача, конечно или привремено, колективните штитници за спречување падови треба да се реинсталираат. Вертикалните скали треба да се постават така што ќе се обезбеди нивна стабилност во текот на употребата. Подвижните вертикални скали треба да се потпираат на стабилна, силна и соодветно голема неподвижна основа за скалилата да останат хоризонтални.



Висечките вертикални скали треба да бидат сигурно прикачени и, со исклучок на вертикалните скали од јажиња, така што нема да можат да се изместат и така што ќе се спречи нишање. Ногарките на подвижните вертикални скали треба да се заштитат од лизгање во текот на употребата со прицврстување на вертикалните елементи кај или во близина на горните или долните краеве со направа против лизгање или на друг подеднакво ефективен начин. Вертикалните скали што се користат за пристап треба да бидат доволно долги за во доволна мера да ја надминуваат платформата за пристап, освен ако не се преземени други мерки за да се обезбеди цврсто место за држење со рацете. Споените вертикални скали и продолжителните скали треба да се користат на тој начин што ќе се спречи различните делови да се движат едниот во однос на другиот. Треба да се спречи мобилните скали да се движат пред да се стапне на нив. Вертикалните скали треба да

се користат на таков начин што на работниците во секое време ќе им бидат достапни сигурен ракофат и сигурна потпора. Особено, ако треба да се носи товар на рака по вертикални скали, не смее да се оневозможи присуството на сигурен ракофат.

При работа на висина може да се користи и скеле во зависност од комплексноста на одбраното скеле, треба да се подготви план за монтирање, употреба и демонтажа од страна на компетентно лице.



Тоа може да биде во облик на стандарден план дополнет со точки во врска со специфичните детали на предметното скеле. Треба да се спречи лизгањето на носечките компоненти на скелето, дали преку прикачување на носечката површина, обезбедување направа против лизгање или на друг подеднакво ефективен начин, а површината што го носи товарот треба да има доволен капацитет. Треба да се обезбеди скелето да биде стабилно. Скелето на тркала треба со соодветни направи да се спречи да не се движи случајно во текот на работата на височина.

Заштита при работа со струја

Врз електричната опрема се применуваат технички мерки за заштита од индиректни допири, со тоа што техничката мерка за заштита со автоматско исклучување на напојување не се применува врз деловите на електричната инсталација каде што неопходноста од напојување е суштествена и во случаите кога не е ефикасна.



Заштитата на деловите на електричната инсталација од индиректен допир, каде што непрекинатоста на напојувањето е суштествена или заштитата со автоматско исклучување на напојувањето не е ефикасна, се остварува кога електричната опрема се поставува во неспроводни простории или со локално изедначување на потенцијалот без поврзување со земјата.

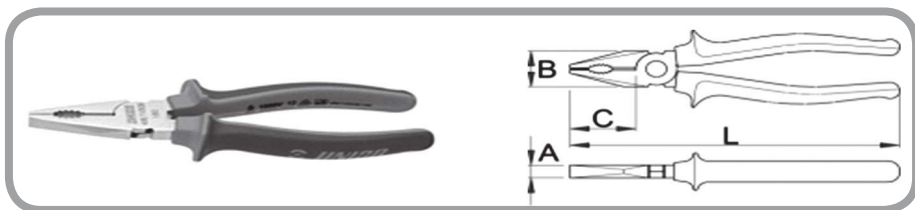
Техничките мерки за заштита со безбедносно мал напон, со користење на опрема од класата II или со примена на еквивалентна изолација, како и со електрично одвојување, можат да се применуваат на целата електрична инсталација или на одредени нејзини делови.



Техничките мерки за заштита од индиректен допир не се применуваат при изведувањето на електрични инсталации врз: потпорни изолатори и метални делови споени со нив, прибор за надземни водови ако е надвор од дофатот на раката, бетонско железо ако не е пристапно, изложени спроводни делови со мали димензии (до 50 mm x 50 mm) или ако се надвор од дофатот на раката, а мерката за заштита со поврзување за заштитниот спроводник е тешко изводлива (на пример: завртки, заковки, натписни плочки, кабелски шелни и ел.), метални цевки или други метални кукишта што ја штитат електричната опрема во согласност со барањата за класата II или за еквивалентна изолација.

Изолирани клешти и опрема и нивна намена во електрониката

Комбинирана клешта - 406/1VDEBI



материјал: специјален челик, ковани, целосно појачани и калени, ивиците за сечење со индукционо појачани полирани челусти.

завршна површина: хромирани робусни двокомпонентни рачки, изолирани, изработена според стандард ISO 5746 и EN 60900.

Електро комбинирки клешти - 420/1VDEBI



материјал: специјален челик, ковани, целосно појачани и калени, ивиците за сечење се индукционо појачани, со полирани челусти и хромирани по стандард EN60900.

Лична заштитна опрема е важна за одржување на безбедноста при работа со електричните системи. Еден важен дел од личната заштитна опрема се гумени безбедносни ракавици. Електричните безбедносни ракавици мора да поседуваат комбинација од издржливост и флексибилност.



Ракавиците се класифицирани врз основа на нивото на заштита на гумена изолација и максималниот дозволен напон. Кожната заштита на ракавиците се наоѓа на врвот на гумените изолациони ракавици.

Опрема за лична заштита (ППЕ) е форма на дополнителна заштита од повреди при работа.



Личната заштитна опрема вклучува: гумени ракавици со ракави, заштитна маска и заштитни очила, пластични капи, незапалива облека и електрички изолирани чизми.

1.4. ВИДОВИ НА ТЕЛЕКОМУНИКАЦИИ, ОПШТИ ПОИМИ

Историја на телекомуникациите

Отсекогаш постоела потребата за комуницирање на луѓето и таа е стара колу што е стар човекот. И обичниот разговор е еден вид на комуникација. Но, за пренос на вести, пораки, информации, на поголеми растојанија биле користени најразлични начини: гласници, поштенски писма, димни сигнали и др. При крајот на XVIII век е употребено првото посериозно решение во комуникациите како светлосна телеграфија. Во 1844 година, Морзе го остварил првиот телеграфски пренос по електричен пат, од кога и започнува брзиот развој на телекомуникациите.

Телефонијата е посовршен вид на пренос на говор во реално време, а нејзин оснивач е Грахам Бел и неговите испитувања и демонстрации во 1878 година. Подоцна со откривањето на електромагнетните бранови се овозможува безжичен пренос на пораки и говор на големи растојанија.

Во почетокот на XX век паралелно со развојот на електрониката се остварува и идејата за пренос на слика и почетоките на телевизијата. Така се доаѓа до развој на два системи. Едниот е од типот „точка-точка“ кога два коресподента се директно поврзани, додека другиот е пропагирање од едно место до што поголем број на луѓе т.н. „радиодифузија“.

Првите телекомуникациски сателити се лансираат во 1960 година со што е отворена ерата на сателитските комуникации кои денес се користат за пренос на телефонски, компјутерски и телевизиски сигнали.

Со развојот на дигиталните телекомуникации започнуваат процесите на дигитализација и формирање на интегрирани мрежи при што различните телекомуникациски системи конвергираат во еден единствен транспортен систем. Пример за тоа е интеграцијата на компјутерските системи и телефонските системи од типот VoIP (Voice over IP) во една единствена мрежа.

Денес телекомуникациите се двигател на развојот на светско ниво како стопанска гранка. Развојот на мобилните телекомуникации и Интернетот се подрачја со огромен подем, а бројот на корисниците постојано се зголемува. Од тука и потребата за технички знаења од овие области се зголемува, а со тоа расте и нивото на техничка култура како дел од општата култура на секој современ човек.

Историјата на телекомуникациите т.е. преносот на систем на сигнали преку поголемо растојание се со цел да се создаде комуникација започнала пред илјадници години со употребата на димните сигнали и тапани во

Африка, Америка и во некои делови од Азија. Првите електрични системи за телекомуникации се појавиле во 1830-тите, а подоле се дадени настаните во развојот на телекомуникациите по хронолошки редослед со реализација на различни видови на сигнали:

Визуелни сигнали (не електрични):

- Праисториски: оган, сигнално светло, димни сигнали
- 6-ти век п.н.е.: пошта
- 5-ти век п.н.е.: пошта преку гулаб
- 1790-та година од нашата ера: оптички телеграфи
- 19-ти век од нашата ера: Сигнални светла

Аудио сигнали:

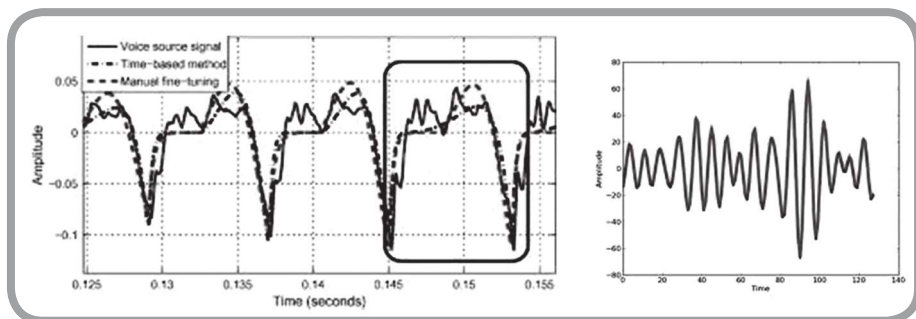
- Праисториски: тапани, хорни
- 1838-ма година од нашата ера: електрични телеграфи
- 1876-та година: телефон
- 1896-та година: радио

Напредни електрични/електронски сигнали:

- 1927-ма година: телевизија
- 1930-та година: експериментален видеофон
- 1964-та година: телекомуникација преку оптички влакна
- 1969-та година: компјутерско мрежно поврзување
- 1981-ва година: аналогни мобилни телефони
- 1982-ра година: електронска пошта
- 1983-та година: интернет
- 1998-ма година: сателитски телефони
- 2003-та VoIP телефонија

Модулација

Речиси во сите области на електротехниката, а исто така и во многу други научни области, значајна улога заземаат теоријата, анализата и проектирањето на сигналите. Во секојдневниот живот поимот за сигналот се поврзува со информацијата која тој ја носи. Од математичка гледна точка сигналот е некаква функција која зависи од една или повеќе независни променливи. Најчесто сигналите се прикажуваат графички во зависност од времето како на слика 1.20.



Слика 1.20.

Сигналите се појавуваат во многу различни облици: кај говорните сигнали информацијата е содржана во изговорените гласови и звучниот сигнал ја претставува информацијата со помош на боја и висина на тон, кај топлотниот сигнал информацијата е искажана со различни вредности на температурата, светлосниот сигнал информацијата ја претставува визуелно, со различен интензитет на светлина или со различно траење на светлите и темните сегменти, електричниот сигнал ја прикажува информацијата со некои од неговите карактеристики – амплитуда или фреквенција.

Технички системи се комплексна структура на меѓусебно поврзани елементи и уреди кои делуваат како една целина и кои се користат да обработуваат и произведуваат сигнали: телевизиски систем, телефонски систем, сателитски систем, систем за пренос на електрична енергија, радарски систем, противпожарен систем, систем за видеонадзор, систем за контрола на пристап и многу други.

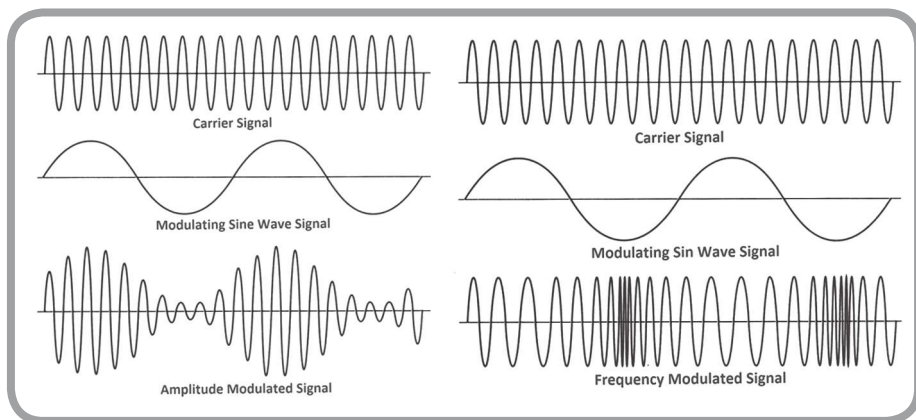
Сигналите се обработуваат во системот од различни причини. Сигналот може да се обработува за да од него се извлече информацијата и истата да се представи на некој погоден начин или врз основа на информацијата да се предвидат некои феномени кои ќе се случат во иднина. Но исто така со обработка сигналот може да се трансформира во облик кој е погоден за пренос на далечина.

Поимот модулација подразбира менување на параметрите на помошен сигнал во зависност од сигналот кој ја содржи информацијата. Помошниот сигнал се нарекува носител (carrier), а сигналот кој ја содржи информацијата и врши промена на носителот се нарекува модулациски сигнал. Како резултат на модулацијата се добива модулираниот сигнал. Уредот во кој се одвива модулацијата се нарекува модулатор.

Така на пример кога се зборува на микрофон некоја радио станица, гласот се претвара во електричен сигнал кој ја содржи информацијата на говорот. Тоа е модулацискиот сигнал. Потоа, модулацискиот сигнал влегува во модулаторот каде ќе се помеша со сигналот на носителот и како резултат на тоа на излезот од модулаторот ќе се добие модулиран сигнал со висока фреквенција. Таквиот сигнал се емитува во етерот до секој радио приемник. Во самиот радио приемник се одвива обратен процес од процесот на модулација, кој се нарекува демодулација. На излез од демодулаторот се добива оригиналниот модулациски сигнал кој се емитува на звучник.

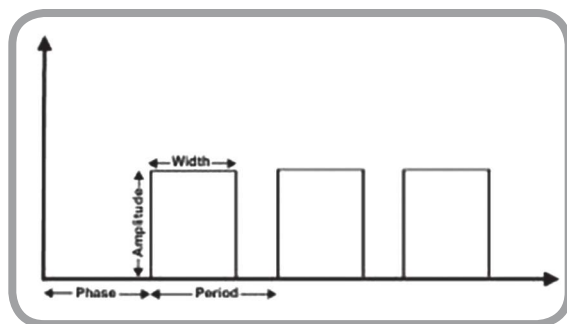
Модулираниот сигнал може да биде континуиран и дискретен. Кај континуираниот модулиран сигнал носителот е секогаш синусоиден и основните негови параметри се : амплитуда, фреквенција и фаза.

Процесот на амплитудна и фреквентна модулација и добивањето на континуиран модулиран сигнал е прикажан на слика 1.21.



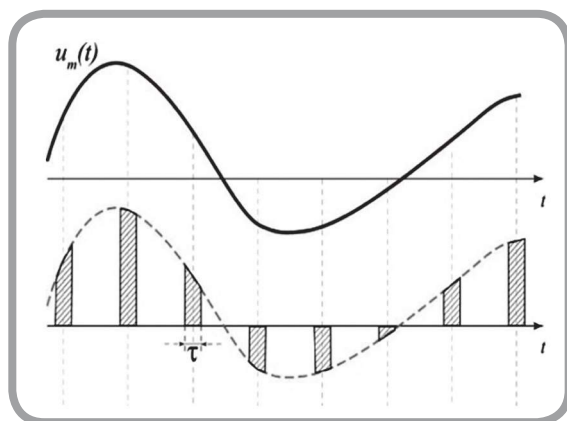
Слика 1.21.

Основна карактеристика на дискретната импулсната модулација е дека како носител се користи дискретен сигнал составен од периодични правоаголни импулси на кои со модулацијата може да се менуваат: амплитудата, траењето и положбата. Ваквиот дискретен носител е прикажан на слика 1.22.



Слика 1.22.

На слика 1.23 е прикажан дискретен модулиран сигнал со импусно амплитудна модулација.



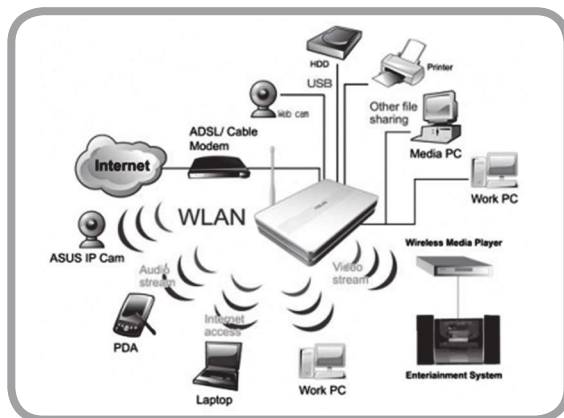
Слика 1.23.

Дискретните сигнали се основа на дигиталните телекомуникации.

Интернет протокол и адресирање

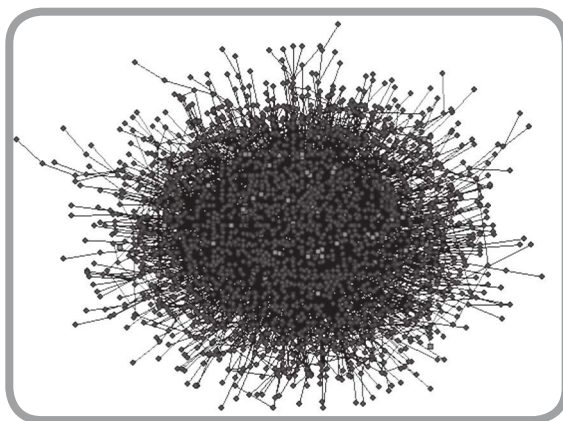
Во денешно време сите користат мобилни телефони и Интернет (INTERnational NETwork - меѓународна мрежа). Бројот на интернет корисниците постојано се зголемува на глобално ниво, така што денес согласно статистиките во светот има повеќе околу 2.5 милијарди корисници или 35 % од вкупното светско население. Пристапот до интернет може да биде од статичен компјутер, пренослив компјутер, таблет, мобилен телефон и различни други уреди. Сите овие уреди приклучени на интернет мора да следат строга адресна хиерархија која овозможува поврзување на уредите и нивна

комуникација. За да не настане хаос и за да целиот систем функционира, сите овие уреди го користат **Интернет протоколот**. Целокупната комуникација функционира со праќање и примање на **IP пакети**. Сите крајни станици (компјутери, IP камери или други IP уреди) се нарекуваат хостови и се вмрежени во локална компјутерска мрежа – LAN (Local Area Network) во рамките на еден објект или зграда. На слика 1.24 се прикажани различни IP уреди поврзани во една локална мрежа.



Слика 1.24.

Локалните компјутерски мрежи се поврзуваат помеѓу себе користејќи мрежни уреди – рутери. На слика 1.25 е прикажана комплексноста на глобалната интернет мрежа.



Слика 1.25.

Почетниот хост кој има IP пакет за праќање, истиот го праќа до најблискиот рутер во рамки на неговата локална мрежа. Овој рутер го прифаќа IP пакетот, го сместува во локална меморија и го проверува дали има некоја грешка. Доколку IP пакетот нема грешки, овој рутер го препраќа до следниот рутер и преку патека низ повеќе рутери, IP пакетот стигнува до дестинацискиот хост. При тоа секој IP пакет се разгледува и праќа посебно и независно од останатите пакети. Затоа помеѓу два крајни хоста пакетите може да патуваат по различни патеки (рути) и при тоа да не стигнуваат последователно на истата дестинација. Доколку има некаков проблем, IP протоколот едноставно го отфрла пакетот и праќа информација за тоа до почетниот хост.

IPv4 е четвртата верзија на Интернет протоколи, но прва верзија која е широко распространета и моментално најкористена на светско ниво. Оваа верзија на Интернет протокол користи 32 битно адресирање кое дозволува, или овозможува користење на вкупно 4,294,967,296 различни уникатни адреси.

IP адресирање

IPv4 адресите се доделуваат по „делегатски“ принцип. Корисниците ја добиваат **IP адресата** од давателот на интернет услугата – **ISP** (Internet Service Provider). Интернет провајдерите ги добиваат IP адресите од локалните, националните и регионалните интернет организации. Македонската национална организација е **МАРНет** каде е регистриран врвниот домен за Македонија, доменот **.mk**. Во рамките на тој домен, МАРНет може да регистрира поддомени на соодветни организации и установи.

Во согласност со одлуката на Управниот одбор на МАРНет од 8 мај 1995 година, а врз основа на правата делегирани од страна на IANA (International Assigned Number Authority), избран е хиерархиски модел на адресирање во рамките на врвниот македонски домен **.mk**.

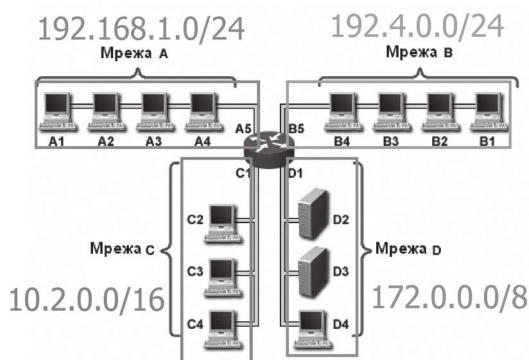
Адресите на Интернет не се земени по места туку по дејности, бидејќи дејностите, како што се образование, стопанство, управа итн. ги има во секоја држава. Овие дејности се наречени домени. Во интернетот постојат 6 домени. Нивните имиња се кратенки од англиското име за дејноста и тоа:

- edu - за образование
- com - за стопанство
- gov - за управни органи и установи
- mil - за војска
- org - за непрофитни организации

Притоа, маската го дефинира мрежниот дел од IP-адресата. Има два начина за означување на мрежите адресирани на овој начин, кои ќе ги илустрираме преку пример:

1. 131.108.122.204/255.255.255.0 (во овој случај маската е во децимален формат, ист како и IP-адресата);
2. 131.108.122.204/24 (во овој случај маската е број кој го дефинира бројот на единици во 32-битната маска, почнувајќи секогаш од левата страна – во случајов маската /24 одговара на децимален формат 255.255.255.0, односно првите 24-бита од форматот на IP-адресата се сетирани на “1”).

На слика 1.27 е прикажано адресирање на повеќе мрежи со различни маски, кои се поврзани во една целина преку рутер.

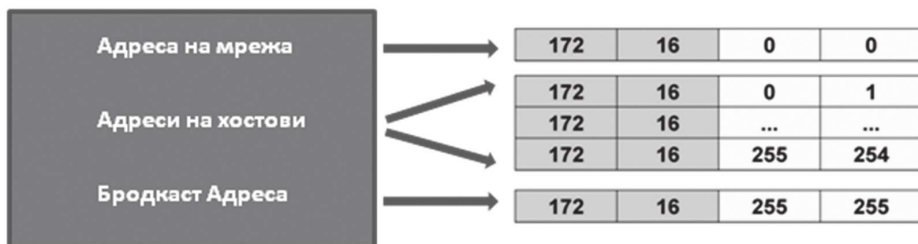


Слика 1.27.

На пример ако е дадена IP адресата 172.16.0.0 со маска на подмрежа 255.255.0.0:

Мрежа	Мрежа	Хост	Хост
172	16	0	0

Тогаш ќе има една адреса на мрежата (172.16.0.0), вкупно 65.534 адреси на хостови и една бродкаст адреса (172.16.255.255).



IPv6 е следното “нешто” во еволуцијата на Интернет протоколи, и најверојатно ќе биде идниот протокол кој ќе биде широко користен и ќе го замени IPv4. Најголемата причина за тоа е што ограничувањето кое IPv4 го има на уникатни IP адреси станува незадоволителен за бројот на корисници на Интернет и популацијата во светот, но секако се очекуваат и одредени подобрувања на полето на безбедноста на комуникацијата.

Вмрежување

Преку мрежите се пренесуваат дигитални и аналогни податоци кои мора да бидат прилагодени кон соодветни системи за пренос. Некои податоците треба да се пренесуваат во реално време (говор, видео и сл.), а некои може да се пренесуваат со одложено време (електронска пошта, пренос на датотеки и сл.). Вмрежување претставува поврзување и комуникација помеѓу компјутерите, серверите и различните мрежни уреди: Концентратори (Hubs), Комутатори (Switches), Рутери (Routers) и меѓумрежни премини (Firewall) по однапред дефинирани правила.

Збирот од два или повеќе компјутери кои се поврзани преку комуникациски медиум и кои меѓусебно можат да комуницираат и да делат ресурси се вика **Компјутерска мрежа**. Вмрежувањето на компјутерите во компјутерски мрежи се прави поради:

- заедничка работа на повеќе корисниците
- размена на податоци и комуникација помеѓу корисниците
- заедничко користење на хардверски ресурси (печатачи, скенери, дискови, и други уреди)
- заедничко користење на софтверски ресурси (апликации, игри и сл.)
- заедничко користење на датотеки (документи, слики, музика и др.)

Компјутерските мрежи според големината и распространетоста главно се поделени на три основни групи:

- локални мрежи LAN (Local Area Networks)

Овие мрежи се просторно ограничени односно поврзаните компјутери се наоѓаат на релативно мал простор, како што е зграда или комплекс од згради. Во локалните мрежи секој компјутер има можност да пристапи до податоци и уреди на некој друг компјутер во мрежата и да користат заеднички податоци и опрема, како што се ласерски печатачи или плотери. Корисникот на секој компјутер одлучува кои ресурси ќе ги дели во мрежата. Кај локалните мрежи преносни медиуми кои се користат се кабли, или пак безжична врска кога се работи за безжична локална мрежа WLAN (Wireless Local Area Network). Безжични локални мрежи имаат помала брзина на пренос на податоци, но обезбедуваат поголема мобилност на корисниците поради едноставното вмрежување.

■ регионални / градски мрежи MAN (Metropolitan Area Networks)

Во овие компјутерски мрежи се поврзуваат компјутери кои се наоѓаат на територија на еден град или регион. Како преносен медиум се користат оптички кабли или телефонски линии и кабли.

■ глобални мрежи WAN (Wide Area Networks).

Во ваквите компјутерски мрежи се поврзуваат компјутерите во поширок регион, држава како национални мрежи или глобални светски мрежи. Тоа е всушност мрежа од повеќе локални и регионални мрежи, а овозможува и комуникација помеѓу мрежи кои не се на ист географски простор. Интернетот е најдобриот пример за овој вид на мрежи. Глобалната мрежа ги поврзува сите мрежи во една целина која овозможува користење на податоци и ресурси низ целата планета.

Според начинот на поврзување, компјутерските мрежи се делат на:

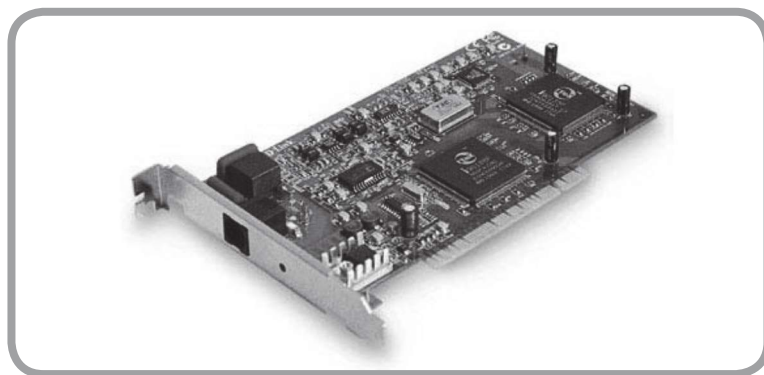
- жичани компјутерски мрежи – користат оптички или бакарни кабли
- безжични компјутерски мрежи – користат радио-бранови.

Според архитектурата на компјутерските мрежи тие можат да се поврзат според две основни архитектури:

- мрежа од рамноправни компјутери (**peer-to-peer**) - Сите компјутери имаат еднакви можности и одговорности, односно секој компјутер може да биде и клиент и сервер. Не постои главен компјутер кој ги надгледува останатите компјутери и кој ќе контролира како податоците се делат во мрежата. Ова е практично за поврзување на помал број на компјутери, најчесто во домашни услови, каде секој компјутер работи како независна *работна станица* која чува податоци на сопствен хард диск, но податоците може и да ги дели со сите останати компјутери во мрежата. Корисникот на секој компјутер одлучува кои податоци од неговиот компјутер можат да се делат во мрежата. Мрежи од овој вид се нарекуваат и *работни групи* (Work Group). Софтверот за мрежи со рамноправни компјутери е вграден во поголемиот дел на модерните оперативни системи, како што се Windows и Mac OS.
- мрежи базирани на сервери (**клиент-сервер архитектура**) - Кај овие мрежи се користат **сервери** – компјутер кој ги опслужува сите други компјутери кои имаат улога на клиенти. Клиентите обично се активни корисници кои праќаат барања и чекаат додека тие не се исполнат. Серверот ги исполнува барањата и ги праќа назад до корисникот. Сервер може да биде било кој компјутер, но тоа се обично моќни машини со добри конфигурации и карактеристики од причина што тие во исто време треба да опслужат многу клиенти и целата комуникација се одвива преку него. Клиентите со серверот се поврзани преку локална или регионална компјутерска мрежа.

Клиент-сервер мрежите покрај основниот оперативен систем бараат и додатен мрежен оперативен систем.

За да може уредите да се вмрежат потребно е да поседуваат **мрежна картичка**. Тоа е дел кој го поврзува уредот во локалната мрежа. Улогата на мрежната картичка е да претвора дигиталните сигнали од компјутерот во сигнал погоден за пренос преку мрежата и обратно. Тоа е електронска картичка која се вградува во компјутерот и на која има приклучни точки (порти) на кои можат да се прикачи мрежниот кабел. Мрежната картичка често се нарекува и NIC (Network Interface Card), мрежен интерфејс или мрежен адаптер, прикажан на слика 1.28. Денес етернет стандардот (Ethernet - IEEE802.3) е најраспространет за вмрежување на IP уредите, а типот на самиот конектор на мрежната картичка е од типот RJ45 со осум пина и соодветен за FTP или UTP бакарни кабли со впредени парици.



Слика 1.28.

Постојат и безжични мрежни картички (модули) кои наместо порти за кабли имаат антени за сигналојсепренесувапобезжиченпатдосоодветниот безжичен рутер (**access point**). Безжичните уреди работат по стандардот етернет IEEE802.11 на слободни фреквенции согласно регулативата на **АЕК** (Агенција за Електронски Комуникации) на фреквенциските подрачја во опсезите 2.4 GHz и 5 GHz, а со брзини од 54 Mbps.

Уредот кој дозволува корисниците да праќаат дигитални информации преку аналогните средства за комуникација, како што се телефонските врски се нарекува Модем. Тој врши конверзија на дигитални сигнали во аналогни сигнали (модулација) и обратно (демодулација).

Свич или **Комутатор** е уред кој има повеќе конектори на кои се поврзува по еден кабел од секој поединечен компјутер, сервер или друг мрежен уред. Се разликува од хабот по тоа што сигналот кој ќе го добие не го праќа до сите уреди туку само до уред за кој тој сигнал е наменет, прикажан на Слика 1.29. Во последно време се повеќе се употребуваат свичеви од типот **PoE** (Power

over Ethernet) со кои се овозможува напојување на поврзаните IP уреди преку самиот мрежен кабел, без користење на дополнителни напојувања од енергетската мрежа. Со ова се олеснува вмрежување на самите уреди. Но, исто така се гарантира непрекинато работење на сите уреди во случај на снемивање на електрична струја, доколку самиот свич е поврзан преку **UPS** (Uninterruptible Power Supply), што е најчесто и случај кај професионалните системи.



Слика 1.29.

Рутер или **Насочувач** е уред за насочување на податоци на нивниот пат низ мрежата до крајната дестинација. Тој овозможува повеќе локални мрежи да се поврзат помеѓу себе. Кога рутер ќе добие сигнал упатен до некој компјутер, тој сигналот понатаму го праќа до мрежата во која бараниот компјутер е поврзан. Ако не може директно да пристапи до саканата мрежа, сигналот го праќа до друг рутер кој е на патот до мрежата. Рутерите можат да бидат жичани или безжични, прикажани на слика 1.30.



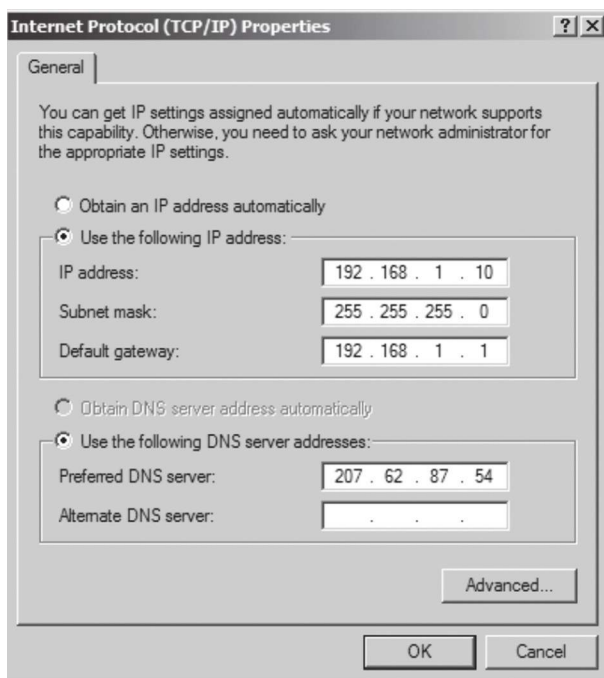
Слика 1.30.

При жичаното поврзување се користат мрежни кабли. Постојат три вида на мрежни кабли: кабли со вплетени парици (twisted pair), коаксијални кабли и оптички кабли. Кабловските врски овозможуваат најголема безбедност и најголема брзина на пренос.

Брзината на пренос се мери со бројот на пренесени битови во секунда (bps – bit per second) или со поголемите единици Kbps, Mbps, Gbps итн. Согласно денешните стандарди за етернет вмрежување се користат брзини од: 100 Mbps (Fast Ethernet) и 1 Gbps (гигабитен етернет), а за поврзувања во големи мрежи помеѓу главните точки веќе се употребува и 10 Gbps.

По остварувањето на физичкото поврзување, потребно е на уредот да се исконфигурираат одредени мрежни параметри: IP адреса, Маска на подмрежа (Subnet mask), IP адреса на Default Gateway, DNS (Domain Name System). Овие мрежи се со статички зададени мрежни параметри. Постојат и типови на мрежи кај кои мрежните параметри се добиваат динамички од самата мрежа. На слика 1.31 се прикажани основните мрежни подесувања на компјутерите. Слични подесувања се неопходни да се направат и при вмрежување на други IP уреди, како што се: камери, телефони, контролери идр.

Компјутерите и другите мрежни уреди ги разбираат само IP адресите. Луѓето пак, полесно ги разбираат и памтат имињата, како што е на пример: *google.com* или *aleksandarstojanov@yahoo.com*. Затоа, се користат DNS сервери кои ги преведуваат имињата што ги избираат луѓето, во соодветни IP адреси разбирливи компјутерите.



Слика 1.31.

Firewall – „Огнен ѕид“ или „Меѓумрежен премин“, е хардверски уред или софтвер кој се поставува помеѓу локална мрежа и надворешната мрежа односно приклучокот за интернет. Намената на Огнениот ѕид е да ги штити податоците во мрежата од неавторизираните корисници со блокирање и забрана на пристап според правила кои корисникот ќе ги дефинира. Со поставување на огнен ѕид помеѓу два сегмента во мрежата, можат да се контролираат правата на пристап на поедини корисници до поедини делови на мрежата.

Професионален мобилен радио систем – ТЕТРА

Институциите и службите задолжени за јавната безбедност и итните интервенции, секогаш имаат потреба од градење на професионални и сопствени радио комуникациски системи. Овие системи треба секогаш да се достапни и функционални, независно од комерцијалните телекомуникациски услуги што се нудат од страна на телекомуникациските оператори. Нивното нефункционирање значи загрозување на јавната безбедност или загуба на човечки животи.

Најраспространет стандард за вакви системи моментално во светот е ТЕТРА стандардот (TETRA – Terrestrial Trunked Radio). ТЕТРА стандардот е развиен согласно стандардите на ETSI (European Telecommunications Standard Institute). Тоа е радио комуникацискиот систем кој го користат повеќето Полициски структури во Европа, а се повеќе и на останатите континенти. Бидејќи во итни ситуации и криза се наметнува потребата за покомплексно делување на повеќе различни институции, покрај Полициските служби, ТЕТРА системот го користат и припадниците на Противпожарните служби, Итната медицинска помош, одредени делови на Царината, Центрите за справување со кризи, Службите за спасување итн.

ТЕТРА Инфраструктура

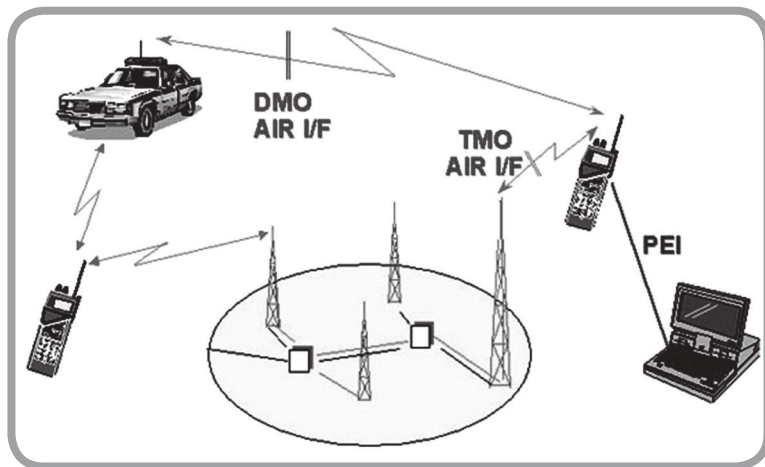
За да ТЕТРА системот работи, потребна е одредена инфраструктура. Секој ТЕТРА систем има една или повеќе централни локации каде се инсталираат централните Кмутатори (Switches), компјутерите за мониторинг и администрирање на системот и сервери за апликациите кои се користат во системот. Во делот на инфраструктурата постои мрежа од Базни станици инсталирани на високи и доминантни географски распространети локации од каде може да се направи соодветно мрежно покривање. За да базните станици можат да зрачат со својот сигнал потребно е да се инсталираат соодветни антени на столбови изградени за таа намена или ако се работи за урбана област одредено кровни конструкции на згради или други објекти.

Самите локации се одбираат според погодностите за градба и квалитетот на мрежното покривање што се очекува во фазата на радио планирање. На слика 1.32 се прикажани некои од мрежните елементи.



Слика 1.32.

Сите базни станици мора да се поврзани помеѓу себе и со централните Комутатори користејќи подземни кабли или микробранови линкови. Со вака поставената инфраструктура се обезбедува покривање со дигитален сигнал на одреден регион (регионален систем) или на целата територија на државата (национален систем). На слика 1.33 е прикажан начинот на комуникација во еден TETRA систем.



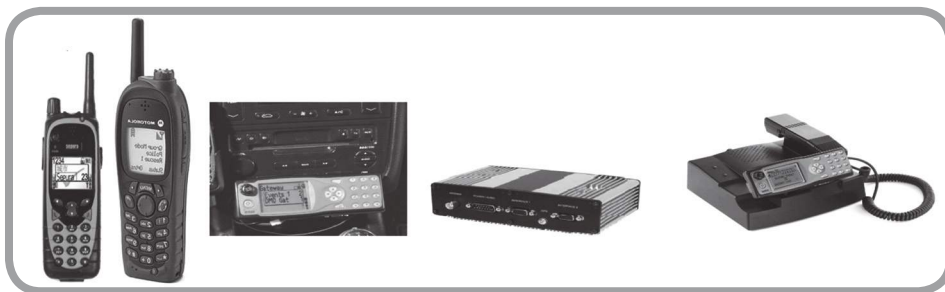
Слика 1.33.

ТЕТРА терминали

За да корисниците на ТЕТРА системот може да комуницираат помеѓу себе, потребно е да поседуваат соодветни ТЕТРА терминали или радиостаници. Со ТЕТРА терминалите се остварува безбеден пренос на говор или податоци помеѓу корисниците без оглед каде тие се наоѓаат во мрежата. Постојат три вида на ТЕТРА терминали:

- **Рачни терминали** – корисниците ги носат со себе, лесни се и практични. Имаат цветен екран и за напојување користат батерија. Постојат голем број на специјални додатоци кои ја подобруваат оперативноста на корисниците: надворешно копче РТТ (Press to Talk), дополнителни слушалици и микрофони.
- **Мобилни терминали** – се инсталираат во возилата на корисниците, користат надворешна антена и имаат добар прием на сигналот. Погодни се за поврзување на соодветни мобилни компјутери за остварување на податочна комуникација.
- **Фиксни терминали** – се инсталираат внатре во објектите за потребите на дежурните диспечери.

На слика 1.34 се прикажани различни видови на ТЕТРА терминали.



Слика 1.34.

ТЕРА безбедноси

Главна карактеристика на ТЕТРА системот покрај стабилноста во работењето, секако дека претставува безбедноста на информациите кои се пренесуваат преку него. Институциите задолжени за јавната безбедност бараат безбеден систем со кој ќе се заштитат информации од важен карактер. Затоа ТЕТРА системите користат специјално развиена енкрипција на целокупниот сообраќај. За енкрипцијата се користат криптографски алгоритми, со кои говорот и податоците во системот се шифрираат во неразбирливи сигнали за надворешниот свет. Кога

информацијата ќе пристигне на другата страна се применува обратниот процес на дешифрирање.

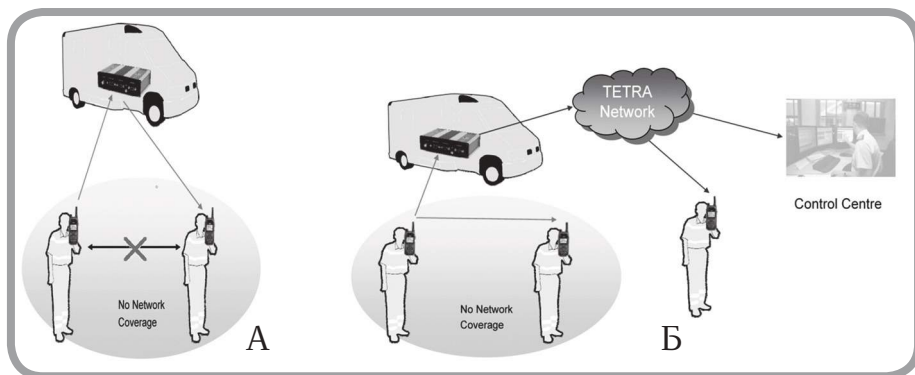
ТЕТРА функционалности

Корисниците на ТЕТРА системот комуницираат во рамките на дефинирани Кориснички групи според организациската припадност или територијалната припадност. Во рамките на корисничката група, основниот начин на комуникација е Групниот повик при што еден корисник зборува, а сите останати корисници на соодветната група слушаат. Доколку е потребно, корисникот со повисок приоритет може да го прекине корисникот со понизок приоритет. Во одредени ситуации доколку е потребно, може да се изврши регрупирање односно да се спојат повеќе групи заедно и по завршување на активноста, групите повторно да се разделат во нормален режим на работа.

Корисникот може да оствари и Индивидуален повик, директно кон друг корисник со избирање на неговиот број, како што е во телефонијата. Исто така корисникот на ТЕТРА терминалот има можност, доколку му е дозволено, да избере претплатник од мобилните или фиксните оператори во државата и во овој случај терминалот се однесува како мобилен апарат.

Од ТЕТРА терминалот може да се испраќаат пораки до еден или повеќе корисници т.н. SDS (Short Data Masssages) или одредени статусни пораки за состојбата на терен.

Основното функционирање на корисниците е во т.н. тетра мод ТМО (Tetra Mode Operation). Доколку некаде нема покривање од Базните станици или ситуацијата го бара тоа, може да се работи и во директен мод DMO (Direct Mode Operation). Во тој случај со едноставно користење на функциите на Рипитер (Reapeater) под А на слика 1.35 или Гејтвеј (Gateway) под Б на слика 1.35 кои ги поседуваат мобилните и фиксните ТЕТРА терминали, може да се оствари покриеност и на овие области. Користењето на овие функции е прикажана на сликата.



Слика 1.35.

TETRA апликаци

Работата на Командно-Контролните Центри е незамислива без користење на соодветни апликации во нивното секојдневно работење. Некои од овие апликации се директно поврзани со TETRA системот. Одговорните во овие центри мора секогаш да имаат квалитетни и точни информации од терен, врз основа на што треба да носат брзи и исправни одлуки.



Слика 1.36.

Апликации кои редовно се користат во TETRA системите се:

- **Диспечерска апликација** – работи на компјутерска работна станица со специјални додатоци за РТТ, микрофон и слушалици. Се користи за говорна комуникација со силите на терен, управување со корисничките групи и нивно регрупирање. Исто така може да праќа пораки со инструкции до сите корисници или некој поединечен корисник.

- **AVL апликација** – (Automatic Vehicle Location) работи на компјутерска работна станица на која може да се лоцираат поединечните корисници на географска мапа. Секој ТЕТРА терминал има вграден **GPS** (Global Positioning System), кој праќа податоци со географски координати до централен сервер. Со овие податоци дежурниот оператор знае секогаш кој од корисниците е најблиску до местото на настанот, може да ги разликува корисниците во движење со возило или патрола без возило и полесно да ги пренасочува и координира силите на терен.

КОРИСТЕНА ЛИТЕРАТУРА:

1. Миодраг Раноевиќ, Основи електротехнике, Грачевинска књига, Београд, 1975
2. Емилија Џундева, Комуникациона техника, Просветно дело, Скопје, 2001
3. Мирослав Дукиќ, Принципи телекомуникација, Академска мисао, Београд, 2008
4. Ристо К. Ачковски, Надземни и кабелски водови, (предавање), Скопје, 2012г.
5. Ристо К. Ачковски, “Заземјувачи и заземјувачки системи во електроенергетските мрежи“, (второ, дополнето и проширено издание), Скопје, 2008г.
6. Ристо К. Ачковски, високонапонски мрежи и системи, Скопје, 1995г.
7. Директива бр. 2001/45/ЕЗ на Европскиот парламент и на Советот од 27 јуни 2001 година за дополнување на Директивата бр. 89/655/ЕЕЗ на Советот за минимум безбедносни и здравствени услови при употребата на работна опрема од страна на работниците на работното место (втора поединечна директива во рамките на значењето на член 16(1) од Директивата бр. 89/391/ЕЕЗ) (Текст со важност за ЕЕО)
8. Правилник за техничките нормативи за електрични инсталации за низок напон (службен весник)
9. Коаксијален кабел, http://probaa.weebly.com/km.html#LinkTarget_2520
10. Оптички кабел, http://probaa.weebly.com/km.html#LinkTarget_2520
11. Верица Васиљевиќ, Е-предавања дигиталне телекомуникације, 2011

ТЕОРЕТСКИ ДЕЛ

Видови на системи за техничко обезбедување

-
- | | | |
|------|--|-----|
| 2.1. | Видови системи за техничко обезбедување | 69 |
| 2.2. | Системи за детекција и дојава на најрајник, кражба, напад и љаника | 80 |
| 2.3. | Системи за детекција, дојава и џасење на љожар | 88 |
| 2.4. | Системи за детекција и дојава на вода, љоксични џасови и љечен нафљен џас (љлин) | 98 |
| 2.5. | Системи за видео надзор CCTV | 103 |
| 2.6. | Системи за контрола на љрисљай | 121 |
| 2.7. | Инљеѓрирани системи | 126 |
| 2.8. | Мониторинѓ ценљри | 130 |



2.1. ВИДОВИ СИСТЕМИ ЗА ТЕХНИЧКО ОБЕЗБЕДУВАЊЕ

Развојот на технологијата, информатиката и телекомуникациските услуги, како и зголемувањето на стапката на криминитетот, доведуваат до паралелен развој и на начинот на обезбедување на животите на луѓето, информациите како и материјалните добра. Се повеќе во последно време традиционалното физичко обезбедување се заменува со понов, посовршен пристап во обезбедување на лица, информации и материјални добра со таканаречено техничко обезбедување.

Техничкото обезбедување во никој случај не е 100 % замена на физичкото обезбедување, туку претставува алатка на физичкото обезбедување преку која се добива дополнителен инструмент за зголемување на мерките за заштита и служи единствено за:

- Навремено добивање на информации за одредени активности
- Архивирање на настани и нивна анализа
- Растеретеност на физичкото обезбедување
- Заштита на животите и здравјето на физичкото обезбедување
- Намалување на цената на обезбедувањето
- Одбивање на случајни напади

За остварување на квалитетно обезбедување покрај техничкото обезбедување потребо е и физичко обезбедување кое има задача да изврши отстранување на ризикот по објектот¹, лицето или материјалното добро.

Според статистиката, со вградување на системите за техничкото обезбедување, штетата е намалена за 4,5 пати.

Сигурна заштита со техничко обезбедување се постигнува со правилен избор на техничката опрема, адекватно распоредување на елементите од техничкото обезбедување, адекватно монтирање како и нејзино правилно користење и одржување (слика 2.1).

Во видови на техничко обезбедување спаѓаат:

- Системи за детекција и дојава на натрапник, кражба, напад и паника
- Системи за детекција, дојава и гасење на пожар
- Системи за детекција и дојава на вода, токсични гасови и течен

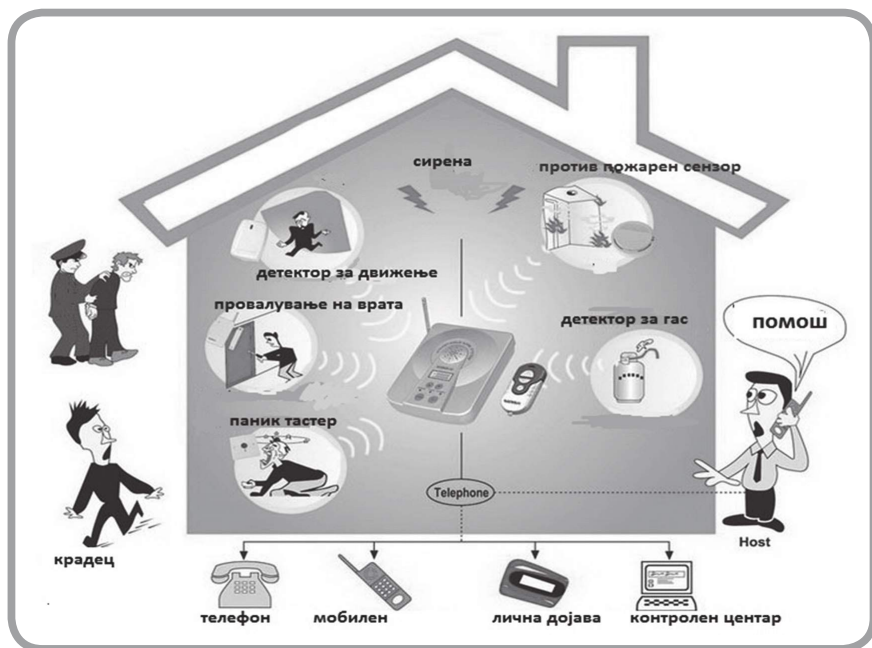
¹ Објект - под објект се подразбира:
Лице, Простории, дом, канцеларии, магацини, Отворен простор, Предмет, финансиски средства, информации и се она кое е предмет на обезбедување.

нафтен гас (плин)

- Системи за видео надзор
- Интегрирани системи и
- Мониторинг центри

Секој од овие системи се состои од повеќе делови:

- Периферни делови (сензор, камера)
- Централен дел (софтвер и хардвер за менаџирање на информации)
- Медиум за пренос на информации



Слика 2.37. Видови на системи за техничко обезбедување

Периферен дел

Периферниот дел на овие системи всушност претставуваат очите и ушите на системот. Нивна задача е да благовремено извршат детектирање на настанатите промени и согласно процедурите ја достави информацијата до централниот дел или друго дефинирано место.

Периферниот дел се состои од:

- Сензори
- Камери

- Паник копчиња
- Уреди за тревожење и алармирање

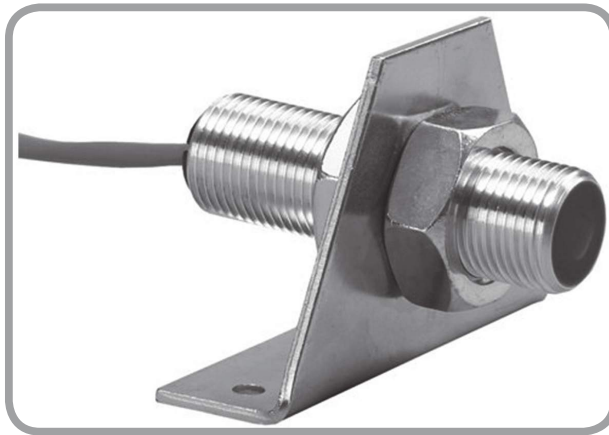
Сензори

Сензорот (детектор) претставува конвертор кој што ја мери физичка големина и ја претвара во сигнал кој може да се прочита и анализира од страна на инструмент или одреден софтвер.

Според начинот на функционирање, видот на изработка и намената, постојат повеќе видови на сензори.

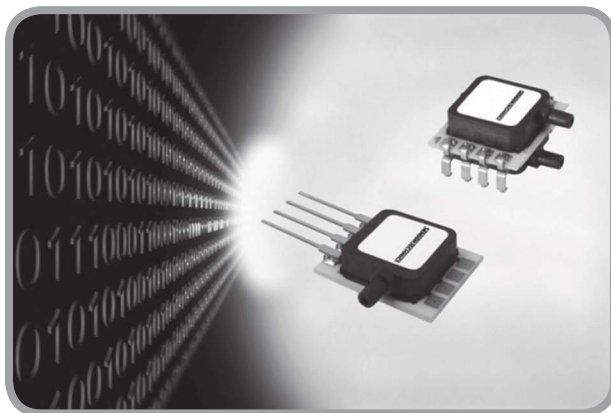
1. Според видот на сигналот кој го испраќа:

- *Аналожни сензори (слика 2.2.)* - претставуваат вид на сензори кои испраќаат аналогни информации до централниот дел. Овие информации всушност претставуваат променливи електрични напони кои се генерираат од страна на сензорот и се линеарни со нивото на надразнувањето на сензорот. Ваков тип на сензори претежно се користат за места каде е потребно да се врши мерење на одреден тип на информација (резервоари, светлина, проток)



Слика 2.38. Аналоген сензор

- *Дигитални сензори (слика 2.3.)* - претставуваат електронски или електро хемиски сензори. Специфично кај овие сензори е што информацијата и преносот на информацијата се извршува дигитално. За разлика од аналогните сензори оваа информација подлежи на дополнителна анализа со што се зголемува опсегот на искористеност и истата најчесто се користи за аналитички мерења.



Слика 2.39. Дигитален сензор

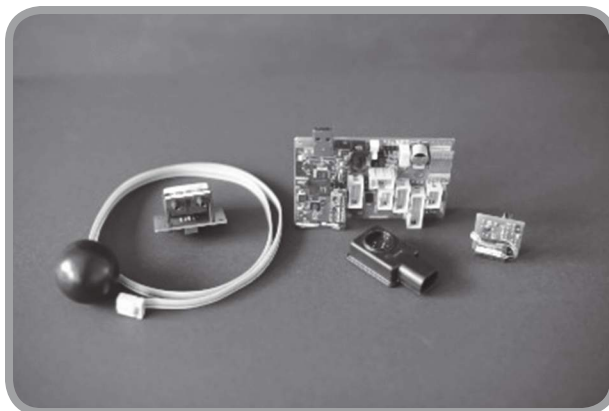
2. Според местото каде што се монтираат може да се поделат на:

- *Сензори за надворешна употреба* - истите се користат во надворешни услови и се изработени од материјали кои се отпорни на надворешни атмосферски влијанија и истите се специфицирани со стандард ИП 56 (слика 2.4.),



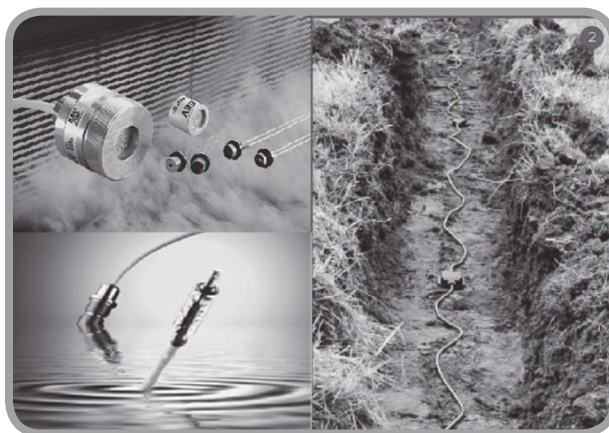
Слика 2.40. Сензор за надворешна употреба монтиран на ограда

- *Сензори за внатрешна употреба* - се користат во затворени простории или простори заштитени од атмосферски влијанија, каде според условите не побаруваат повисок степен на заштита на сензорот (Слика 2.5.).



Слика 2.41. **Слика 5.** Внатрешен сензор

- *Сензори за употреба во специјални услови* (под земја, вода, специфични гасови и течности) - ова се специфичен тип на сензор кој се дефинира со висока издржливост од атмосферски влијанија, издржливост на материји со висока точка на нагризување на метал и легури, како и водоотпорност. Овие сензори се користат за екстремни услови како на пример резервоари со гориво, киселини, отровни материји како и обезбедување на периметар под вода (Слика 2.6.).



Слика 2.42. Видови на сензори во специфични услови

3. Според намената:

- Сензори за регистрирање на движење
- Сензори за регистрирање на потрес,
- Сензори за мерење на притисок,
- Сензори за регистрирање на светлина,
- Сензори за мерење на температура
- Сензори за мерење на проток
- Сензори за регистрирање влажност, опасни материи и т.н.

Камери

Камерите слободно може да се наречат дигитални сензори бидејќи во системот на обезбедување функционираат како периферни делови. Основна намена на камерите во овие системи е да го зголемат визуелното покривање на објектот што се покрива (слика 2.7).

Архивираниот материјал добиен од камерите, дополнително подлежи на видео анализа преку која може да се откријат сторителите, или да се добијат информации за евентуални слабости во системот на обезбедување.



Слика 2.43. Камери за видео надзор

Паник копчиња

При релизација на системите за обезбедување кога се работи за безбедноста на објектот кој што се обезбедува како и кога одреден објект се заштитува со помала жива сила, потребно е инсталирање на ваков уред кој има за задача да со негово активирање иницира алармен сигнал до службите за физичко обезбедување, кои согласно процедурите ќе превземат дејства за заштита на објектот (слика 2.8.).



Слика 2.44. Паник копче

Уреди за шревожење и алармирање

Овие уреди се наменети да извршат алармирање на физичкото обезбедување преку светлосни или звучни сигнали (слика 2.9.). Покрај навременото алармирање на физичкото обезбедување намената им е да предизвикаат шок и одбивање на намерата на натрапникот. Својата цел ја остваруваат преку активирање на разни звучни (аларми, звучници) и светлосни системи (рефлектори) кои даваат до знаење дека е откриена намерата на натрапникот а воедно и го запознава целото физичко обезбедување и околината дека објектот е во фаза на аларм. Овие уреди најчесто се користат на објекти кои се блиску до населени места каде вниманието на околните жители е доволен да го предомисли натрапникот во реализација на својата цел.



Слика 2.45. Уреди за тревожење и алармирање

Централна единица

Ако сензорите во овој систем претставуваат очи и уши, тогаш мозокот на целиот систем е Централната единица.

Таа има за задача да собира информации добиени од периферните уреди, и потоа во зависност од информациите да изврши низа на операции кои претходно се дефинирани од страна на корисниците и да доставува команди до уредите за тревожење и алармирање како и преку разнит евидови на пренос на информации врши информирање за настанатата состојба на објектот кој се обезбедува.

Централна единица за да може правилно да ја извршува својата намена потребно е:

- Навремено да прибира информации од периферните уреди,
- Правилно интерпретирање на сигналите
- Навремено известување за настанатите ситуации
- Непрекинатост во работата
- Заштита од несакано или намерно деактивирање
- Потребно е да врши архивирање на сите настани
- Потребно е да има имплементирани стандардни оперативни процедури со што би се намалил ризикот од човечка грешка.

Медиуми за пренос на информации

Со развојот на телекомуникации во голема мера се олеснува преносот на информации од системите за техничко обезбедување до крајните

корисници. Покрај брзината на пренос на информации се зголемува и количината на информации кои можат да се пренесат на оддалечено место. Побарувањата на потрошувачите од ден на ден се повеќе расте. Од потребата и тие да бидат благовремено информирани за безбедноста на објектите во последно време се повеќе се користи мрежата на мобилните оператори во Република Македонија (дојави на мобилен, електронска пошта, увид во видео надзорот на објектот преку интернет и.т.н).

Секој систем преку адекватен модул може да се подеси да испраќа информации преку:

- Жичен сообраќај и (*wire traffic- LAN, PSTN, signal cable, optic*)
- Безжичен сообраќај (*wireless traffic- Microwave, GSM*)

Жичен сообраќај

Самото име на овој вид на пренос на информации кажува дека се работи за пренос на информации преку кабел. Ваков вид на пренос на информации е стабилен, брз и во зависност од инфраструктурата истиот е заштитен. Најчеста инфраструктура за пренос на податоци во нашата држава е инфраструктурата на телекомуникациските провајдери, доколку не се има сопствена инфраструктура.

За да може системот да комуницира преку еден од овие медиуми постојат уреди т.к.н модули кои преку соодветни порти и протоколи се поврзани со централните единици од една страна и жичните врски од друга страна. Постојат повеќе видови на модули и тоа:

- *TCP/IP модул* - претставува уред за трансформација на сигналот од централната единица (serial) во етернет, кој преку интернет се пренесува до бараното место (слика 2.10.).



Слика 2.46. TCP/IP модул

- *PSTN dialer* – претставува уред за трансформација и пренос на сигналот од централната единица користејќи ги комерцијалните линии од телеком операторите (слика 2.11.).



Слика 2.47. PSTN dialer

- *Fiber media converter* - претставува уред за трансформација на сигналот од централната единица (serial) во Ethernet, Fast Ethernet, Gigabit Ethernet, E1, како и конекции за разни видови на каблирања: коаксиален кабел, ФТП/УТП, паричен систем на кабел и останато (слика 2.12.). Во принцип работи на ист начин како TCP/IP convertor, со тоа што овој начин на комуникација нуди поголеми можности за пренос на информации. Со користење на оптичкото влакно како медиум за пренос на информации постигнато е да може да се пренесуваат големи податоци на далечини за многу кратко време.



Слика 2.48. Оптички конвертор

Без жичен сообраќај

Овој вид на сообраќај се користи на објекти каде не е во можност да се искористи или ја нема жичната инфраструктура. За разлика од жичните врски овој вид на конекција е многу подложен на попречување како и капацитетот на информацијата која се пренесува. Во најголем број случаи овој вид на пренос се користи како резервна (back up) линија на системите, за да се реализира начелот за непрекинатост во работата.

За пренос на информациите се користат следните уреди:

- *Microwave линкови* - се карактеризираат со голем капацитет, брзина но истите се многу подложни на атмосферски влијанија и лимитирани се во однос на поставувањето т.е потребна е оптичка видливост за нивно поставување (слика 2.13.),



Слика 2.49. Microwave линкови

- *GSM (2G, 3G, 4G) модули* - преку овој уред се користи мрежата на комерцијалните мобилни провајдери за пренос на информациите (слика 2.14.). За разлика од линковското решение ова е постабилно но значително е помал капацитетот и брзината на пренос на информациите. Друга слаба страна на овој систем се финансиските трошоци кои произлегуваат од користење на услугите од мобилните провајдери, како и неможноста за загарантиран пренос во секое време (оптовареност на мрежа за време на празници, вонредни ситуации). GSM модулот како и останатите модули е тип на модем кој добиената информација ја препраќа преку GSM мрежата до саканата дестинација. Има можност информацијата да ја праќа на друг модем поврзан во мониторинг центарот или да се препраќа преку интернет конекцијата.



Слика 2.50. GSM модул

2.2. СИСТЕМИ ЗА ДЕТЕКЦИЈА И ДОЈАВА НА НАТРАПНИК, КРАЖБА, НАПАД И ПАНИКА

Стапката на криминалитет на нашето поднебје во последните години е во константен пораст. Криминалците кои вршат тешки кражби и разбојништва се повеќе, паралелно со нив и ситниот криминал се зголемува, особено кражбите по домовите, колите и останатите објекти се позачестени.

Штетите кои може да настанат како последица на провала и напад се огромни. Покрај финансиските штети кои во некои случаи неможат да се обештетат (индустриски информации, лични добра и информации) може да дојде и до загуба на човечки живот.

За да се изведе квалитетно физичко обезбедување и да се заштитат материјалните добра и животите на еден објект, повлекува голем број на жива сила а со тоа и финасиски средства, која би имала задача непрестајно да врши патролирање и обезбедување на просторот. Во многу случаи ваков вид на обезбедување не ја исполнува задачата пред се поради факторот човек, кој за разлика од техниката има многу променлив пристап кон работата (поткуп, замор, лични и професионални проблеми, неадекватна обука и останато).

При ваков вид на криминал, една од најважните задачи на обезбедувањето е да се детектира заканата во најраната фаза, т.е во:

1. Фаза на подготовка
2. Фаза на извршување

Фазата на подготовка претставува процес во кој криминалецот врши набљудување на објектот кој сака да го нападне. Набљудувањето може да биде непосредно пред нападот (специфично за ситни криминалци и аматери) или предходно поопширно набљудување (тежок криминал). Целта во оваа фаза е да се воочат ваков тип на активности и да се подготви обезбедувањето за превземање на дејства како и отстранување на сомнителните лица од непосредната близина на објектот кој се обезбедува, со што би им се дало на знаење на лицата дека се приметени. Со самото дејствие голем процент од опасноста кон објектот се намалува т.е сведува на нула.

Фазата на извршување претставува процес во кој лицето врши навлегување во објектот или периметарот кој се обезбедува. Целта во оваа фаза е да се детектира лицето уште во време на поминување на првата линија на заштита (ограда), или при влегување во објектот со обивање на врата, кршење прозор и друг тип на насилно влегување. Со самото навремено детектирање може успешно да се реализира системот на обезбедување и да се заштити објектот.

За да може квалитетно да се изведе процесот на физичко обезбедување

на одреден објект како и заштита на животото и здравјето на луѓето, во денешно време се воведува и систем за техничко обезбедување т.е Систем за детекција и дојава на натрапник, кражба напад и паника.

Системот претставува сложен склоп на повеќе подсистеми кои првенствено имаат задача да детектираат појави (претходно дефинирани) и користејќи различни видови на медиуми за пренос на информации, навремено ја достави информацијата на потребното место, а со тоа и да изврши навремено информирање и алармирање на персоналот за физичко обезбедување, кое согласно утврдените постапки ќе може навремено да превземе соодветни дејствија.

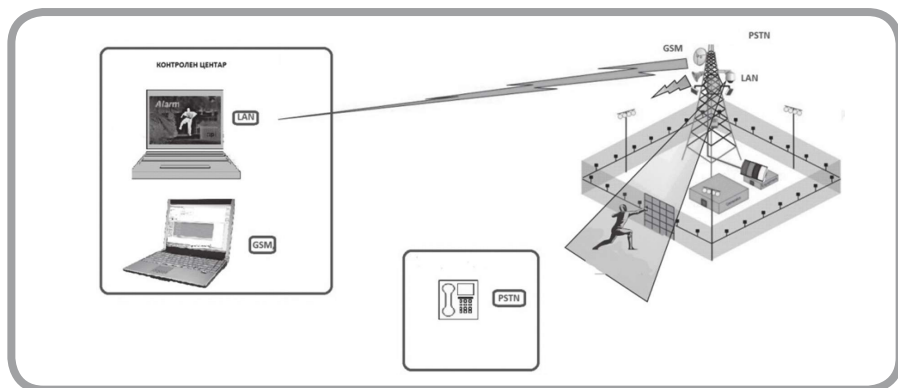
Системот може да се подели во два подсистеми, и тоа:

1. Систем за детекција и дојава на натрапник, провала и кражба и
2. Систем за дојава на напад, паника

Систем за детекција и дојава на натрапник, провала и кражба

Системот за детекција и дојава на натрапник, провала и кражба претставува систем за техничко обезбедување кој има за задача навремено и точно да врши детектирање и дојава на алармни состојби на објектот кој се обезбедува (слика 2.15.).

Детектирањето на овие појави, системот ги врши преку периферните уреди кои се поставени во зависност од планот на обезбедување. Главна цел на сензорите е секоја физичка побуда- стимулација да ја претворат во електричен сигнал и преку разни медиуми ја испратат информација до централната единица.



Слика 2.51. Приказ на систем за заштита од натрапник, кражба на базна станица

При изработка на ваков систем, потребно е да се знаат неколку параметри:

- *Карактеристики на објектот што треба да се обезбедува* - Карактеристиките се важна почетна точка во подготовката. Со правилно профилирање на објектот што се обезбедува, неговата закана и целта што треба да се постигне може да се изготви квалитетно техничко обезбедување, без да се предимензионира или осиромаша системот.
- *Опасноста од која треба да се заштити* - правилна анализа и проценка на ризикот кон објектот доведува и до правилна поставеност на самите системи за заштита. Би било непотребно да се оптоварува системот за заштита со некои делови за кои не постои реална опасност (пр. поставување на безбедносна ограда а објектот е дефиниран од отворен карактер, контролиран пристап во трговски центри и.т.н),
- *Реална проценка на вредноста на објектот што се обезбедува* - финансиската вредност на системот за заштита не треба да е поголема од вредноста на објектот што се заштитува,
- *Време на реакција на физичкото обезбедување по дојава на аларм* - за оддалечени локации каде времето за интервенција на физичкото обезбедување е големо потребно е да се дефинира системот така што би информирал уште во најраната фаза на правалување, со дополнителни мерки за задржување на натрапникот.

Системот за детекција и дојава на натрапник и кражба се состои од:

- Централен систем- или PCU² мозокот на овој систем, кој има задача да ги прибира информациите од сензорите и истите да ги анализира. Во најчест случај тој претставува склоп од компјутерски елементи, спакувани во заштитни куќиште, опремено со резервно напојување. На него има дополнителна заштита изведена со tamper protection која има задача да извести кога има насилно оштетување или демонтирање на уредот.
- Сензори- уреди кои го детектираат натрапникот. Има различни видови за овој систем како на пример:
 - **Пасивни инфракцрвени детектори** - најчести сензори за детектирање на движење. Најчесто се користат во домаќинството и малите компании, кога е потребно низок степен на заштита. Во суштина овој вид на сензори не детектира движење туку работи на принцип на промена на температурата кој ја мери преку инфрацрвен зрак кој не е видлив за човечкото око. Кога

² PCU – premises control unit

натрапникот ќе помине преку овој зрак автоматски се зголеми температурата што претставува и сигнал овој сензор да ја алармира централната единица.

- **Ултра звучни детектори** - сензори за детектирање на движење. Работат на принцип на емитување на ултразвук кој не е опасен и чуен за човечкото уво. Кога натрапникот ќе помине преку овој бран тој ја менува фреквенцијата со што го става сензорот во алармна состојба.
- **Микробранов детектор** - сензор за детектирање на движење и се користи за покривање на поголеми површини. Работи на принцип на емитување и примање на микро бранови. Кога ќе дојде до деформација на емитувачкиот бран тогаш сензорот преоѓа во алармна состојба. Поради големиот број на грешки кои се јавуваат од ваков тип на сензор препорачливо е да се комбинираат со инфраред сензори. За отворени простори се користи и таканаречена микро бранова бариера која функционира на ист начин како и сензорот.
- **Сензори за скршено стакло** - се монтираат на самото стакло или во непосредна близина. Работат на принцип на преслушување на звук од скршено стакло (акустични) или сеизмички кои се активираат од фреквенцијата на потресот кој се добива при кршење на стаклото и истите се монтираат директно на стаклото.
- **Вибрациони сензори** - се монтираат на заштитните огради, подземни инсталции, преградни зидови. Работат на принцип на придвижување на многу осетлива активна супстанца вградена во нив која. Со самото придвижување генерира електричен импулс кој го активира алармот. Овие сензори во денешно време имаат голем дијапазон на употреба, поготово поновите генерации кај кои степенот на чувствителност се подесува а и самите сензори се адресабилни, со што се овозможува изградба на комплексни системи за заштита.
- **Оптички кабел** - понова генерација на сензори за детекција на движење која се користи за подземно периметарско обезбедување. Работи на принцип на мерење на количествот на светлина која поминува низ него. Кога кабелот ќе се нагазне се менува и количествот на светлина со што се активира и алармот.
- **Уреди за известување и шревожење** - претставуваат уреди кои имаат задача да извршат известување, алармирање и првично одбивање на опасноста кон објектот што се обезбедува. Најчесто тоа се сирени, трепкачки светла (слика 2.16.), панични копчиња.



Слика 2.52. Уред за известување и тревожење

- *Тасџаџура* - претставуваат интерфејс за комуникација помеѓу човек и системот. Наменети за системско работење со системот, негово активирање/ деактивирање (слика 2.17).



Слика 2.53. Тастатура

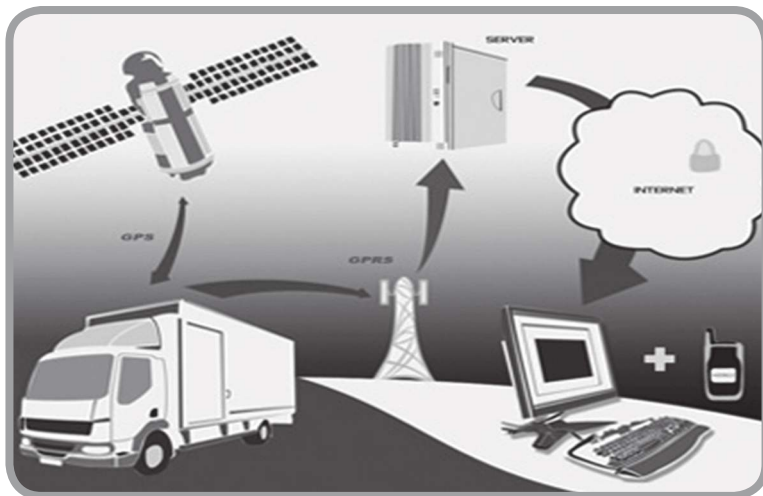
- *Каблирање* - систем од разни видови на конекции кои ги користи системот за негово поврзување со своите елементи (слика 2.18.). Се користат разни видови на кабли (ФТП/УТП, сигнален кабел, коаксиален кабел, напонски кабел и останат), во зависност од компонентите кои треба да се поврзат.



Слика 2.54. Видови на кабли кои се користат во алармните системи

Важно е да се напомене дека овој систем секогаш се комбинира со системот за видео надзор со цел да се зголемат мерките на безбедност.

Во поново време за обезбедување на објекти во движење (возила, транспорт на материјални добра) се користи и ГПС (global positioning system) системот, кој има задача да врши позиционирање на објектот кој се обезбедува а со тоа и добивање на реална слика за положбата на објектот. ГПС системот е базиран на сателитска технологија и работи на принцип на сателитско позиционирање на ГПС приемникот. Карактеристично е што работи во сите временски услови и во зависност од бројот на сателити кои го позиционираат точноста може да му варира до +/- 2 метри. Како што рековме наоѓа голема примена во обезбедувањето на возила, транспорт на пари, опасни материи, но се повеќе зема замав и во комерцијалното работење т.е увид во локација на возен парк. ГПС системот преку адекватен софтвер може да креира и архива на активности, со што може дополнително да се анализира рутата и брзината на движење на објектот што се обезбедува. ГПС системот и неговото користење е слободно.



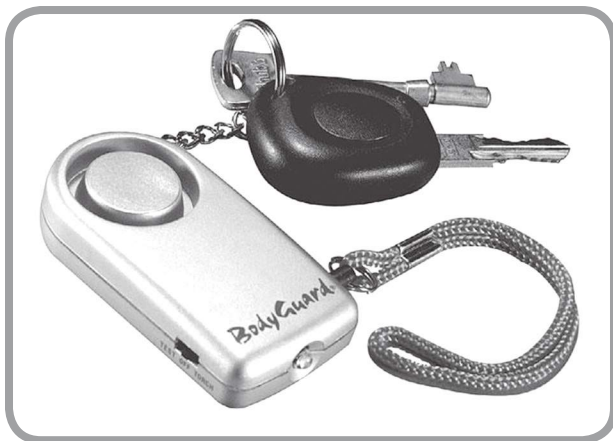
Слика 2.55. Графички приказ на ГПС системот

Систем за дојава на напад и паника

Една од причината зошто е направена посебна поделба на овие системи е тоа што системот за детекција и дојава на напад и паника покрај тоа што е дел од системот за детекција на натрапник, провала и кражба може самостојно да делува, поготово за заштита на личности и истиот може да биде мобилен т.е да не се врзува за некоја инфраструктура.

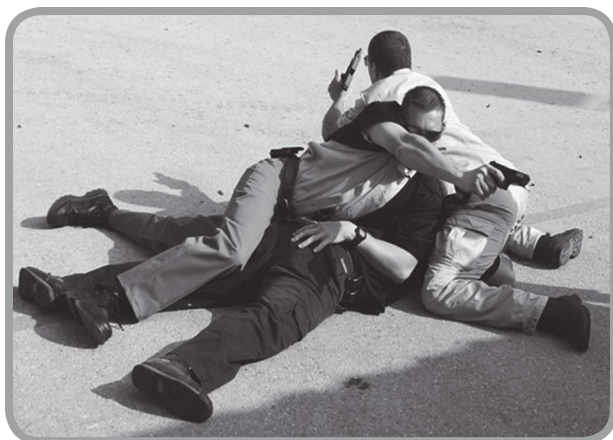
Модерните времиња, професиите на луѓето како и нивниот приватен живот често пати се ставени во опасност. Поради своите професии и примањата многу луѓе стануваат цел на напади на криминални структури. Тие не треба да бидат заштитени само во своите домови, канцеларии или автомобили. Најчесто место за напад е кога овие лица се надвор од безбедносното подрачје или кога покрај нив не е присутно физичкото обезбедување (тоалет). Еден од системите кои се користи во овие ситуации е и системот за дојава на напад и паника.

Тоа претставува преносен уред кој има за задача да со пристискање на копче (техничката изведба на овие уреди е изведена така да тие не бидат видливи или упадливи а да бидат секогаш при рака на објектот кој се обезбедува- слика 2.20.) благовремено да биде известен персоналот за физичко обезбедување, за настанатата опасност, со што физичкото обезбедување навремено би превзело мерки за отстранување на опасноста од објектот или дислокација на објектот на безбедна локација (слика 2.21.).



Слика 2.56. Панично копче изведено како приврзок

Преносот на овие информации најчесто се врши преку ГСМ мрежата. Физичкото обезбедување во себе носат приемници кои добиваат алармни информации од страна на предавателот (копче за напад/паника).



Слика 2.57. Интервенција на физичкото обезбедување

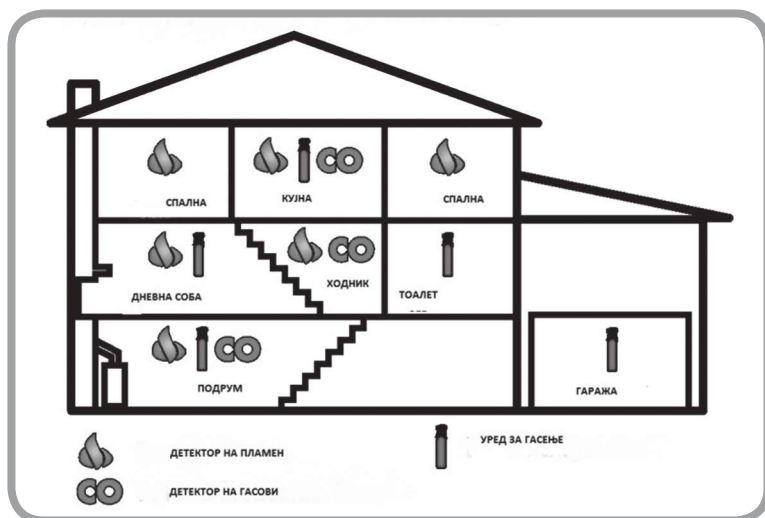
2.3. СИСТЕМИ ЗА ДЕТЕКЦИЈА, ДОЈАВА И ГАСЕЊЕ НА ПОЖАР

Покрај опасноста од физички напад на објектот што се обезбедува, постојат и други видови на опасности. Една од нив е опасноста од пожар.

Пожарот претставува брза оксидација на материјалот во екзотермички процес на согорување при што се ослободува голема количина на топлина, светлина, согорувачки гасови и останати пропратни продукти. Пожарот по својата природа може да предизвика големи материјални штети по објектот кој се обезбедува како и загуба на човечки животи.

Општо познато е дека пожарот најлесно се гаси и остава најмали последици, доколку се открие и интервенира во неговата најрана фаза на започнување. Ако се погледне дефиницијата на пожарот и неговите пропратни елементи може лесно да се заклучи и каков ќе биде системот за детекција, дојава и гасење на пожар.

За да може навремено да се открие и изгаси, се користи систем за детекција дојава и гасење на пожари. Системот за детекција дојава и гасење на пожари во денешно време наоѓа широка примена во заштитата на објектите. Денеска речиси нема јавна установа, економски објект, па дури и објекти за домување каде не е инсталиран ваков систем. Објектите кои се наменети и вршат дејност каде се собира или гравитира голем број на луѓе (трговски центри, театри, кино, спорстки сали и.т.н) се обврзани и согласно законот да спроведат мерки за заштита од пожари. Една од тие мерки е и поставувањето на систем за детекција дојава и гасење на пожари.



Слика 2.58. Приказ на распоред на уреди за заштита од пожар

Како што веќе спомнавме пожарот покрај пламен се манифестира и со придружни појави, како што се чад, светлина, висока температура, гасови (јаглен диоксид, јаглен моноксид и др.). Со пронајдокот на детекторите (сензори) за откривање на овие придружни појави на пожарот и со нивно поврзување во еден централен систем за следење на нивните дојави се осмислиле и првите системи за откривање на пожари. Системот мора да има резервно напојување, а електричната ПП инсталација мора да е посебно издвоена и заштитена.

Начелно принципот на работа на системот за детекција дојава и гасење на пожари претставува детекција на овие придружни појави на пожарот. Тоа се врши преку периферните делови на овој систем а тоа се сензорите.

Во зависност од техничката изведба системите за детекција, јавување и гасење на пожари се делат на:

- *класични* - постар тип на системи каде се користат аналогни сензори. Карактеристично за нив е тоа што не може точно да се одреди сензорот кој е во алармна состојба туку само зоната (серија на сензори врзани сервиски еден по друг),
- *адресибилни* - современ тип на системи каде точно се знае кој сензор е во состојба на аларм, кој подлежи на дополнителни анализи (секој сензор има своја адреса и секој од нив комуницира со системот и се поврзани паралелно)

Делови на системот за детекција, дојава и гасење на пожар

Системите за детекција, дојава и гасење на пожари се состојат од:

- сензори (сензор за чад, топлина, гас,)
- централа за автоматско јавување на пожар
- уреди за сигнализација
- уреди за управување на извршни функции
- индикатори
- електро инсталација за поврзување на елементи

Сензори

Сензорите се периферниот дел на овој систем. Тие имаат задача да детектираат некој од манифестациите на пожарот и благовремено добиената информација да ја пренесат до централата.

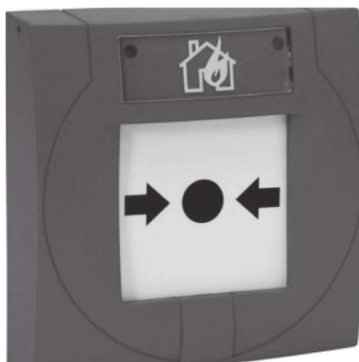
Според начинот на активирање се делат на:

- **автоматски** - детекцијата и информирањето се врши автоматски и не е потребна човечка реакција (слика 2.23.) и



Слика 2.59. Автоматски сензори

- **рачни** - каде информирањето се врши рачно т.е алармот го поттикнува човек (слика 2.24.).



Слика 2.60. Рачен јавувач кој се иницира со кршење на заштитното стакло

Според манифестацијата на пожарот што ја откриваат:

- **Јавувачи на чад (јонизациони и оптички)**
 - **Јонизационите јавувачи** се вид на автоматски сензори кои реагираат добро на ситни честички и се базираат на принципот на јонизирани молекули на воздухот во комората на јавувачот под дејство на радиоактивна материја при што кога честички

од чад ќе навлезат во комората истите се лепат на јоните и тие го успоруваат своето движење што се одразува на промена на струјата во колото. Се користат кај пожари на материјали од органско потекло (дрво, хартија) кои имаат ситни честички во чадот, или аеросоли кај течности и гасови кога истите испаруваат или истекуваат. Се поставуваат на плафон и можат да покријат површина од 20 до 80 м².

- **Оптичките јавувачи** реагираат добро на крупни честички и се базираат на принципот на пореметување на струјата што се добива од светлината што паѓа на фотокелија. Се поставуваат на плафон и можат да покријат површина од 20 до 80 м². Може да се постават паралелно (поврзани со 2 цевки) со канал за вентилација за регистрирање на чад во вентилацијата. Се користат кај пожари на PVC.
- *Термички јавувачи (термомаксимални или термодиференцијални)*
 - **Термичките јавувачи** може да реагираат на некоја максимална температура (од 63 до 120) или на промена на температура (на пр. 5 степени за 1 минута). Во себе содржат РТС или НТС елементи кои имаат својство да ја менуваат електричната отпорност при промена на температурата.
- *Светлосни (јавувачи на пламен)*
 - **Јавувачи на пламен** реагираат на промена на дел од светлосниот спектар (инфрацрвени или ултравиолетови). Се поставуваат на плафон и покриваат поголеми површини, на пример во фабрички хали каде висината на плафонот е 12 до 20 метри или на места каде брзо доаѓа до пламен (како што е магацин со запалливи течности).
- *Биметални, механички како и други видови на јавувачи.*
 - **Капиларни пневматски јавувачи** се стаклени тенки цевки чие дно е од метал кој на температура се шири и притисокот на воздухот во цевката паѓа од што произлегува и алармот. Порано се користеле за системи за гасење.

Сите претходно наведени јавувачи се автоматски и истите имаат индикатори на себе како и паралелни индикатори. Индикаторите се светлосни диоди кои кажуваат дали јавувачот е активиран, при што паралелните индикатори се поставуваат на пример на врата од просторијата каде е јавувачот со цел побрзо да се открие дека е активиран.

Централна за автоматско јавување на пожар

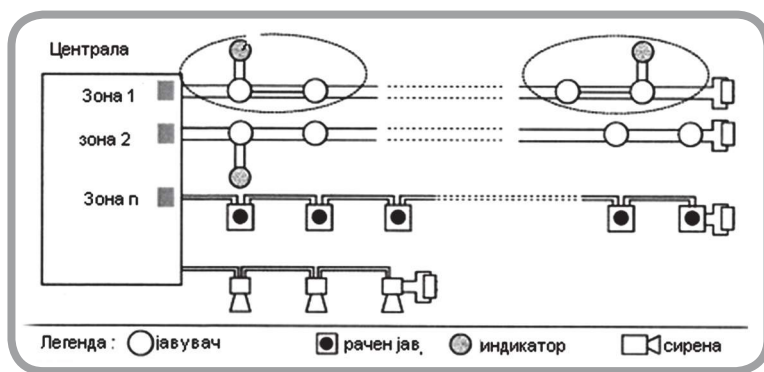
Кога сензорите ќе откријат некоја од манифестациите на пожар во истиот момент тој пренесува до централата електричен сигнал за аларм.

Централната единица врши анализа на добиените информации од сензорите, и доколку информацијата се потврди од повеќе различни сензори превзема процедури кои се дефинирани од страна на стручни екипи како на пример:

- вклучува интерната сигнализација која може да е светлосна или звучна,
- вклучува надворешна сигнализација која исто така може да е светлосна (црвено или трепкачко светло) или звучна (сирена),
- пренесува автоматска телефонска порака,
- вклучува извршни функции
 - спуштање на лифтот на приземје,
 - вклучување на систем за отчадување,
 - исклучување на систем за вентилација,
 - затворање на клапни за комплетен престанок на доток на нов воздух или
 - вклучува автоматско гасење.

Централа претставува електронски уред базиран на микропроцесорска технологија. Според технологијата на изработка тие се делат на:

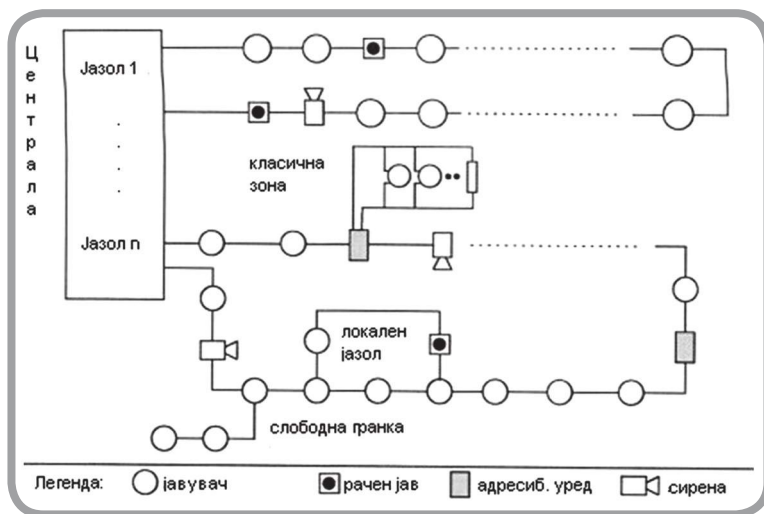
- *Класична централа* - организирани во зони и може да имаат 4 до 32 зони (зона е група на јавувачи поврзани со една линија до централата (слика 2.25.), при што јавувачите се сервиски поврзани меѓусебе), а во една зона може да има до 20 јавувачи и дојавата се базира на принципот на промена на напонот.



Слика 2.61. Изведба на класичен тип на противпожарен систем

- *Агресибилна централа* - организирани се во јазли од 1 до 16 (јазол е затворена линија која оди од централата до сензорите на тој

јазол и потоа се враќа до централата, при што сензорите меѓусебе се поврзани сериски - слика 2.26.). Во една зона може да има до 128 или 256 сензори и дојавата се базира на дигитална комуникација на централата со секој сензор (амплитудна или фреквентна модулација).



Слика 2.62. Изведба на адресибилна противпожарна централа

Карактеристично за секоја централа е различниот вид на приклучоци за нејзино програмирање и комуницирање. Стандарден приклучок за програмирање на нејзините функции преку компјутер е RS232 приклучокот, а со RS485 приклучокот се извршува комуникацијата со други центри, паралелен панел или компјутер со кориснички интерфејс како и конвертор за умрежување во некоја LAN мрежа.

Исто така централата има и уреди за извршување на функции (релиња за управна контрола на надворешни системи и уреди).

Кај големи објекти во пракса се користат повеќе центри поврзани меѓусебе и контролирани од големи паноа или компјутер со кориснички интерфејс (клиентски софтвер). Клиентскиот софтвер овозможува графички приказ на целиот објект со јакувачите, како и сите функции и контроли на централата.

Централата има LED – ови за индикација (црвени за аларм и жолти за пречки), тастери за прекин на алармот, тастери за прекин на интерната или надворешната сигнализација, тастери за ресетирање на состојбата на централата, тастери за прекин на извршни команди, дисплеј за приказ на состојби итн.



Слика 2.63. Централна единица за против пожарен систем со придружни елементи

Централната единица пред да превземе одредена активност врши проверка на информацијата од повеќе сензори. Причината за тоа е да се намали можноста за лажни дојава поради комплексните активности кои ги превземаат извршните функции. Лажните аларми се многу честа појава кај сите системи, но во овој случај при лажен аларм можни се тешки последици по објектот што се обезбедува. На пример престанок на работа на лифт во некоја висока зграда, активирање на системи за гасење во архиви, ТК и ИТ сали, канцеларии и т.н.

Лажни аларми се честа појава и можат да настанат од:

- чад од цигари
- чад од ауспух од моторни возила
- случајно притискање на тастерот од рачниот јавувач
- заварување (температура и пламен)
- светлина (имитација на пламен) од неонки, фарови, сонце

Сите овие компоненти можат негативно да влијаат на функционалноста на системот. Поради ова системите за детектирање, јавување и гасење на пожари главно имаат рачна контрола- соодветен тастер кој со притискање или по престанок на алармот централата може да се доведе во нормална состојба.

Уреди за сигнализација

Како и кај сите останати системи, потребно е алармната состојба на системот да биде визуелно и звучно прикажана. За таа цел во системите за детектирање, јавување и гасење на пожари веќе има интегрирано решение за сигнализација. Еден од најчестите уреди за сигнализација е звучната, од причина што може навремено и на поголема површина да се разгласи алармот. Покрај звучната често се користи и светлосната сигнализација која најчесто е преставена со црвени трепкави светла.

Покрај дополнителните уреди за сигнализација, централната единица има кориснички дисплеј и сигнални лампи исто како и работната станица на која се добиваат информации за состојбата на системот.

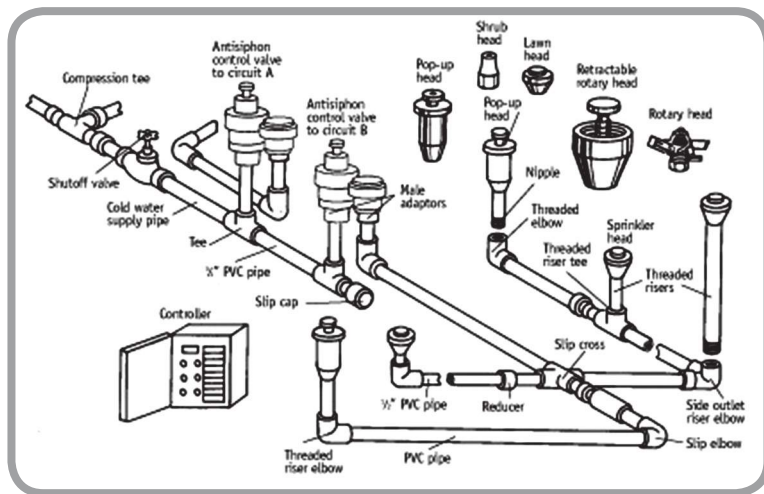
Уреди за управување на извршни функции

За квалитетно проектирање на системите за автоматско јавување и гасење на пожари, потребно е да се познаваат многу добро сите технички карактеристики на системот, упатствата и препораките на производителот, техничките прописи и нормативи во државата, како и условите во кои се поставува односно што и во какви услови треба да се заштити. На пример какви детектори да се одберат, какви средства за гасење на пожари, човечки надзор, периодична проверка и одржување, финансиска издржливост на проектот итн.

Како што претходно спомнавме централната единица при дојава на аларм за пожар покренува однапред дефинирани активности преку уредите за управување на извршни функции. Една од тие активности која е и најчеста е активирање на системот за гасење на пожарот.

Во зависност од видот на пожарот, просторот кој треба да се покрие, постојат и различни видови на системи за гасење на пожар.

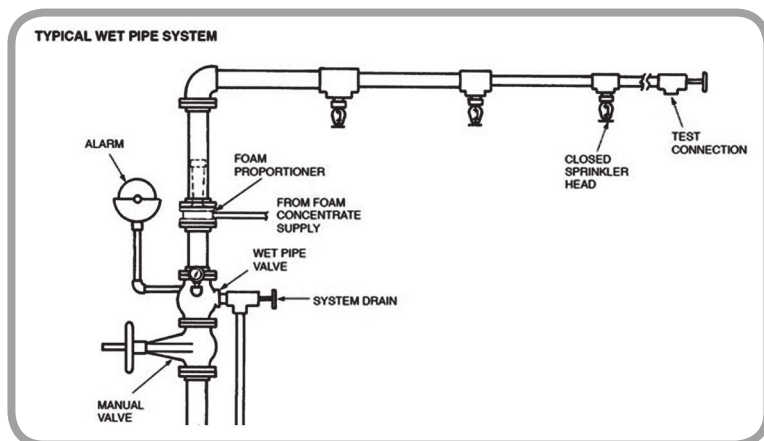
Во начело овој систем преставува инсталација од инфраструктура (цевки) на пренос на материја за гасење пожар (вода, пена, гас), кој преку адекватни системи (прскалки, против пожарни црева, издишници) се распоредува во областа зафатена со пожар (слика 2.28.).



Слика 2.64. Инфраструктура на системот за гасење на пожар

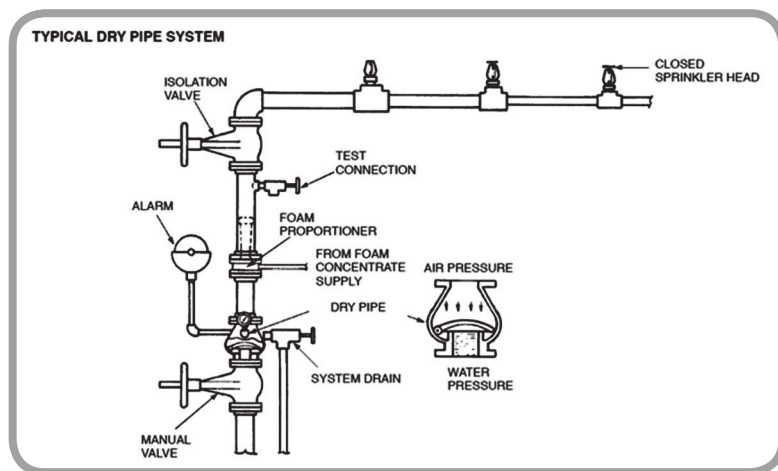
Според начинот на изработка и материјата која се користи за гасење на пожар тие се делат на:

- **Влажен сисѝем** - овој тип на систем е најраспространет. Тие се најсигурен систем за гасење на пожар со можност за комбинирано активирање (автоматски или рачно). Системот е секогаш под притисок, кој се обезбедува преку водоводната мрежа или од посебни цистерни наменети за против пожарниот систем (слика 2.29).



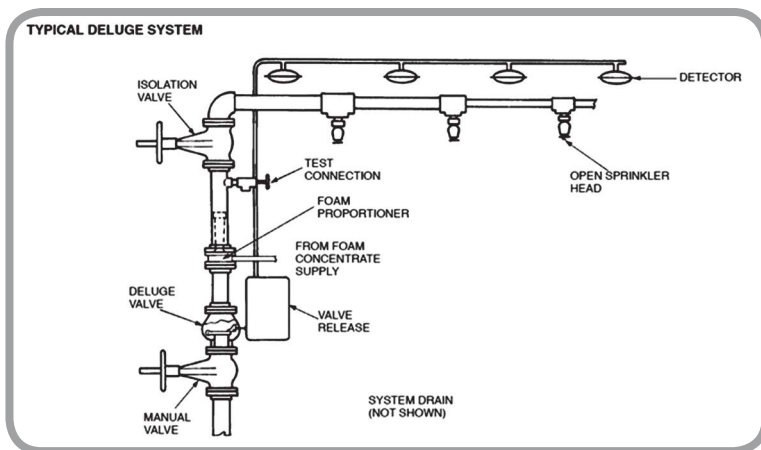
Слика 2.65. Влажен цевководен систем

- *Сув систем* - специфично за овој тип на систем е што во нормална состојба не е под притисок со вода, т.е системот е празен. Цевките се наполнети со воздух со притисок поголем од притисокот на водата така што не и дозволува на водата да продри низ системот (слика 2.30.). Активирањето на овој систем се врши така што во моментот кога централата ќе даде активна команда прскалките се отвараат така што воздухот во системот преку прскалките излегу надвор со што опаѓа притисокот а водата слободно може да надојде низ цевките и прскалките. Овој систем се поставува за заштита на објекти каде амбиенталната температура може да падне под точката на смрзнување, со што може да се предизвика големи штети и нефункционалност на системот за гасење на пожари. Најчесто место за нивно поставување е во објекти кои не се загреваат, гаражи, индустриски фрижидери и останато.



Слика 2.66. Приказ на сув систем

- *Отворен (војвој) систем* - карактеристики на овој тип на систем е тоа што прскалките и другите уреди за гасење се отворени. Инфраструктурата не е под притисок, т.е во цевките нема вода. При активирање на системот за гасење на вода преку електрични вентили се врши отварање на главниот доток на вода кој преку отворените прскалки врши потопување на објектот со вода. Најчеста примена на овој систем има во зони каде се очекува ширењето на пожарот да е интензивно, како што е вентилацијата, коридорите за извлекување во случај на пожар и останато (слика 2.31.).



Слика 2.67. Отворен систем

- *Систем со пена* - овој тип на систем може да биде технички изведен како влажен, сув или отворен систем. Карактеристично за него е тоа што наместо вода која се користи за гасење се користи специјална пена за гасење на високо запливи течности како на пример бензин, нафта, хемиски супстанци. Најчеста примена има во аеродромските хангари, складишта со опасни течности.
- *Систем со прашок* - технички се изведува како и другите системи со единствена разлика во средството за гасење. Карактеристично за овој систем е што користи специјална хемиска супстанца, во прашкаста форма која има карактеристика да го задушува пожарот при тоа да не предизвикува несакани ефекти како течностите (краток спој на инсталација, уништување на документација и т.к.н). Најчесто се користи за обезбедување на ИТ сали, архиви, музеи.

2.4. СИСТЕМИ ЗА ДЕТЕКЦИЈА И ДОЈАВА НА ВОДА, ТОКСИЧНИ ГАСОВИ И ТЕЧЕН НАФТЕН ГАС (ПЛИН)

Системот за детекција и дојава на вода, токсични гасови и течен нафтен гас, претставува систем кој има задача навремено да информира при појава на некои од параметрите. Разликата на овој систем со останатите системи е во употребата на специјално наменети сензори за секој од овие параметри како и начинот на инсталирање на системот. Поради специфичноста на секој сензор овој систем ќе го поделиме на два система:

- систем за детекција на опасни течности (флуиди) и
- систем за детекција на опасни гасови.

Овие системи поради нивната специфична намена и се поголемата распространетост (аеродромско обезбедување) потребно е да бидат инсталирани, како и менаџирани од страна на стручно оспособен кадар. Не почитувањето на процедурите кај овие системи доведува до катастрофални последици како кон животот и здравјето на луѓето така и кон природата.

Систем за детекција на опасни течности (флуиди)

Опасни течности (флуиди), претставуваат хемиски материи кои во услови на чување или при истекување се во течна агрегатна состојба а во допир со надворешни влијанија имаат карактеристика да се samozапалат, прејдат во гасна состојба, корозираат или да го сменат својот хемиски состав.

Начелно овие материи (освен водата) се штетни за човековото здравје и се лесно запаливи. За таа цел во простории каде има можност од опасност од ваков вид на материи се инсталираат системи за детекција на опасни материи.

Како и останатите видови на системи и овој систем се состои од:

- Сензори
- Централна единица и
- Уреди за алармирање и известување.

Централната единица и уредите за алармирање и известување ги носат истите начела како и останатите системи. Главна разлика во овој вид на систем се сензорите. Овој систем за детекција на опасни течности во начело секогаш се комбинира со системот за детекција, јавување и гасење на пожар.

Сензори

Сензорите за детектирање на опасни течности по својата изработка се разликуваат од останатите сензори. Тие спаѓаат во групата сензори за специјални намени. Изработени се од материјали кои се отпорни на вода, корозија, хемиски влијанија како и на електрични празнења. Поделбата ќе ја направиме на два вида:

- **Сензори за незаѝаливи материји (вода)** - Овие сензори се употребуваат на објекти кај кои е потребно да се заштитат од присуство на вода. Сензорите во начело работа на принцип на промена на отпорноста на сондата на сензорот. Во нормална состојба сондата на сензорот има одредена спроводливост но при појава на вода или влага оваа отпорност опаѓа (водата има улога на проводник на електрична енергија) со што сондата дава променлива вредност на сензорот. Во зависност од количеството на вода или влага вредноста е поголема, со што сензорот оваа информација ја доставува до централната единица. Овој тип на сензор е со ИП 67 стандард и е намент за издржливост на честички од прашина како и целосно потопување во вода до 3 метри длабочина.



Слика 2.68. Сензори за детекција на вода/влага

Овој вид на сензори е најраспространет во индустријата каде присуството на вода/ влага во производствениот процес е недозволив (слика 2.33.).



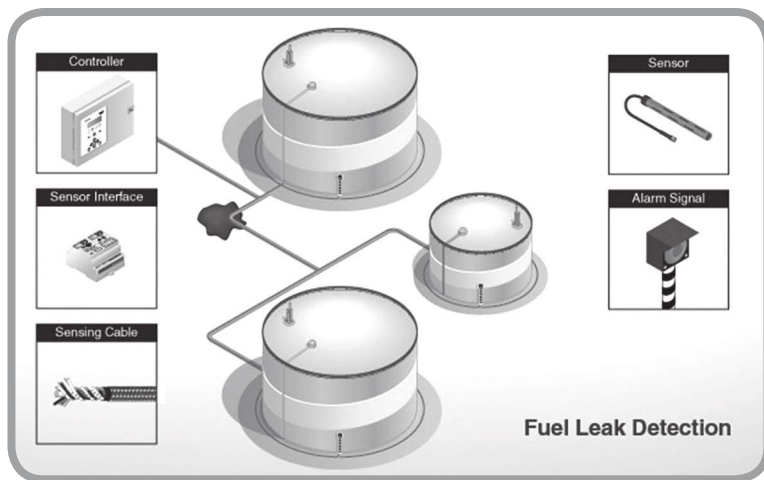
Слика 2.69. Сензор за вода/ влага во производство

- *Сензори за запаливи материји (нафта, бензин, шечен гас, уље).* - Овој вид на сензори се карактеризира со висока издржливост во екстремни околии. Најчеста примена имаат во нафтената индустрија за обезбедување на складишта за запаливи материји, нафтоводи, гасоводи, индустријата за преработка на нафтени деривати како и услужни дејности поврзани со испорака и точење на нафта и нејзини деривати. Во зависност од потребите се користат различни видови на сензори кои се изработени согласно бараните технички спецификации. За обезбедување на нафтени резервоари и нафтоводи се користат таканаречени детектирачки кабли (слика 2.34.).



Слика 2.70. Слика 34. Детектирачки кабел

При обезбедување на комплексни градби од ваков вид на опасност се користи комбиниран систем за заштита каде секоја точка од објектот се монитира (слика 2.35.).



Слика 2.71. Сензори за заштита на резервоари

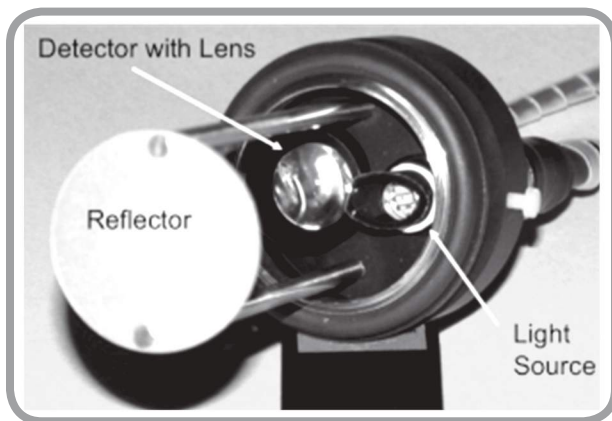
Систем за детекција на опасни гасови

Опасни гасови претставуваат гасовидни материи кои се штетни за животот и здравјето на луѓето и околината. Со нивното истекување и ненавремено детектирање може да се предизвика штета на објектот кој се обезбедува, а со игнорирање на состојбата можни се и поголеми последици на околината. Најчеста примена на овие системи има во хемиската и нафтената индустрија. Примената на овие системи во последно време зема поголем замав и во обезбедувањето на домаќинствата, малите индустриски комплекси каде земјекитот гас се користи како енергенс со цел да се спречи неконтролираното мешање на токсични или експлозивни гасови со воздух.

Еден од најчесто користени гасови е земјениот гас кој во последно време се повеќе се користи како енергенс за загревање, готвење но и за ладење. При инсталација на овој вид на систем секогаш се зима во предвид поставеноста на инсталацијата за пренос на штетните гасови, местата за складирање на овие гасови како и комбинирање на овој систем со системот за детекција, јавување и гасење на пожар.

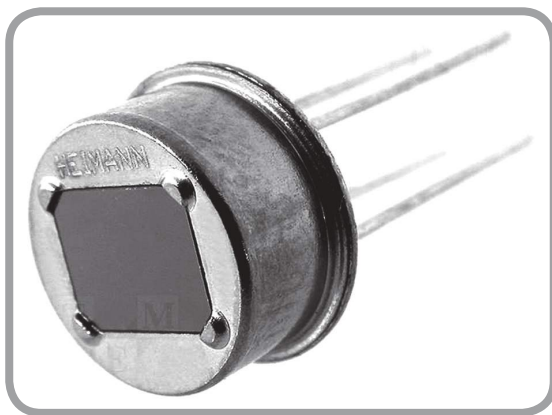
Важен елемент во овој систем е сензорот за детекција на штетните гасови. Тој има задача постојано да врши мерење на односот на воздухот со останатите видови на гасови. Важно е да се напомене дека постојана калибрација на овие сензори е битна за правилно функционирање на системот. Овој тип на сензори може да се подеси за мерење на некој специфичен гас или за мерење на секое отстапување на процентот на кислород. Според технологијата на детектирање на гасови, сензорите се делат на две групи:

- *Оптички детектор* - овој вид на детектор работи на принцип на промена на бојата на сензорот во зависност од концентрацијата на детектираниот гас (слика 2.36.).



Слика 2.72. Оптички детектор на гас

- *Електричен детектор* - работи на принцип на генерирање на електричен сигнал од активната состојка при контакт со детектиран гас (слика 2.37.).



Слика 2.73. Електричен детектор на гас

Во било кој случај кога ќе дојде до промена на параметрите зададени на сензорот тој испраќа сигнал до централната единица која потоа превзема претходно зададени процедури. Најчеста постапка е да изврши алармирање на персоналот, да ја соопшти испораката на гасот и да изврши проветрување на просторијата преку системот за вентилација.

2.5. СИСТЕМИ ЗА ВИДЕО НАДЗОР CCTV

Систем за видео надзор или CCTV (closed circuit television) е систем кој користи видео камери за прикажување на сигнал (слика), на одредено место на ограничен број на монитори. За разлика од комерцијалната телевизија овој сигнал не се емитува јавно и се пренесува исклучиво по принцип точка до точка (P2P- point to point или point to multi point). Преносот на сигнал се остварува преку жична врска или безжична конекција.

Со инсталирањето на овој систем во значителна мера се зголемува системот за обезбедување на објектот. Системот не само што нуди дополнителна мерка на безбедност туку и преку архивираниот материјал се врши дополнителна анализа на безбедноста, увид во настаната состојба, а со модерните системи веќе е возможно и замена на останатите системи само со системот за видео надзор.

Дизајнирање на системот за видео надзор е сложен процес кој мора да ги опфати сите аспекти од безбедносната анализа како што е заканата за безбедноста на имотот, лицата или материјалните добра.

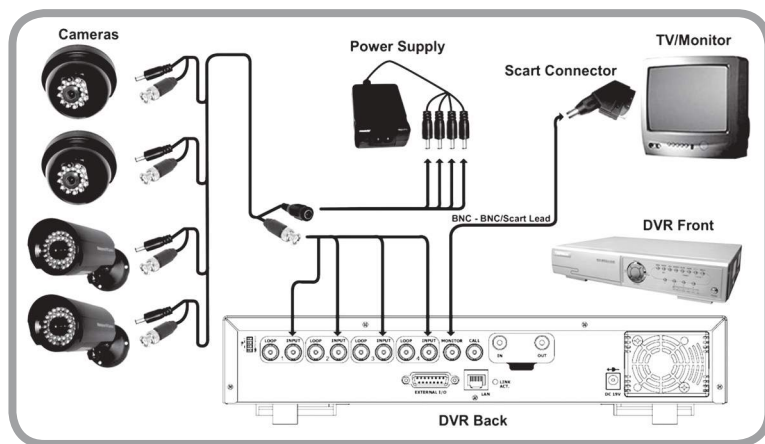
Според технологијата системот се дели на:

- Аналоген систем-
- IP систем
- Хибриден систем

Аналоген систем

Аналогниот систем за видео надзор е прв систем за видео надзор. Самото име кажува дека во овој систем сигналот (сликата) е аналогна. Специфична карактеристика на овој систем е тоа што целокупната инсталација од камерите завршува на едно централно место, каде е сместен снимачот. Воедно снимачот мора да биде во непосредна близина до просторијата која е наменета за мониторинг на овој систем. Поради оваа карактеристика кадарот кој е задолжен за овој систем има директен контакт со снимачот што во голема мера ја нарушува безбедноста на системот. Медиумите за снимање т.е чување на видео записите во почетокот биле на магнетни ленти, ВХС касети за да во брзо време мигрираат на системи за дигитално архивирање на снимениот материјал (DVR- digital video recorder)

Аналогниот систем и денес се користи пред се поради неговата цена но и поради можноста за поставување на камери на поголеми далечини.

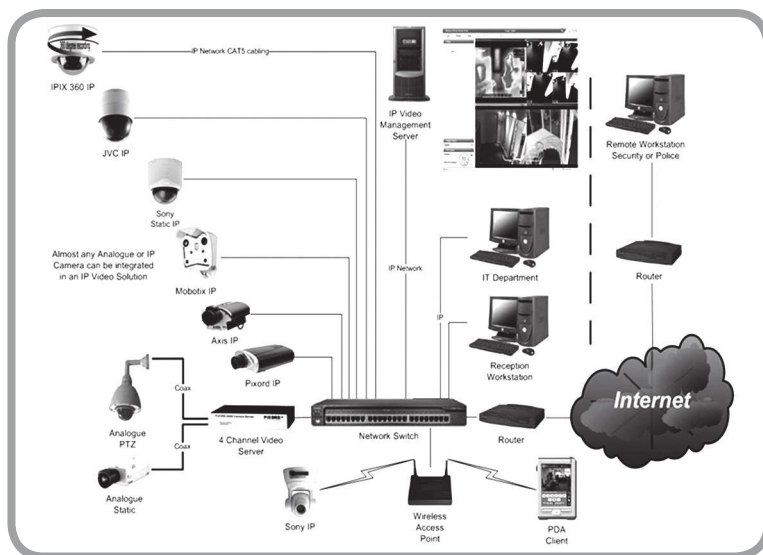


Слика 2.74. Дијаграм на аналоген систем за видео надзор

IP систем

Со напредокот на компјутерската технологија како и на мрежната опрема, се развива и индустријата за видео надзор. Системите за видео надзор базирани на IP технологија користат IP камери кои емитураат дигитални сигнали (слика) кон централното место. Карактеристика за овие системи е тоа што не е потребно каблирањето да се врши од камера до снимачот туку преку компјутерската мрежа на објектот што се обезбедува сигналот може да се дистрибуира секаде каде има потреба. Во рамки на развојот на оваа технологија направен е и развој на снимачите. Согласно технологијата за овие системи се користат и мрежни видео снимачи (NVR-network video recorder) кои се наоѓаат во рамките на ИТ салите на објектите кои се обезбедуваат. Со тоа се постигнува поголема физичка безбедност на снимачите и неможност директно да се работи на нив. Пристапот до архивираниот материјал и гледање во живо, се изведува преку работни станици (компјутери) кои преку LAN/WAN мрежата и кориснички софтвер имаат контролиран пристап до NVR. Користејќи ги интернет конекциите може да се пристапи и од други далечни локации кои не се дел од LAN мрежата на објектот што се обезбедува (слика 2.39.).

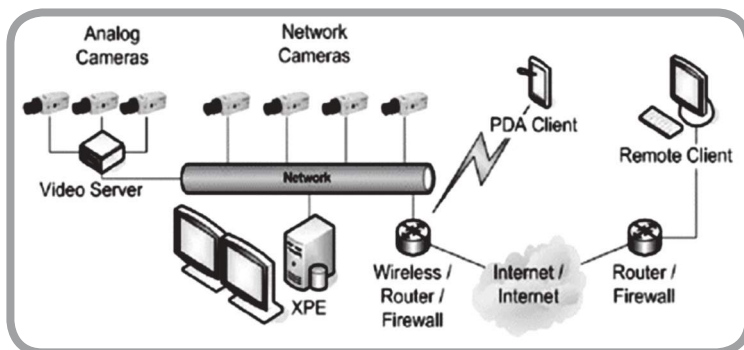
Овој систем за разлика од аналогниот е повеќе кратно поскап, и се користи за поголеми мерки за безбедност од делокругот на работата на полицијата, армијата, државните агенции за безбедност и останати безбедносни структури.



Слика 2.75. Дијаграм на IP систем

Хибриден систем

Со појавата на новите IP системи на пазарот, потребно беше дополнителен систем кој што ќе може да ги интегрира старите аналогни технологии со новите IP системи. За таа цел постои хибриден систем кој што ги подржува и двата типа на технологии. Хибридниот систем всушност преставува NVR снимач кој на себе има приклучоци кои што ги подржуваат аналогните камери. Овој снимач денес има широка употреба, пред се за покривање на објекти каде е потребно поставување на камери на поголема далечина, како и за искористување на веќе постоечките камери при надградба на застарените системи (слика 2.40).



Слика 2.76. Дијаграм на хибриден систем

Компоненти на системот за видео надзор

Системот за видео надзор претставува сложен склоп од елементи кои преку медиумите за пренос на информации комуницираат меѓусебно и доставуваат информации.

Без разлика за каков систем за видео надзор се работи составни делови се:

- Видео камери
- Уред за снимање
- Помошни уреди
- Уреди за поврзување

Видео камери

Видео камера претставува уред кој преку својот сензор ја конвертира визуелната или ИР светлина во времена сензорска величина која потоа процесорот на камерата ја претвара во електричен запис. Во зависност од технологијата камерите се делат на:

- Аналогни камери и
- Дигитални камери

Според техничката изведба камерите се делат на:

- Бокс камери (фиксни камери)
- ДОМЕ камери (фиксна камера)
- ПТЗ (pan-tilt- zoom) камера (вртливи камери)
- Компактни камери (фиксни камери)

Аналогни камери

Аналогните камери се камери кои добиените информации од сензорот на камерата преку колото за синхронизација ги претвара во аналоген сигнал.



Слика 2.77. Предна и задна страна на аналогна камера

Преносот на слика од овој тип на камери се изведува преку коаксиален кабел кој се поврзува на камерата од една страна и ДВР на другата страна со помош на БНЦ конектори.



Слика 2.78. Коаксиален кабел со БНЦ конектори

Напојувањето на камерите во зависност од видот на камерата варира од 220 V AC или 24 V AC, до 12 V DC. За напојување се користат стандардните енергетски кабли.

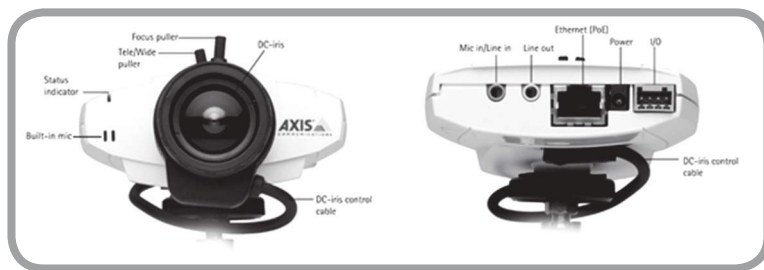
Квалитетот на сликата кај овие камери е лимитиран и тој се движи во опсег на ВГА резолуцијата. Тој се пресметува врз основа на бројот на хоризонтални и вертикални линии кои може да ги прикаже, односно бројот на ТВ линии. Вообичено аналогна камера има капацитет од 380 ТВ линии.

Аналогните камери користат стандардни телевизиски формати како: CIF, NTSC, PAL, SECAM.

Во почетокот видео материјалот бил запишуван на магнетна лента. За да може видео записот од аналогната камера да се запише на лента, брзината на вртење на лентата била многу спора, за да се постигне континуирано снимање на материјалот, т.е. за три часовна лента да може да снима 24 часа брзината на снимање била 4 слики во секунда. Што во суштина не ги задоволува денешните побарувања. Можноста видео записот од аналогната камера да биде снимен на дигитален носач (хард диск), се постигнало со воведување на CCTV видео карта која се монтира на компјутер и за која е потребен адекватен софтвер. Овде улогата на конвертер ја има видео картичката, со тоа што за да обезбеди континуирано снимање конвертираниот сигнал се компресира во сооднос 5:1 (MPEG). Во поново време ДВР се оние кои ја превземаат целокупната работа. Тоа се всушност системи базирани на РС технологија каде сите делови се интегрирани во едно решение.

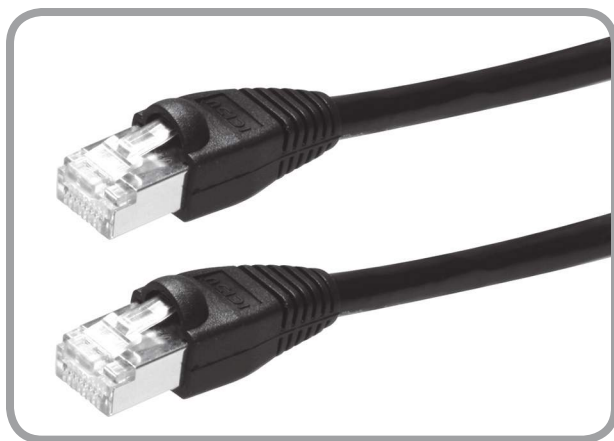
IP камери

IP камера (internet protocol camera), е вид на камера која информациите до НВР ги пренесува користејќи ја компјутерската мрежна инсталација. Бидејќи во денешно време и компјутерските камери (web camera) работат на овој принцип, кога се зборува за IP камера генерално се мисли за камера предвидена за CCTV.



Слика 2.79. Предна и задна страна на IP камера

Преносот на слика од овој тип на камери се изведува користејќи FTP/UTP кабли за мрежно поврзување, кој се поврзува со RJ45 конектори од една страна на камерата и на мрежен уред (HUB, Switch) на другата страна. Напојувањето кај овие камери генерално е 12 V DC. Голема предност е можноста за PoE (Power over Ethernet), што претставува напојување преку PoE свич, со што се намалува потребата за дополнителна инсталација.



Слика 2.80. ФТП кабел со RJ45 конектори

Квалиетот на сликата кај овие камери како што напредува технологијата како да нема граница. Со почетоците и резолуција од 1.3 МР, денес на пазарот може да се најде и резолуција од 12 МР. Овие високи резолуции допринесуваат да овој тип на камери се користи за повеќе специфични намени како на пример во системи за препознавање на регистарски таблички, мерење на брзини на движење, системи за препознавање на лица, покривање на поголеми периметри со една камера, употреба на камерите за посложени операции како на пример броење на проток на посетители, препознавање на оставени објекти, дополнителна анализа на снимениот материјал и друго.

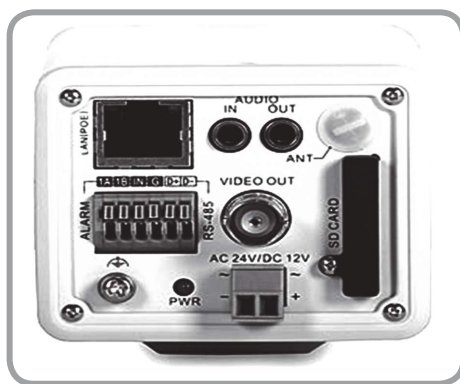
Во последно време како дополнителни можности на овие камери е и опцијата за двонасочно аудио, кое е дополнителен чекор кон добивање на поквалитетен систем за обезбедување. Двонасочното аудио може да се искористи како средство за алармирање, комуникација, но и како дел од системот за обезбедување (детектирање на звук во некоја забранета зона). Друга опција е можноста за локално снимање на мемориска картица. Снимањето на мемориска картица е од големо значење во случај кога имаме чести појави на губење на конекцијата со НВР, дали од техничка природа или од друга причина.

Со зголемувањето на резолуцијата на камерите се зголемува и потребата од поголем проток на инфромациите низ компјутерската мрежа, како и зголемувањето на капацитетите за чување на снимениот материјал. Како за споредба ако за 16 аналогни камери беше потребно 500 МБ хард диск за чување на материјал од 20 дена, за истиот број на IP камери со резолуција од 2 МП потребно е 3 ТБ на капацитет. За да може да се задоволат

потребите на корисниците а воедно и да не се оптерети инфраструктурата, IP камерите користат кодек на компресија H.264/ MPEG-4 кодек кој нуди голема компресија за транспорт и чување на HD видео записи.

Хибридни камери

Овие камери всушност преставуваат IP камери кај кои има вграден аналоген приклучок. Намената на овие камери е да може да се употребуваат во различни системи во зависност од потребата. Важно е да се напомене дека преку аналогниот приклучок не може да се добијат високи резолуции иако камерата преку IP конекцијата го нуди тоа.



Слика 2.81. Задна страна на хибридна камера

Поделба на камериџе

Според местото каде се монтираат камерите се делат на:

- *Внатрешни* - внатрешните камери се стандардни камери кои ја имаат основната заштита од влага и прашина. За нивна монтажа се користат држачи кои во зависност од потребите се изработуваат во најразлични форми. Постојат камери за кои не потребен посебен држач (ДОМЕ камери) и тие се предвидени за внатрешно таванско монтирање.



Слика 2.82. Држачи за внатрешна употреба

- *Надворешни* - всушност преставуваат камери наменети за внатрешна употреба (БОКС камери) ставени во посебни куќишта со држачи, кои се водоотпорни и опремени со адекватен систем за ладење и греење. Постојат и камери кои фабрички се опремени за надворешна употреба (ПТЗ камерите). Кај IP камерите кои се монтираат во куќишта потребно е изведба на посебна инсталација за напојување на куќиштето.



Слика 2.83. Куќиште со држач за надворешна камера

Според техничката изведба камерите се делат на:

- *Бокс камери* – претставуваат фиксни камери кај кои сите компоненти се спакувани во заштитна пластично куќиште. Овие камери се наменети за внатрешна употреба а ставени во куќиште за надворешна употреба се употребиваат и во надворешна средина.



Слика 2.84. Бокс камера

- *ДОМЕ камери*- претставуваат фиксни камери кои се наменти за внатрешна и надворешна употреба. Специфично за овие камери е што на нив веќе има вградена леќа и нема можност за нејзина надградба. првенствено се предвидени за монтирање на тавани, но со ротација на камерата може многу лесно да се монтираат на сидови.



Слика 2.85. ДОМЕ камера

- *ПТЗ (pan-tilt-zoom) камера* - претставува вртлива камера, кај која има вградена vario focal леќа која дава можност за рачно или автоматско зумирање или фокусирање. Овие камери заедно во комбинација со корисничкиот софтвер нудат широк спектар на операции како што се зонско патролирање, дефинирање на зони на набљудување, во содејство со системот за детекција на движење има можност за детектирање на правецот на движење. Камерите се фабрички изведени во заштитно кукиште со адекватно ладење и греење, кое ги задоволува стандардите за надворешна употреба (слика 2.49).



Слика 2.86. ПТЗ камери

Компактни камери – претставуваат фиксан камера како комбинација од сите три видови на камери со тоа што се опремени со дополнителен систем за осветлување IR рефлектор како и вградена леќа. Карактеристика им е што може да се употребуваат и за внатрешно и за надворешно инсталирање.



Слика 2.87. Компактни камери

Уреди за снимање

Уредот за снимање (ДВР, НВР) е склоп на компјутерска електроника и апликативен софтвер кој имаат задача добиеното видео од страна на камерите, дигитално да го обработат и запишат во дигитална форма на хард диск или друг дигитален уред за запишување на податоци. Како што спомнавме во зависност од видот на камерите кои се користат, така и снимачите се делат на ДВР кај кои се користат аналогни камери, НВР кој користи IP камери и хибриден снимач кој ги подржува и двата вида на камери.

ДВР – дигитален видео рекордер

Дигиталниот видео рекордер претставува склоп на компјутерски елементи и софтвер интегрирани со хардверот и софтверот на видео картата. Главна улога во секој ДВР ја има видео картата. Таа е носител на делот за видео надзор и има задача да изврши конектирање на аналогните камери со ДВР како и да изврши дигитална конверзија на добиените информации. Секој ДВР во зависност од видео картата е лимитиран во однос на бројот на камери што можат да се приклучат. Генерално конфигурацијата на ДВР доаѓа како 4, 8, 16 и 32 канален. Надградба на ДВР се врши со паралелно спојувањесо друг ДВР со број на конекции кои што се потребни.



Слика 2.88. Предна и задна страна на ДВР

Покрај приклучоците за камери на ДВР-ите се наоѓаат и други видови на приклучоци. Стандардни приклучоци се:

- LAN- за мрежно поврзување на ДВР,
- Конекции за ПТЗ контроли
- VGA, BNC, S-Video приклучок за монитори,
- УСБ приклучоци за надворешни мемории
- Во комбинираните системи се наоѓаат и алармни приклучоци (COM порти)

Важен елемент во секој ДВР е софтверот за обработка и прикажување на видео сигналот. Во зависност од видот на софтверот може да се врши видео анализаида сеизвршуваат помалку комплексни операциикоиселимитирани поради квалитетот на видеото. Прикажувањето на видео записот во живо, прегледувањето на видео записот како и администрирањето се врши преку корисничкиот интерфејс, кој му дава можности на операторот да избира кои камери да ги гледа и на каков распоред, дополнителни информации врзани

за состојбата на системот (статус на снимање, слободен простор, детекција на движење и останато), преглед на снимениот материјал како и постапка за архивирање на материјалот. Корисничкиот интерфејс е достапен само преку LAN конекција преку работна станица (компјутер).



Слика 2.89. Слика 53. Кориснички интерфејс

HBP (NVR-Network video resorder) мрежен видео рекордер

HBP претставува мрежен уред кој преставува склоп на компјутерски компоненти кои заедно со софтверот вршат превземање на дигиталните сигнали добиени од камерите. За разлика од ДВР овде не постои видео карта за превземање на видео сигналот туку сигналот го добива преку мрежата на која се приклучени камерите. Бројот на видео камери кои може да се менаџираат преку HBP зависи од бројот на лиценци за кои е наменет софтверот. Надградбата овде е многу полесна и се базира на надградба на софтверот.



Слика 2.90. Предна и задна страна на НВР

За разлика од ДВР на задната страна на НВР иам стандардни компјутерски приклучоци. Во главно НВР се изработуваат во верзија за монтажа во РАК ормар, со што се ограничува пристапот и директното работење на операторите со НВР. Пристапот до снимениот материјал како и следење на видео сигналот во живо се остварува преку работна конзола на која има инсталирано кориснички софтвер. Со оглед на тоа дека квалитетот на видеото е во голема мера поквалитетно од аналогните камери, овозможено е да се врши комплексни операции на разработка на сликата, воочување на детали, дигитален зум, поделба на сликата по сектори, користење на видеото за зонирање на просторот со избор на забранети зони на пристап, детектирање на промена на слика (оставени торби, помрднати или исчезнати предмети), анализа на претходни движења, поквалитетна анализа на регистарски таблички, препознавање на лица, броење на објекти, воочување на сомнителни активности, мерење на брзина на движење и многу други операции.

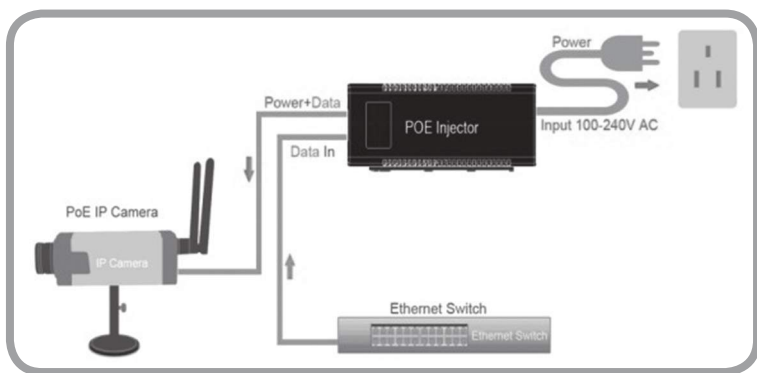


Слика 2.91. Приказ на видео анализа

Помошни уреди

За успешно поставување и функционирање на системот за видео надзор потребни се дополнителни помошни уреди кои треба да го олеснат функционирањето на системот. Помошни уреди во системот за видео надзор се:

- *IR рефлектор* - претставува извор на инфра црвена светлина, која е невидлива за човечкото око, но е видлива за камерата. Наменет е за осветлување на отворени и затворени простории каде нема доволно светлина за правилно функционирање на камерата. Според намената постојат повеќе видови кои се користат во зависност од потребите.
- *PoE injector/splitter* - претставува извор на електрична енергија која преку мрежниот кабел се носи до ИП камерата. Во услови кога нема PoE свич, овие инјектори се решение за напојување. Работат на принцип на искористување на слободните парици од мрежниот кабел предвидени за напојување (слика 2.56.).



Слика 2.92. Шематски приказ на работа на PoE инјектор

- *БНЦ балуни* - наменети се за трансформацијанна видео сигналот добиен на БНЦ излезот и негово проследување до ДВР до друг балун користејќи двожила прица или ФТП/УТП кабел. На ваков начин преку ФТП кабел може да се пренесе слика и до 400 метри. Со користење на активни балуни и кабел ФТП кат 5е може да се пренесе видео и до 1800 метри.



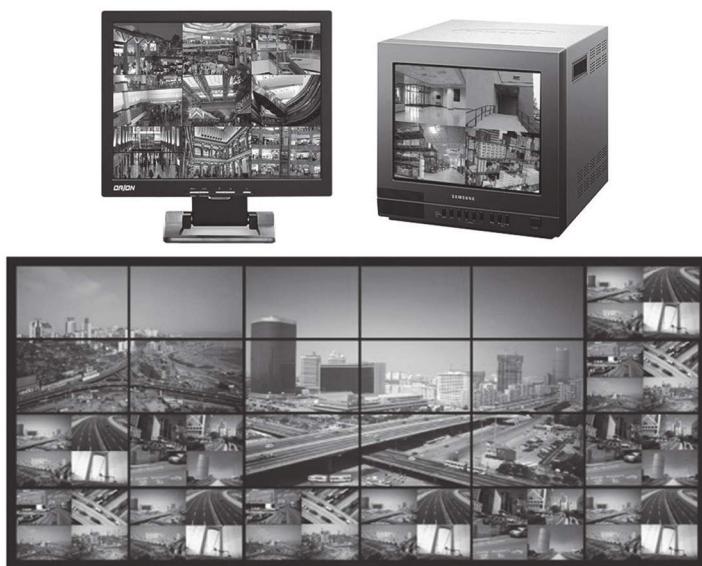
Слика 2.93. БНЦ балуни

- *Леќа* - Леќата претставува оптички уред кој има задача рефлектираната светлината која произлегува од објектот да ја префрли на сензорот на сликата. Леќите се важен фактор во дизајнирањето на системот за видео надзор. Изборот на правилна леќа претставува една од најтешките задачи при дизајнирањето на системот за видео надзор. Со правилен избор на леќи се постигнува поголемо и поквалитетно покривање на објектот што се обезбедува. Постојат повеќе видови на леќи кои се разликуваат по своите технички параметри. Според видот на камера за која се користат, се делат на аналогни и дигитални (мега пикселни). Според фокусот постојат леќи со фиксен фокус и варијабилан фокус. Денеска се користат различни видови на леќи кои одговараат на потребите на системот за видео надзор. Тие се достапни со различен агол на покривање од рибино око 1800, широко аголни 900, средни 400 и стеснувачки 50. Во последно време се повеќе се користат и панорамски леќи кои покриваат 3600 од просторот.



Слика 2.94. Различни видови на леќи

- *Дисплеи* - мониторите и видео ѕидовите преставуваат дисплеи преку кои може да се врши надгледување на камерите кои се во склоп на видео надзорот. За професионални системи постојат дисплеи кои се дефинирани за 24/7 режим на работа. Резолуцијата и карактеристиките варираат од производ до производ, па за таа цел потребно е при конфигурирање на системите да се земе оптималната конфигурација на овие уреди.



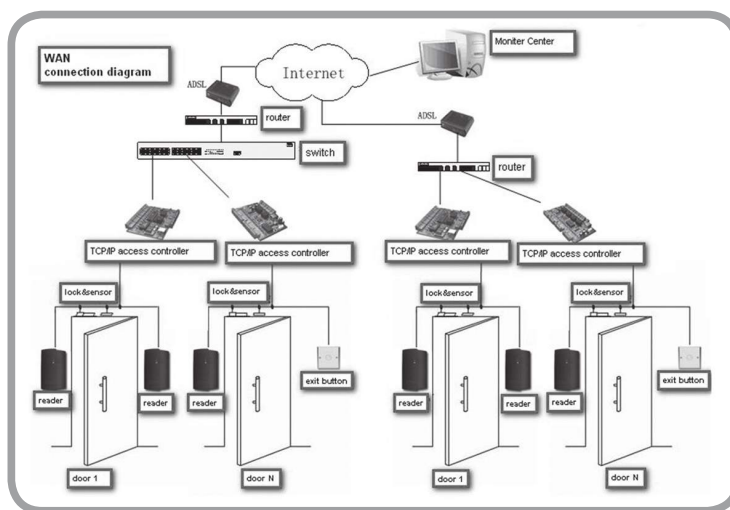
Слика 2.95. Различен вид на дисплеи за приказ на видео надзор

2.6. СИСТЕМИ ЗА КОНТРОЛА НА ПРИСТАП

За организирање на правото на пристап на различна група на лица на различно безбедносно ниво се користи систем за контрола на пристап. Системот за контрола на пристап претставува склоп на уреди и подсистеми кои имаат задача да извршат категоризирање на правото на пристап на лица спрема нивните потреби како и оневозможување на пристап на лица кои немаат привилегии за влез/излез. Паралелно овој систем се почесто се користи и како систем за контрола на работното време. За зголемување на безбедноста системот за контрола на пристап секогаш се комбинира со системот за видео надзор.

Составни делови на овој систем се:

- Уреди за регистрирање и идентификување
- Централен систем за менаџирање
- Дополнителни уреди



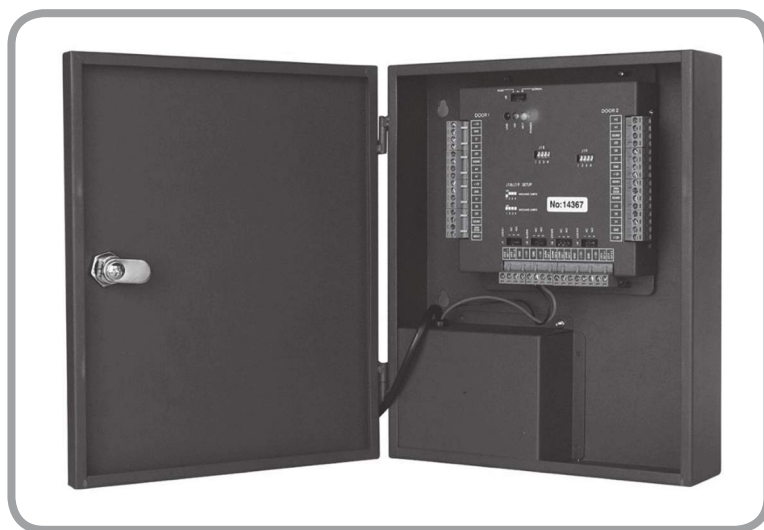
Слика 2.96. Топологија на системот за контрола на пристап

Уреди за регистрирање и идентификација

Уредите за регистрирање и идентификација претставуваат периферни делови на системот и се хардверски компоненти кои преку поставената инфраструктура комуницираат со централниот систем. Главна намена им е да извршат проверка на правото на пристап на барателот и по проверката да одобрат или да одбијат право на пристап на барателот.

Во уреди за регистрирање спаѓаат:

- **Контролери** – Контролерите се хардверски компоненти на системот кои преставуваат врска помеѓу централната единица (софтвер за менаџирање) и читачите. Нивна задача е информациите добиени од читачите да ги обработат или проследат до централната единица. Според изведбата тие може да работат самостојно и во тој случај се интегрирани заедно со читалот (stand alone card reader) или да бидат дел од комплексна мрежа управувани од централниот софтвер. Контролерите имаат внатрешна меморија која им овозможува да работат самостојно во случај на прекин на конекцијата со централниот софтвер. Исто така внатрешната меморија се користи и за вчитување на базата на корисници со дозволен пристап со што се овозможува побрза комуникација. За обезбедување на 24 часовен режим на работа системот потребно е да биде приклучен на резервно напојување (УПС, вградлива батерија).



Слика 2.97. Контролер во заштитно кукиште и резервно напојување

- **Читачи на картици или биометриски податоци** - читачите на картици или биометриски податоци се уреди преку кои се вчитуваат информациите на барателот за пристап. Читачите се поврзани со контролерите и во содејство со нив преку своите средства за сигнализирање го известуваат барателот на пристап за одобрен или одбиен пристап. Постојат повеќе видови на читачи и тоа:

- **Читачи на картици** - идентификација на лицето се врши преку картичка. Во зависност од изведбата може да има и тастатура која се користи за дополнително утврдување на идентитетот на барателот на пристап. Според техничката изведба постојат читачи за внатрешна инсталација, надворешна како и читачи отпорни на вандализам.



Слика 2.98. Читачи на картици

- **Читачи на биометриски податоци** - ова се посовремени системи и се користат за обезбедување и контрола на пристап на објекти со висок степен на безбедност. Карактеристично за нив е постапката за утврдување на идентитетот на барателот. Самото име кажува дека барателот се најавува преку своите биометриски податоци: отпечаток на прст, скенирање на глас, рожница на око.



Слика 2.99. Читач на биометриски податоци со тастатура

- **Картици** - преставуваат уреди преку кои барателот на пристап се идентификува на системот. При креирање на правило за пристап на секој корисник му се доделува единствена картичка преку која корисникот се најавува во системот. Според технологијата што ја користи постојат различни видови на картички. Најраспространети се Proximity картиците, потоа smart cards каде има имплементирано чип, HID iclass картици и други. Според начинот на изработка можни се изведба како приврзок за клучеви или пластична картичка.



Слика 2.100. Видови на картички

Централен систем за менаџирање

Централниот систем за менаџирање е мозокот на овој систем. Тој има главна задача во спроведување на мерките за контролиран пристап и преставува софтверска апликација која е инсталирана на сервер. Централниот систем преку својата апликација има задача да:

- Комуницира со контролерите
- Креира сигурносни нивоа за пристап (различни нивоа на пристап)
- Врши администрирање на корисниците (внесување на нови, бришење на стари корисници, одобрување на право на пристап)
- Архивира настани, аларми и логови од целиот систем
- Врши алармирање при недозволен пристап или насилан пристап
- Преку работните станици дава приказ на состојбата на системот
- Ја контролира работата на сите елементи од системот и врши ажурирање.



Слика 2.101. Приказ на софтвер за контрола на пристап

Дополнителни уреди

За да може системот за контрола на пристап правилно да функционира потребни се дополнителни уреди. Тие имаат извршна улога во процесот на контрола на пристапот, воедно и имаат задача да ги зајакнат мерките на безбедност на системот.

Дополнителни уреди во системот за контрола на пристап се:

- **Безбедносни врати**³ - За правилно воведување на мерките на безбедност во системот за контрола на пристап потребни се безбедносни врати, кои според мерките кои се потребни за заштита се делат на:

³ Безбедносни врати- стандард за безбедносни врати EN 1143-1

- Заштитна врата тип 1- најслаб степен на заштита
- Заштитна врата тип 2
- Заштитна врата тип 3
- Заштитна врата тип 4- најголем степен на заштита
- *Контролори на влез/излез* - всушност преставуваат уреди за контролиран проток на луѓе и возила. Во пракса најчесто се користат рампи за возила и триподи за контрола на проток на луѓе.
- *Сензори* - сензорите се користат како дополнително обезбедување, на вратите. Главна примена имаат при детектирање на насилно отварање на врата или во случаи кога одредена врата подолго време стои отворена.
- *ТЦП/ИП модули* - модули за конекција на контролорите со централната единица
- *Камери* - дополнителни мерки на обезбедување, во начело секоја врата на која има контролиран пристап потребно е да биде покриена со видео надзор.
- *Електрични и магнетни брави*
- *Механички брави, шилдови*
- *Домофони, видеофони*
- *Буџкачи на врати*

2.7. ИНТЕГРИРАНИ СИСТЕМИ

Интегрирани безбедносни системи се комбинација од сензори, контролни уреди и софтвер кои работат во една целина и кои им служат на корисниците, да ги заштитат животите и имотот кој го обезбедуваат од различни видови на опасност.

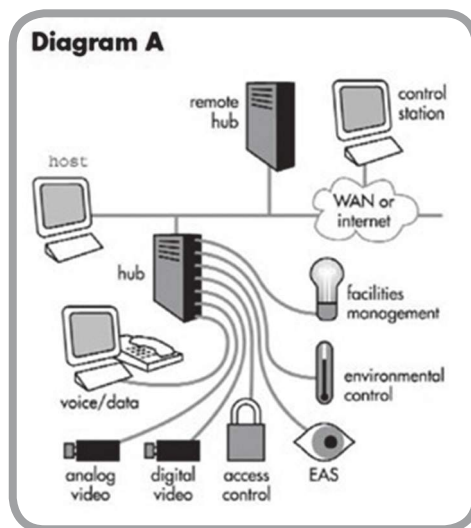
Интеграцијата на повеќе видови безбедносни системи е релативно нов концепт во светот на обезбедувањето. Во минатото, безбедносните системи биле по дискретни и одвоени еден од друг. Видео надзорот или CCTV користеше комерцијална видео технологија за трансфер на аналогно видео преку коаксијален кабел, секој аларм и секоја електронска брава за контрола на пристап беа поврзани преку кабли што користат различни протоколи до командниот центар. Со оглед на наведеново така и секој систем посебно беше вградуван од различни технички лица. Така архитектите ги бираа вратите, консултантите за безбедност ги бираа системите за контрола на пристап и системите за мониторинг и видео надзор, а техничарот за заштита од пожари ги бираше противпожарните системи и го планираше системот за евакуација.

За разлика од тогаш, денес сме сведоци дека истата технологија која послужи за развој на компјутерските мрежи и интернетот се користи да се креираат напредни интегрирани безбедносни системи.

Значи кога зборуваме за интегрирани безбедносни системи, мислиме на повеќе видови на уреди за заштита кои се споени во еден систем и функционираат заедно, видео надзор, аларми, контрола на пристап, ПП заштита и следење на стоки, се преку една мрежа. Главната цел на интегрирањето е да се намали времето на реакција на обезбедувањето кои ги контролира сите системи преку еден контролен уред, најчесто компјутер и да се зголеми степенот на обезбедување на објектот. За оваа цел, потребно беше и креирање на нов софтвер кој има можност сите овие уреди да ги следи во исто време и да јавува навремено и брзо за евентуални опасности.

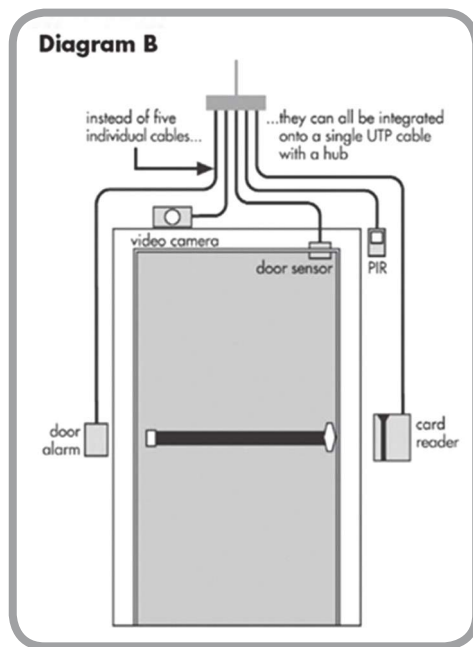
За полесно да се разбере интегрираниот безбедносен систем и неговата структура и зошто ни е потребен таков систем, ќе се осврнеме на следниве два диаграми:

- *Дијаграм А* - ни покажува шема на интегриран систем за обезбедување и неговата мрежа. За разлика од порано кога секој систем се инсталираше point-to-point сега може да забележиме дека сите безбедносни уреди се дел од една мрежа. Комуникацијата, камерите, ПП системи, контролата на пристап, се е поврзано преку еден HUB преку кој овие системи комуницираат со централната станица (компјутерот) и му овозможуваат на операторот истовремено да ги следи.



Слика 2.102. Шема на интегриран систем за обезбедување

- *Диаграм Б* - за разлика од претходно ни покажува како изгледа еден обичен безбедносен систем, пред интегрирањето. За пример ни е дадена врата, на која се поставени повеќе видови на безбедносни системи и од секој посебно оди инсталација до централната станица (компјутерот).



Слика 2.103. Шема на неинтегриран систем

Интегрираниот систем се ослободува од целата оваа непотребна (вишок) инсталација и користи еден кабел за комуникација со централната станица.

Интегрираните системи, многу потсетуваат на компјутерски мрежи затоа што ги користат истите мрежни протоколи. Во контекст на ова, мора да се спомене дека преносот на видео сигнал од системот за видео надзор преку компјутерска мрежа е најзаслужен за интегрирањето на безбедносните системи. Како систем кој најмногу црпи од сообраќајот на мрежата системот за видео надзор им даде иницијална идеја на компаниите кои развиваат безбедносни системи дека и останатите компоненти можат да го користат истиот протокол и начин на пренос. Дополнително олеснување беше и фактот што сите останати системи заедно без системот за видео надзор користат многу помалку сообраќај од компјутерската мрежа. Во реализација на нивната замисла за спојување на сите системи во еден, помогна и стандардизацијата на компјутерската инсталација и

на протоколите за пренос на податоци преку кабел како на пример TCP/IP протоколот, кој во денешно време го користат сите модерни системи за обезбедување.

За овој брз напредок на системите за видео надзор се исто така многу заслужни и мрежните рекордери, кои ги заменија старите видео рекордери на касети и кои овозможуваат на снимениот материјал да може да му се пристапи од било каде на локацијата на која се обезбедува, а доколку е рекордерот поврзан на интернет и од било каде во светот каде што има интернет пристап.

Развојот на интегрираните системи и нивниот брз напредок, направи возможно уште една технологија да се имплементира во системот, а тоа е биометричката идентификација за контрола на пристап. Биометричката идентификација, користи повеќе технологии, како на пример: отпечатоци од прсти, геометрија на дланка, препознавање на лик и препознавање на глас. Сите овие технологии во нивното користење, бараат голема база на податоци за споредба и многу брз трансфер на податоци преку инсталацијата на системот. Со компјутерските протоколи и со модерните компресии на звук и слика, овие системи се се повеќе достапни и трошоците за нивно инсталирање се многу помали за разлика од порано.

Иако има неколку индикации во која насока ќе се движат интегрираните системи за обезбедување во иднина, невозможно е да се предвиди што се корисниците или инженерите ќе посакаат и измислат. Сепак најважно од се е да се направи инфраструктура која ќе подржи брз пренос на податоци која ќе може да ги поддржи тие измени и сите нивни желби. Нема сомневање дека безбедносната мрежа паралелно ќе се развива со компјутерската мрежа и комплетната интеграција е само прашање на време.

2.8. МОНИТОРИНГ ЦЕНТРИ

Со појавата на интегрираните системи, зголемената побарувачка за обезбедување, како и потребата од создавање на центри за контрола и надзор на мерките за обезбедување, се отвори прашањето за создавање на еден вид на контролен центар кој би имал задача да врши 24/7 мониторирање на сите системи за техничко и физичко обезбедување.

За таа цел се создадени мониторинг центрите кои се организирани да функционираат непрекинато во текот на целата година, технички се опремени за следење на сите потребни системи.

Во рамки на мониторинг центрите работи персонал кој што одлично ги познава карактеристиките и процедурите на реагирање на сите системи кои се надгледуваат.



Слика 2.104. Мониторинг центар

ТЕОРЕТСКИ ДЕЛ

3

Скицирање и планирање на изведба и изведба на системи за техничко обезбедување

3.1. Стандарди **109**

- EN54 - Детекција на пожар и аларм на пожарен систем **109**
- EN50131 - Алармни системи, системи за напираници и задржување **113**
- EN50132 - CCTV системи за набљудување за употреба во сигурносни апликации **115**
- EN 50133 - Систем за контрола на пристап и користење на сигурносни апликации. **117**
- EN 50137 – Комбинирани односно интегрирани алармни системи **117**

3.2. Читање на техничка спецификација: **127**



3.1. СТАНДАРДИ

■ **EN54 - Детекција на пожар и аларм на пожарен систем**

- Стандардот EN54 за Детекција на пожар и аларм на пожарен систем е задолжителен стандард кој ги специфицира основните побарувања и лабораториски тестови за секоја компонента на системот за детекција и овозможува слободно движење на овие производи во земјите од европската унија. Овој стандард е донесен од Европскиот комитет за стандардизација (European Committee for Standardization CEN), освен земјите од Европска унија, овој стандард го препознаваат и земјите од Латинска Америка, Бразил, Африка и Азија.
- Целта на денешните организации за стандардизација е да промовираат сигурност, квалитет и техничка компатибилност за да се создаде основна инфраструктура за да се поткрепи општеството. Со други зборови, овој стандард ги промовира основните, минималните побарувања кои производителите и инженерите кои го осмислуваат овие системи, мора да ги исполнат. Производителите мора да бидат сигурни по здравјето на луѓето и околината каде што ќе бидат монтирани.
- Само оние производи кои имаат EN54 стандард може да добијат CE сертификат, институцијата што ќе сертифицира, мора да биде акредитирана од ЕАБ (се врши тест, контрола, па сертификација).
- Стандардот EN54 има 27 потточки каде што се специфицирани основните потреби што треба да ги исполнува системот:
 - EN 54 дел 1 Детекција на пожар и аларм пожарен систем. Вовед;
 - EN 54 дел 2 Детекција на пожар и аларм пожарен систем. Контролни панели и индикатори.
 - EN 54 дел 3 Детекција на пожар и аларм пожарен систем. Уреди за аларм. Сирени;
 - EN 54 дел 4 Детекција на пожар и аларм пожарен систем. Напојување;
 - EN 54 дел 5 Детекција на пожар и аларм пожарен систем. Термички детектори
 - EN 54 дел 6а Детекција на пожар и аларм пожарен систем. Термички детектори; Термо-диференцијални детектори
 - EN 54 дел 7 Детекција на пожар и аларм пожарен систем. Детектори на чад. Детектори кои користат распрскана светлина, емитувана светлина или јонизација;

- EN 54 дел 8 Компоненти за автоматска детекција на пожар. Спецификација за детектори на висока температура;
- EN 54 дел 9 Компоненти за автоматска детекција на пожар. Методи за тестирање на осетливоста на пожар;
- EN 54 дел 10 Детекција на пожар и аларм пожарен систем. Детектор на пламен;
- EN 54 дел 11 Детекција на пожар и аларм пожарен систем. Рачни дојавувачи на пожар;
- EN 54 дел 12 Детекција на пожар и аларм пожарен систем. Детектори на чад. Линиски детектори кои користат оптички зрак, бим детектори;
- EN 54 дел 13 Детекција на пожар и аларм пожарен систем. Проценка на компатибилноста на компонентите во системот;
- EN 54 дел 14 Детекција на пожар и аларм пожарен систем. Планирање, дизајнирање, инсталација, Planning, design, installation, пуштање во употреба, користење и негово одржување;
- EN 54 дел 15 Детекција на пожар и аларм пожарен систем. Комбинирани детектори;
- EN 54 дел 16 Детекција на пожар и аларм пожарен систем. Компоненти за гласовна дојава на пожар. Контролна плочка за гласовна дојава и индикатори;
- EN 54 дел 17 Детекција на пожар и аларм пожарен систем. Изолатори за кратка врска;
- EN 54 дел 18 Детекција на пожар и аларм пожарен систем. Влезно/излезни уреди;
- EN 54 дел 20 Детекција на пожар и аларм пожарен систем. Аспираторски детектори на чад;
- EN 54 дел 21 Детекција на пожар и аларм пожарен систем. Опрема за трансмисија на аларм и лажни предупредувања;
- EN 54 дел 22 Детекција на пожар и аларм пожарен систем. Линиски температурни детектори;
- EN 54 дел 23 Детекција на пожар и аларм пожарен систем. Пожарни алармни уреди. Визуелни дојави;
- EN 54 дел 24 Детекција на пожар и аларм пожарен систем. Гласовен аларм- Озвучување
- EN 54 дел 25 Детекција на пожар и аларм пожарен систем. Компоненти кои користат радио врска и нивни побарувања;
- EN 54 дел 26 Детекција на пожар и аларм пожарен систем. Детектори на CO;
- EN 54 дел 27 Детекција на пожар и аларм пожарен систем. Детектори на прав;

Системот за пожар се состои од детекција на пожар и звучна и гласовна дојава на пожар.

Системи за детекција на пожар

- Системите за детекција на пожар начелно се делат на две групи и тоа: конвенционални и адресабилни. Клучната разлика меѓу овие два системи е што кај конвенционалните системи централата – контролниот панел ги прима дојавувањата од сензорите по зони, и кога ќе детектира пожар дојавува во која зона е пожарот – со што не овозможува брло лоцирање, додека кај адресабилните системи, секој уред е адресиран посебно, кога ќе избие пожар се знае точно кој уред детектирал пожар и овозможува брзо локализирање на пожарот.
- Постојат неколку типа на детектори на пожар (без разлика дали се конвенционални или адресабилни):
 - Термички детектори – кога ќе се постигне некоја фиксна температура
 - Термодиференцијални – кога ќе се направи нагло температурна раслика
 - Детектори на чад – јонизирачки – имаат мала количина на радиоактивен материјал, чие зрачење поминува низ јонизирана комора исполнета со воздух меѓу две електроди низ која тече постојана струја. Чадот кој влегува во комората, абсорбира алфа честички со што се намалува јонизацијата и се активира аларм.
 - Детектори на чад – димнооптички – со помош на фотокелии и извор на светлина, кога чад ќе го прекине зракот, дојавува пожар
 - Детектори на чад – јонизирачки и димнооптички – комбинација на двете техники
 - Детектори за чад - Бим детектори
 - Детектори за чад – аспиратори
 - Детектори на CO
 - Детектори на CO₂
 - Детектори на течен гас LPG
 - Комбинирани детектори
- Фирмата која ќе го работи системот, треба да ги испланира детекторите во зависнос од просторот и потребите. Термичките детектори поспоро детектираат пожар и затоа се предвидени за помали простории каде температурата нагло би се зголемила, но не и за големи и високи простории, додека димнооптичките детектори побрзо детектираат пожар и се предвидени за големи простории.

Препорачани детектори во разликни простории								
	Јонизирачки Детектор за чад	Фотоелектричен Детектор за чад	Праволиниски бим детектори	Аспираторски детектори	СО детектори	Термички детектори со фиксна температура	Термодиференѝјални детектори	Детектори на пламен
Спални/простории за спиене	√	√	ок	ок	√	ок	ок	ок
Канцеларии/продавници	√	√	ок	ок	√	√	ок	ок
Театри/клубови (вештачки чад)	х	х	х	х	√	√	ок	ок
Купатила/перални	х	х	х	х	ок	√	х	ок
Соби со котли/бојлери	х	х	х	х	х	√	х	х
Паркинг простории	х	х	ок	х	хх	√	√	ок
Кровови и покриви со пристап	ок	ок	ок	ок	ок	√	ок	ок
Кровови и покриви до тежок ористап	х	х	ок	ок	х	√	ок	ок
Ладилници/фрижидери ¹	х	х	х	ок	х	ок	√	ок
Простории со електроника	√	√√	х	ок	х	√	ок	ок
Електрична табла/рак ормари	√	√√	ок	ок	х	√	ок	ок
Области со запаливи течности	√√	√	ок	ок	х	√	ок	√
Високи и тешко достапни плафони	ок	ок	√√	√	√	ок	ок	ок
Кујни	х	х	х	х	ок	√	ок	ок
Фарбари	х	х	х	х	х	√	ок	ок

Легенда: √√ - многу препорачливо; √ - препорачливо; ок - може да биде добро;
х - не е препорачливо; хх - не се користи;

¹ напомена: во големи ладилници доста тешко е да се постави обичен детектор,
најчесто ваквите простории треба специјално дизајнирани детектори со грејачи
кои ќе го заштитуваат детекторот од мрзнење, истото важи и за рачните јавувачи
и сирени.

Системи за звучна и гласовна дојава на пожар

- Дојавата на пожар може да биде звучно преку алармни сирени кои имаат специфичен тип на звук, или преку гласовна дојава и гласовно упатство за евакуација на затекнатите во пожарот.
 - Европската комора за сертификација го претпочита гласовното дојавување на пожар, кое овозможува насочена евакуација, за разлика од звучната дојава која само сигнализира пожар и ствара паника кај луѓето затекнати во пожар.
 - Побарувањата за гласовната дојава се објаснети во делот 24 од овој стандард. Тука се дефинирани побарувањата, методите на тестирање и перформансите на системот за озвучување.
 - Во европски рамки, системот на гласовна дојава и евакуација се централизира во рамки на една установа, која води евиденција за дојавите и ја организира евакуацијата преку централно озвучување.
- **EN50131 - Алармни системи, системи за најблицници и задржување**
- Начелно овој стандард е донесен за да се заменат британските стандарди BS4737, BS7042 и BS6799.
 - Овој стандард како и останатите ги определува минималните карактеристики, перформанси и тест методи што треба да ги поседуваат производителите. Стандардот ги утврдува побарувањата и критериумите на системот како и дизајнот на опремата. Овој сертификат подразбира правење на сеопфатна проценка на ризикот пред дизајнирање на производот и системот. Овој сертификат е применлив и на жичаните и на безжичните алармни системи. Отценување на системот, креирање на степен од 1 до 4 е за да се предвиди ризикот на провала.
 - Проценка на ризикот – едно од најзначајните прашања кај овој стандард, е проценувањето на висината на ризикот поврзан со објектот каде се инсталира системот и негово оценување. Штом еднаш еден систем ќе добие степен за ризик, автоматски се дефинира и потребата од сигнализација и тригерирање на алармниот систем.
 - Безбедносни оценки или степен на ризик – еден од најважните аспекти на побарувањата на EN50131 стандардот е концептот за отценување на сигурноста на системот. За секоја инсталација треба да биде одреден степенот на сигурност разгледувајќи низа фактори. Во EN стандардот, оценките/степенот се опишани според видот на натрапникот и колку труд би вложил натрапникот за да изврши провала.

СТЕПЕН 1: Објекти со низок степен на ризик за кражба, имотот не привлекува натрапници, се претпоставува дека крадецот нема да креира план за провала во ваков објет, и дирекно би извршил провала. Се претпоставува дека крадоцот би провалил и отворена врата.

СТЕПЕН 2: Објекти со малку повисок степен на ризик од кражба. Имотот може да привлече искусен крадец. Во овој случај се очекува натрапникот да има извесни познавања за тоа како работат алармните системи и можеби носат некоја опрема која ќе овозможи да се сруши основен алармен систем. Крадецот би ја проверил достапноста на вратите, прозорите и други можни пристапи.

СТЕПЕН 3: Објекти со значителен ризик за кражба, имотот на прв поглед дава впечаток дека содржи предмети од висока вредност и се очекуваат провалници. Крадецот најверојатно ќе проба да најде пристап преку прозорци, врати или други места, крадецот може да биде доста искусен со алармни системи и да поседува доста опрема за онеспособување на алармен систем.

СТЕПЕН 4: Објекти со многу висок ризик за кражба, големината на имотот ги покажува вредностите на прв поглед. Се претпоставува дека натрапниците однапред направиле план за провала, ги знаат сите влезови и излези, имаат опрема за менување на делови на алармниот систем со што би го онеспособиле системот и да спречат негова дојава. Се претпоставува дека натрапникот би пробал да влезе преку сидови, подови и тавани. Малку веројатно е натрапникот да работи сам.

- Кој степен на ризик е постоечката инсталација? Ова е најчесто поставувано прашање при инсталција на еден систем, и е доста комплексно прашање, на кое не може да се даде брз и краток одговор, и мислењата на ова прашање може да варираат од земја во земја. Велика Британија има најстрога проценка на ризикот, ако една продавница во Белгија би се класифицирала во 2 степен, во Велика Британија би била во 3 степен. Начелно степенот на ризик би требало да го наметнува осигурителната компанијата. Типичен пример за оформување на степен може да биде:
 - СТЕПЕН 1: приватни мали имоти
 - СТЕПЕН 2: приватни имоти и ниско ризични компании како цвеќари
 - СТЕПЕН 3: висок ризик на приватни имоти и повеќето компании (трафики, колонијални продавници, продавници за облека)
 - СТЕПЕН 4: екстремно висок ризик на приватни имоти и и висок ризик на деловни простории (златари, музеи)
- Алармните системи може да бидат жичани или безжични. Без разлика за кој тип станува збор, еден систем за детекција на провала и негова дојава се состои од следните компоненти:

- Контролен панел – кој ги прибира сите информации од детекторите, централата може да има телефонска дојава за да испраќа говорна порака директно до клиентот, или да дојавува на мониторинг станица на агенција за обезбедување;
- Детектори на движење: пир детектори, детектори кои не детектираат животни до 18кг/40кг, детектор завеса, детектор 360°, праволиниски детектори, бим детектори, постојат посебни детектори кои се монтираат во надворешни услови и други за внатрешни.
- Вибро детектори: реагираат на вибрации, најчесто се поставуваат во сефови, банкомати.
- Тастатура за конекција со централата: тастатурата овозможува активација и деактивација на системот со код кој ќе го знае само сопственикот;
- Сирени: надворешни или внатрешни, сирените не смеат да бидат со јачина повеќе од 110dB на растојание од 1m;
- Кои уреди ќе се искористат за еден систем зависи од просторот и од ризикот за провала на просторот.
- До алармните системи може да се пристапува преку интернет со одредена апликација направена од производителот на опремата, со што на корисникот му овозможува активација/деактивација и контрола на системот од било каде, дури и преку паметен телефон.

■ **EN50132 - CCTV системи за набљудување за употреба во сигурносни апликации**

- Целта на овој стандард е да обезбеди насоки за CCTV системите, и да се осигура дека неговата функционалност и перформанси се целосно исполнети според барањата.
- Овој стандард е корисен за оние кои се одговорни за воспоставување на оперативни барања, пишување на спецификации, инсталирање, пуштање на системи во работа, користење и нивно одржување.
- CCTV системите, во својот наједноставен облик значи креирање на слики преку камера за нејзино гледање на телевизор преку приватен систем за пренос на податоци.
- Теоретски не постои лимит колку камери може да се постават на еден објект, но во пракса може да сме ограничени од ефикасноста и истовремениот преглед, и нивна контрола од страна на операторот.
- Успешен систем подразбира активна соработка со корисникот при спроведување на препорачаните процедури.
- Главните цели на овој систем се:

- Да им обезбеди водечка рамка на корисниците , инсталатерите и производителите при креирање на системите;
- Да им помогне на корисниците и креаторите на спецификации во утврдување на соодветна опрема која е потребна за одредени ситуации;
- Да обезбеди објективно оценување на инсталиран систем;
- За безбедносниот систем да биде ефикасен и да ги задоволи барањата и на клиентот и барањата утврдени од осигурителните компании, треба да биде инсталиран согласно со барањата на стандардот, а тоа може да го овозможи само професионална компанија.
- Овој стандард го воведува општите услови за видео пренос. Детална спецификација на аналоген пренос преку различни медиуми е дефиниран во EN 50132-5-3. За безбедносните системи базирани врз IP технологија, перформансите и побарувањата се дефинирани во два стандарди. Овој стандард во својата клаузула ги опфаќа општите услови за видео пренос, перформансите и основните побарувања за IP сигналот врз основа на светски познати стандарди. Во области каде има подетални побарувања за IP конекцијата се даваат дополнителни спецификации за да се постигне компатибилност со побарувањето. Европскиот стандард нема детали и специјални CCTV протоколи. Во дел 2 од овој стандард се дефинираат IP протоколите за целосна интероперабилност (PTZ контрола, настани..). Дел 1 од овој стандард ги дефинира минималните барања за изведба на еден IP видео систем
- Овој систем дава препораки за избор, планирање и инсталација на CCTV систем.
- Системот за видео надзор може да биде составен од аналогни камери и уреди за снимање, или дигитален со IP камери и мрежни видео рекордер, исто така постои и можност за комбинација на овие два системи во еден, со што самиот дигитален видео рекордер ќе биде комбиниран и на него ќе може да се поврзат аналогни и IP камери истовремено.
- Еден систем за видео надзор без разлика дали е аналоген или IP, тој се состои од:
 - камери: дневни, ден/ноќ (со IR или ден/ноќ чип), и тие може да бидат камери за внатрешна монтажа и камери за надворешна монтажа;
 - видео рекордер;
 - монитор и
 - помошна опрема како напојувања, конектори, кабли

- Како ќе изгледа системот за видео надзор зависи од просторот и побарувањата на клиентот. Во согласност со барањата на клиентот, вклучувајќи го и законот за заштита на личните податоци се прави план за изработка на систем за видео надзор.

- **EN 50133 - Систем за контрола на пристап и користење на сигурносни апликации.**
 - Овој стандард ги опишува општите барања и функционалности на системите за контрола на пристап при употреба за безбедносни потреби.
 - Исто така ги опишува општите барања и еколошки побарувања.
 - Кога дел од системот за контрола на пристап е дел од алармен систем (дури и заеднички интерфејс) системот треба да ги исполнува двата стандарди и за контрола на пристап и за аларми системи за детекција на провала.
 - Овој стандард се однесува за секоја пристапна точка од системот за контрола на пристап, а тој може да има многу точки, и сите да имаат различно ниво на пристап.
 - Овој стандард ја специфицира структурата и основните побарувања на системот за контрола на пристап, основните функционалности, дефинирање на побарувањата согласно животната средина и електромагнетното зрачење.
 - Системот за контрола на пристап се состои од:
 - уреди за отчитување на картички, кодови, отисоци, препознавање на ликови;
 - Уреди за отворање на врати – електрични брави, магнети, болтови
 - Уреди за напојување
 - Уреди за непрекинато напојување
 - Мрежна опрема
 - Софтвер за контрола на пристап.

- **EN 50137 – Комбинирани односно интегрирани алармни системи**
 - Овој стандард претставува спој на стандардот за алармни системи и CCTV системи, доколку еден безбедносен систем се состои од алармен систем и CCTV систем интегриран во еден, треба да ги земе во предвид правилата и прописите предвидени од овој стандард.

Скицирање и планирање на системи:

Скицирање и планирање на пожарен систем.

- Пред да се започне со монтажа на еден противпожарен систем потребно е да се обезбеди скица на објектот според која ќе се изработи план за работа и инсталација на опремата. Според направениот увид и скицата се специфицира системот за детекција на пожар. Се утврдуваат просториите каде што мора да се постават детектори, во зависност од типот на просториите ги дефинираме и типовите на детекторите кои соодветно ќе бидат поставени. Начелно правило е дека термички детектори се поставуваат во мали простории каде брзо и нагло може да дојде до покачување на температурата, во спротивно треба да се постави димнооптички или јонизирачки детектор за чад кој има побрза реакција од термичкиот детектор. Како што може да се погледне и во табелата дадена погоре:
- во простории каде што се спие препорачливо е да се стават детектори за чад, помалку препорачливо е детектор за температура;
- во кујни препорачливо е да се стави температурен детектор со фиксна температура, може како дополна да има LPG и CO детектор, но не треба да се поставуваат детектори на чад (било јонизирачки или оптички) заради тоа што овие простории се прави доста пареа па дури и чад и такви детектори би правеле доста лажни дојави;
 - во простории каде што има котли за парна, бојлери – се препорачуваат исто така термички сензори со фиксна температура;
 - во купатила и перални препорачливо е да термички сензори, а не е препорачливо детектори на чад;
 - во простории каде што има можност за запаливост на течни материи, силно се препорачува да се стават јонизирачки детектори на чад, може да се стават и термички детектори но не се препорачува CO детектори;
 - во канцеларии, продавници, соби за престој препорачливо е да се стават детектори за чад, како и детектори за температура, на вакви места може да се постават и комбинирани детектори кои ги имаат двете технологии во себе;
 - во простории каде има електрични апарати, рутери, електрични табли многу препорачливо е да се постави оптички детектор наместо јонизирачки, не е препорачливо да се користат бимови и CO детектори во вакви простории;
 - во паркинг простории не се препорачува детектори за чад, аспираторни детектори, никако CO детектори, во вакви простории

препорачливо е да се стават термички детектори со фиксна температура или термодиференцијални;

- на високи тавани со тешка пристапност не се препорачуваат детектори за чад, туку праволиниски бим детектори или аспираторски детектори;
- во големи адила иници тешко е да се постават обични детектори, треба да се постават специјално дизајнирани термодиференцијални детектори кои ќе имаат грејачи како превенција од замрзнување;
- во клубови, кина, театри каде има доста вештачки чад се препорачуваат термички детектори или термодиференцијални, но не и детектори на чад кои би предизвикувале лажни дојави;
- простории со високи тешко достапни тавани се препорачува да се постават праволиниски бим детектори;

Еден детектор за чад или термички детектор препорачливо е да се постави на $30m^2$, на висина од максимум 5m.

Кога ќе се предвидат детекторите, се проверуваат сите излези на објектот и тука се предвидуваат рачните јавувачи, кога некој ќе забележи пожар веднаш да прати дојава до централата преку рачните јавувачи. Исто така на секој излез се предвидува светлосна сигнализација со знак за насочен излез.

По дефинирање на детекторите и рачните јавувачи, се планира звучната сигнализација на објектот. Освен звучните сирени кои се поставуваат и внатре и надвор од објектот, според европските стандарди, за поголемите објекти препорачливо е да се инсталира и гласовна дојава за пожар. Гласовната дојава за пожар подразбира озвучување на целиот објект, и при пожар ќе се емитира снимена порака за евакуација или доколку системот за пожар е поврзан со централна установа, евакуацијата ќе се врши од страна на установата.

Гласовна дојава на пожар е поефикасна од звучната дојава, затоа што е насочувачка и смирувачка, таа не предизвикува паника, треба да ги смири учесниците во пожарот, и да ги насочи по најкраткиот начин кон излезот.

Доколку се работи за мал систем, се предвидуваат конвенционални системи, во спротивно за големи објекти, со многу детектори се предвидуваат адресабилни системи.

- Конвенционалните системи се постар модел на уреди за детекција на пожар. Детекторите се организираат во зони, при што на една зона може да се постават повеќе детектори, при што најчесто на една зона се поставуваат детектори кои припаѓаат на една просторија за полесно дефинирања и локализирање на пожарот. Конвенционалните центри не може да локализираат кој уред

детектирал пожар, дојавува само во која зона е детектиран пожарот, затоа препорачливи се само за мали објекти, и тоа што помалце детектори одат во една зона тоа е подобро за локализација.

- Адресабилните детектори се препорачливи за поголеми системи. Кај овие контролни панели сите уреди поврзани на системот – детектори, рачни јавувачи, сирени, имаат своја адреса. Што значи кога некој уред ќе детектира пожар, системот веднаш знае од каде дошла таа дојава и веднаш го лоцира уредот и просторијата каде се наоѓа тој. Постојат апликации каде на мапа се обележуваат сите дојавувачи, и штом се направи дојава веднаш се појавува на мапата каде постои проблемот и може да се почне со проверка и евакуација ако е шптрбно.

Штом се утврди за каков систем станува збор, дали е мал или голем, со што се одговара на прашањето кој тип на систем ќе се инсталира, се исцртуваат уредите на скицата и се предвидува каблирањето. Системите за пожар користат тешкогоречки кабел 2x0,8 или 2x2x0,8. При што кај адресабилните детектрои се пушта една јамка (или повеќе во зависност од големината на системот/контролниот панел) и на таа јамка се адресираат сите уреди (детектори, јавувачи, сирени), додека кај конвенционалните детекторите и јавувачите се пуштаат по кабел во зони, а сирените се поврзуваат преку посебен кабел до централта. Во зависност од централата, адресабилните системи на една јамка може да се поврзат околу 250 уреди за разлика од конвенционалните каде на една зона не се препорачува повеќе од 10 детектори.

Поврзувањете на детекторите оди сервиски, влез/излез во детектор па влез на зона на конвенционална централа или влез во јамка кај адресабилна централа.

- По дефинирање на типот на централата, точките за инсталација на опремата, местото каде ќе биде поставена централа, се започнува со каблирање. Кабелот секогаш треба да се бележи при каблирање за подоцна полесно да се најде кој кабел за која зона е предвиден.
- Се поставуваат детекторите, рачните јавувачи, сирените, светлечките насочувачи за излез, кај адресабилните системи се забележуваат адресите на уредите за подоцна да можат да се стават на мапа, додека централата може сама да ги препознае. Во одредени случаи во зависност од типот на детекторите, може да биде потребен и програматор за програмирање на адресабилните уреди.
- По поставување на опремата, се тестира секој сензор пооделно со специјални тестери на детектори, дали се исправни. Потоа се поврзува целиот систем и повторно се врши тестирање на целиот систем.

- До секој излез и рачен јавувач треба да се постави мапа и план за евакуација.
- По завршеток на инсталацијата на системот, на корисникот треба да му се издаде документ за стандардна процедура за користење на системот. Што треба да содржи тој документ:
 - Каков тип на систем е инсталиран, адресабилен или конвенционален и што подразбира тоа.
 - Точниот модел на централата, каде се наоѓа, во која просторија.
 - Кој тип на детектори се користат, во која просторија кој тип е поставен.
 - Од што се состои системот: најчесто детекција, иницирање и уред за мониторирање, краток опис на системот.
 - На колку време мора да се прави проверка на системот (зависи од препораките на производителот), најчесто системот треба да биде чистен и тестиран на секои 3 до 6 месеци.
 - Упатство како се чистат детекторите – за секој тип одделно.
 - Тестирање на целиот систем на секои 3-6 месеци.
 - Тестирање на детектори во високоризични простории на секои 1-2 месеци.
 - Системот препорачливо е да се тестира од обучен сертифициран кадар.
 - Треба да содржи скица со точна локација на секој уред од системот.
 - Доколку има потреба може да се изработи електронска скица која може да се поврзе со програма за лоцирање на проблеми, детекција на пожар и евакуација.

Скицирање и планирање на алармен систем.

- Исто како и за било кој безбедносен систем, и за алармните системи се започнува со проверка и утврдување на состојбата на објектот каде треба да се инсталира системот.
- Се прави проценка од кој степен на загрозеност или кој степен на ризик го има објектот. Како што беше кажано и погоре, според Европска унија постојат четири нивоа или групи на ризик.
 - Во првиот степен на ризик спаѓаат мали приватни домови, кои не се привлечни за професионални крадци, туку најчесто се работи за непрофесионални натрапници кои нема да пробаат да го инеспособат системот, па затоа се поставува алармен систем без некои специфичности и се зачитуваат најчесто вратите и прозорците. Со што голема е веројатноста дека ќе се спречи крадецот да влезе во објектот.

- Во втората група на ризик спаѓаат поголеми имоти и деловни објекти кои може да привлечат внимание кај полупрофесионални крадци. Тука спаѓаат продавници кои не се високопрофитни како цвеќари, туристички агенции, фризерници, козметички студиа. Тука се претпоставува дека крадецот има мали познавања од системите за безбедност и ќе биде внимателен при провалувањето, крадецот би ја проверил достапноста на вратите. Во вакви ситуации треба да бидеме повнимателни со системот.
 - Во третата групаспаѓаат приватни имоти со висок ризик и повеќето компании (трафики, колонијални продавници, продавници за облека) се претпоставува дека крадецот има доста познавања на системот, треба да се внимава на поставувањето на каблите, да не може да се дојде до нивно сечење, секое отстранување на уред, да се прати дојава до централа и мониторинг станица.
 - Четвртата група е високо ризична, тука спаѓаат имоти кои привлекуваат професионални натрапници, кои може да носат уреди и алати за сечење стакло, исто така уреди за влегување преку сид, таван, или под. Во вакви случаи мора да се вклучат и други типови на детектори освен основните, како детектор на вибрации, бим детектори и др.
- По наравената проценка се скицира просторот, се дефинираат ризичните позиции од каде може да влезе натрапникот. За мали системи се заштитуваат само вратите, и прозорците доколку се достапни без крадецот да вложи премногу труд. Високоризичните објекти се заштитуваат од сите можни пристапи, врати, прозорци, таван, подрум, кров иако се работи за навидум недостапни места, на ваквите објекти крадците се доста обучени за работата на системот и имаат алат кој може да го онеспособи системот.
 - Централата се поставува на нестостапно место, далеку од влезот, додека тастатурата за активација и деактивација се поставува до самиот влез.
 - Алармните системи може да бидат жичани или безжични. Доколку се жичани, прва фаза во инсталацијата и положување на каблите. Кабел се поставува од централата до секој детектор, како и до уредите за звучна сигнализација. Сензорите во централата се распределуваат во зони, најдобро една зона да претставува една просторија, за да може најдобро да се специфицира местото каде е направена провала.
 - Штом се дефинира системот, се почнува со инсталација на кабелот, алармните системи користат сигнален кабел 6x0,22. Кабелот се пушта од централата до секој сензор, како и до сирените.
 - Се препорачува кај секој сензор да се поврзе и тамперот, кој при било каков обид за негово отстранување ќе изврши дојава до централа.

Тамперот многу често не се поврзува од страна на инсталатерите што претставува голем недостаток на системот.

- Звучната сигнализација или сирените, исто така треба да бидат поврзани на тампер, за при било каков обид за отстранување да дадат дојава до централа.
- По поврзувањето на системот, се врши негово програмирање и сетирање.
- Системот при провала има или може да се дополни со уред за дојава на провала може да дојавува директно кај клиентот, со говорна порака или SMS, исто така препорачливо е системот да биде поврзан на централен мониторинг систем во некоја агенција која може понуди брза реакција на терен.
- На крајот на инсталацијата треба да се промени кодот за пристап, и да се доделат кодови кои ќе бидат познати само за корисниците.
- За ваквите системи не се препорачува да се прави скица и локализација на детекторите заради заштита да дојде во допир со крадците.

Скицирање и планирање на CCTV систем

- Инсталација на системот за видео надзор започнува со увид на објектот и разгледување на барањата на клиентите. Со што се прави скица на објектот.
- Како што веќе нагласивме и претходно, постојат два типа на системи за видео надзор. Едниот со аналогни уреди, а вториот со IP уреди.
- Доколку системот треба да се изработува со аналогни камери, ги разгледуваме позициите за монтажа на камерите и се предвидуваат најсоодветните аналогни камери според просторот. Најбитен фактор кој го загрозува квалитетот на камерите е директната светлина. Затоа камерите треба да се постават на начин што осветлувањето нема да ја попречува камерата да ги покаже своите најдобри перформанси.
- За надвор се предвидуваат заштитени камери или куќишта за камери, кои за надворешни услови мора да го поддржуваат IP55 или IP65 стандардот кој овозможува заштита од вода и прашина во надворешни услови.
- Во зависност од потребите камерите може да бидат дневни, или комбинирани ден/ноќ со што се овозможува видео снимка и во минимално осветлување.
- Внатрешните камери исто така може да бидат дневни или ден/ноќ.

- По дефинирање на типовите на камери кои ќе се користат, а воедно и дефинирања на позициите на камерите, се пристапува кон инсталација на кабелот.
- Системот за видео надзор со аналогни камери користи видео кабел RG59. Кабелот треба да се инсталира од секоја камера до влезот на дигиталниот видео рекордер.
- Според бројот на камерите се поставува соодветен дигитален видео рекордер.
- Доколку се работи за IP камери, системот се поврзува со мрежен кабел UTP/FTP/SFTP во зависност од условите каде се поставува.
- Поделбата и на IP камерите е иста како и кај аналогните, во зависност од просторот, аголот кој треба да се опфати, се одредува типот на IP камерата.
- По положување на кабелот, се пристапува кон монтажа на камерите, нивно поврзување преку конектори со кабелот, а воедно и со дигиталниот видео рекордер.
- Камерите се поврзуваат на напојна единица
- Како заштита, се препорачува да се стави уред за непрекинато напојување, со што доколку дојде до прекин на струјата, уредот за непрекинато напојување ќе ја превземе работата на системот.
- Се проверуваат аглите на гледање, дали го задоволуваат барањето на клиентот.
- Без разлика дали се работи за систем со аналогни камери или систем со IP камери постои можност за неково следење преку интернет. Со подесување на IP адресата (која се препорачува да биде фиксна) може да се овозможи пристап со системот од било кое место преку интернет, дури постојат апликации за преглед и следење на системот преку мобилен телефон.
- Системот за видео надзор мора да биде поставен во согласност со законот за заштита на лични податоци.
- Снимките од системот се сопственост на контролорот и смеат најмногу да се чуваат во период од 30 дена, освен ако со некој друг закон не се бара поинаку.
- Според законот за заштита на лични податоци, мора да се направи скица за позицијата на камерите, точниот агол кој го покриваат камерите треба да биде исцтан на скица, да се даде објаснување зошто се поставени на таа позиција и да се гарантира дека не ја загрозуваат приватноста на другите учесници.
- Според законот за заштита на лични податоци, корисникот на системот (доколку се работи за јавна површина – а тоа е се останато освен

домот) е должен да постави знак дека системот е под видео надзор, да го назначи конторлорот (оној што има пристап во снимките) и да истакне телефон за контакт доколку се појави потреба од увид во снимките.

Скицирање и планирање на систем за контрола на пристап

- Системот за контрола на пристап може да зависи од степенот на сигурност што треба да го овозможи.
- Доколку се работи за низок степен на заштита може да се постават читачи на картички или уреди за пристап со внесување на четири или шест цифрен код. Кај овој тип на читачи се внесува одреден број на картички или кодови кои ќе имаат пристап во системот и се додека поминува картичка или код внесен во читачот, тој ќе ја отвора вратата, во спротивно ќе даде порака дека пристапот не е одобрен.
- За повисок степен на заштита се користат уреди за контролана пристап со отисоци на прсти. Кај овие читачи се прави база со отисоци од прсти, во зависност од уредот може да скенира и повеќе прсти на една рака, и според тоа да бара таква авторизација при пристап.
- За највисок степен на заштита се користат уреди за контрола на пристап со детекција/препознавање на лик. Овој тип на читачи меморира клучни точки од лицето на корисникот и ги запишува во база. Доколку тие информации ги нема во база нема да биде дозволен пристап.
- Уредите за контрола на пристап се поврзуваат со мрежен кабел.
- Самите уреди може да бидат мрежни и да се поврзат директно на компјутер, или да мора да се поврзат со дополнителен мрежен уред.
- Преку локалната мрежа може да се поврзат и читачите за контрола на пристап и да се поврзат со специјализиран софтвер за евиденција и преглед на пристапот.
- Преку софтверот може да се додаваат или одземаат привилегии на одредени корисници, во реално време да се има преглед кој корисник во која просторија се наоѓа, колку време се задржал.
- Читачите за контрола на пристап се монтираат до вратата каде што треба да се овозможи пристап или забрана на одредени корисници.
- Вратата мора да поседува специјална електрична брава, електричен болт или електричен магнет, кој ќе се отвора само во оној момент која читачот ќе даде дозвола за пристап.
- Важно за овој систем е дека мора да се обезбеди резервно напојување – непрекинато напојување, во случај да дојде до прекин на струјата, системот да продолжи да работи.

- Доколку системот е изграден врз врати со електрична брава, доколку снеса струја вратата ќе биде заклучена се додека не дојде напон.
- Ова не е случај кај електричните магнети, тие работат дури се под напон, кога ќе дојде до прекин на струја, електричниот магнет се отвора и останува отворен се додека не дојде повторно до напон. Затоа не се препорачливи да се користат во системи каде нема да има предвидено дополнително уред за непрекинато напојување.
- Системите за контрола на пристап исто така се користат и како системи за евиденција на работно време
- Дали истиот систем ќе се користи и како евиденција на работно време зависи само од корисникот.
- Доколку се работи за високо сигурносни објекти, системот за контрола на пристап е одвоен од системот за евиденција на работно време иако истите читачи може да се користат и за двата системи.
- Еден систем за контрола на пристап може да се состои од повеќе читачи и сите да бидат со различен степен на сигурност.
- Во простории каде се бара висока сигурност се поставуваат уреди за препознавање на лица, додека во останатите простории само читачи на картички, и сето тоа е интегрирано во еден систем. Еден корисник на код/картичка може да има пристап во една просторија, додека во друга пристапот да и биде забранет.
- За да се зголеми сигурноста и на читачите кои користат картички или кодови може да се дополни системот со камера, па при секое отчукување на картичка или внесување на пин, да се прави слика од корисникот, и во систем таа слика да ја споредува со корисникот на картичка. Доколку има несогласувања да даде аларм до систем администраторот дека има неправилен влез.
- Софтверот за евиденција исто така овозможува правење запис на слика при секое отчукување на картичката, со тоа што мора да се земе во предвид дека ваков систем би требало да биде поставен на сервер кој ќе има поголема меморија за запис, сликите нема да се чуваат во читачот туку во база на серверот.

3.2. ЧИТАЊЕ НА ТЕХНИЧКА СПЕЦИФИКАЦИЈА:

Детекција на пожар и аларм на пожарен систем

■ Легенда:

-  - Детектор за детекција на пожар
-  - Рачни јавувачи
-  - Внатрешна сирена
-  - Надворешна сирена
-  - Против пожарна централа – контролен панел

Алармни системи, системи за најрајници и задржување

■ Легенда:

-  - Детектор за детекција на движење
-  - Внатрешна алармна сирена
-  - Надворешна алармна сирена
-  - Контролен панел – централа за детекција на провала
-  - Тастатура

CCTV сисѝеми за набљудување за уѝойѝреба во сигурносни аѝликации

■ Легенда:



- Камера за видео надзор



- Дигитален видео рекордер



- Рутер

Сисѝем за контрола на ѝрисѝай и корисѝење на сигурносни аѝликации

■ Легенда:



- Читач на картички



- Помошен читач



- Електрична брава



- Електричен магнет



- Тастер за излез



- Сервер соба / софтвер

4

ТЕОРЕТСКИ ДЕЛ

Закон за приватно обезбедување

-
- 4.1. Видови на приватно обезбедување **131**
- 4.2. Основни услови за физичко лице за вршење на приватно обезбедување (лиценца и легитимација за обезбедување) **135**
- 4.3. Вршење на техничко обезбедување **138**
- 4.4. Запирки на приватност и известување за вршење на видеонадзорот **139**
- 4.5. Квалификации и исправности на техничките средства и уреди **140**
- 4.6. Легитимирање на работниците за приватно обезбедување **141**
- 4.7. Поступување по наредба **142**
- 4.8. Работна облека и ознака на работниците за приватно обезбедување **142**
- 4.9. Прекршочни одредби **143**



Законот за приватно обезбедување е донесен од Собранието на Република Македонија на седницата одржана на 24 декември 2012 година, а објавен е во Службен весник на Република Македонија бр. 166 од 2012 година. Овој Закон влезе во сила осмиот ден од денот на објавувањето во „Службен весник на Република Македонија“ а започна да се применува по шест месеци од денот на неговото влегување во сила, односно од 03.07.2013 година.

Со денот на започнувањето на примената на овој закон, односно од 03.07.2013 година, престана да важи Законот за обезбедување на лица и имот.

Со овој закон се уредуваат:

- Условите за вршење на приватно обезбедување,
- Вршењето на приватното обезбедување,
- Приватното обезбедување за сопствени потреби,
- Задолжителното приватно обезбедување,
- Овластувањата на работниците за приватно обезбедување,
- Работната облека и ознаката на работниците за приватно обезбедување,
- Формирањето, овластувањата и финансирањето на Комората на Република Македонија за приватно обезбедување,
- Евиденциите, заштитата на податоците и информациите,
- Надзорот,
- Овластувањето за подзаконски прописи и
- Прекршочни одредби.

Со овој закон, суштински и концепциски различно од законот што престана да важи, детално се уредува материјата за приватното обезбедување, а особено областа на техничкото обезбедување.

4.1. ВИДОВИ НА ПРИВАТНО ОБЕЗБЕДУВАЊЕ

Што е приватно обезбедување?

Приватното обезбедување е дејност од јавен интерес и претставува заштита на лица и имот што се врши од страна на правни лица кои имаат дозвола за приватно обезбедување.

Приватното обезбедување го вршат правни и физички лица кои ги исполнуваат условите утврдени со Законот за приватно обезбедување, при што обезбедувањето го вршат исклучиво под услови и на начин утврдени со овој закон.

Правните лица кои имаат дозвола за приватно обезбедување може да преземаат законски утврдени мерки и активности заради спречување и откривање на штетни појави и противправни дејствија кои ги загрозуваат телесниот интегритет и достоинството на личноста и имотот што се обезбедува. При тоа од суштинско значење е дека со законот исклучиво е забрането овие правни лица:

- Да обезбедуваат лица и имот кои врз основа на посебни прописи ги обезбедуваат надлежните државни органи, како што е Министерството за внатрешни работи и
- Не смеат да вршат работи поврзани со наплата на долг.

Приватното обезбедување на лица и имот, од страна на правните лица кои имаат добиено дозвола за приватно обезбедување, се врши од страна на работниците за приватно обезбедување. Работниците за приватно обезбедување се физички лица кои се стекнале со лиценца за приватно обезбедување и легитимација за приватно обезбедување, имаат засновано работен однос, односно се вработени во правно лице кое има дозвола за приватно обезбедување и вршат работи и работни задачи за обезбедување на лица и имот врз основа на овластувањата утврдени со Законот за приватно обезбедување.

Приватното обезбедување правните лица може да го вршат:

- Во вид на давање на услуги и
- За сопствени потреби.

Приватно обезбедување во вид на давање на услуги претставува заштита на лица и имот што ја врши правно лице кое има:

- извршено упис на дејноста во Централниот регистар на Република Македонија;
- добиено дозвола за приватно обезбедување и
- склучено договор за приватно обезбедување во писмена форма со корисникот на услугата.

Овие три услови потребно е правното лице да ги исполнува кумулативно, односно потребно е правното лице да ги исполнува сите три услови.

Видно од наведеното е дека ова правно лице својата услуга ја нуди на пазарот по одредена цена. Во нашето општествено опкружување тоа во основа се агенциите за обезбедување, чии услуги ги среќаваме речиси секаде околу нас во секојдневното живеење: физичкото обезбедување во училиштата, обезбедувањето што го вршат работниците за обезбедување во шопинг центрите, на различни спортски натпревари, во банките и слично.

Приватното обезбедување во вид на давање на услуги може да се врши како:

- физичко обезбедување и/или
- техничко обезбедување.

Физичкото обезбедување се врши како:

1. телесна заштита;
2. мониторинг-патролно обезбедување,
3. обезбедување на транспорт и пренос на пари и други вредносни пратки и
4. обезбедување на јавни собири и други настани.

За разлика од приватното обезбедување што се врши во вид на давање на услуги, приватното обезбедување за сопствени потреби, што е видно и од самиот назив, не смее и не може да се нуди на пазарот по одредена цена. Имено, приватното обезбедување за сопствени потреби претставува онаа заштита на имотот и лицата во правното лице што се врши од страна на работници за приватно обезбедување кои се вработени во правното лице кое ја има добиено дозвола за приватно обезбедување за сопствени потреби. Во нашето општествено опкружување, тоа во основа се сите оние фирми, фабрики и слично кои имаат вработено работници за обезбедување, кои вршат заштита на имотот на фирмата, односно фабриката и на лицата во неа.

Приватното обезбедување за сопствени потреби може да се врши само како физичко обезбедување и тоа како телесна заштита и мониторинг обезбедување. Со други зборови, правните лица кои имаат дозвола за приватно обезбедување за сопствени потреби не смеат да вршат техничко обезбедување, а од физичкото обезбедување имаат овластување само да вршат телесна заштита и мониторинг обезбедување на својот имот и лицата во него.

Што се подразбира под потребно наведение начини на кои се врши приватно обезбедување?

Телесната заштита претставува обезбедување на лица и имот што се врши непосредно од страна на работниците за приватно обезбедување.

Мониторинг-патролното обезбедување е постојан физички надзор над вградени технички системи и уреди за обезбедување на лица и имот и телекомуникациски пренос на алармни сигнали во центар за обезбедување и надзор и ангажирање на работници за приватно обезбедување и употреба на возила за обезбедување заради спречување на штетни дејствија над лицата и имотот што се обезбедуваат и обезбедување на лица и имот по пристигнат алармен сигнал од центар за обезбедување и надзор.

Мониторинг обезбедувањето претставува постојан физички надзор над вградени технички системи и уреди за обезбедување на лица и имот и телекомуникациски пренос на алармни сигнали во центар за обезбедување

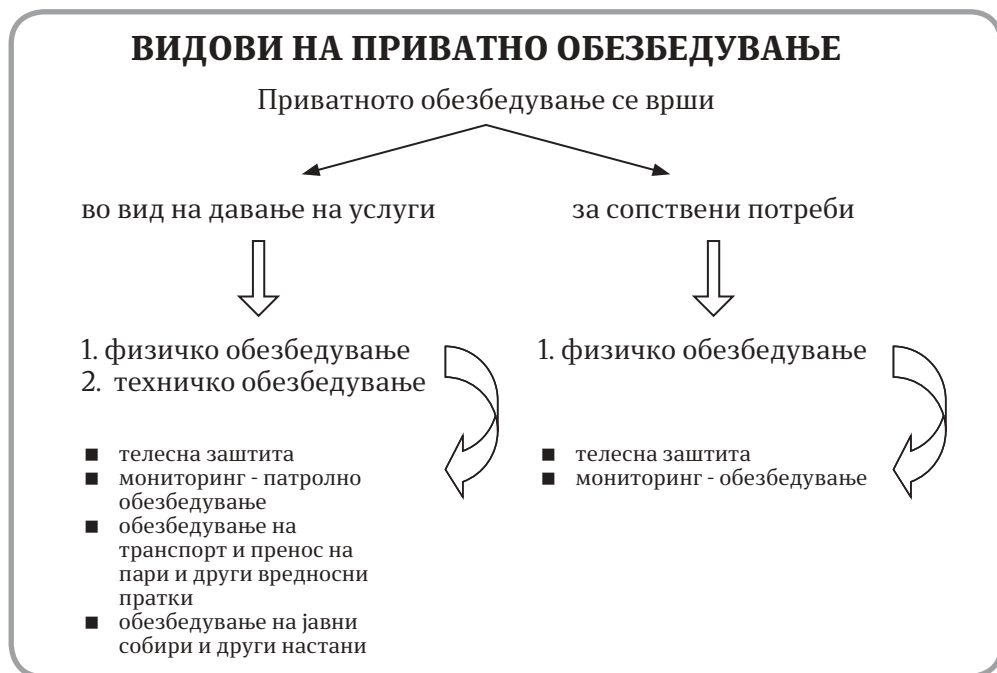
и надзор. Разликата на овој начин на обезбедување во однос на мониторинг-патролното обезбедување е отсуството на патрола, односно отсуството на ангажирање на возила и работници за приватно обезбедување. Но и кај едниот и друг вид на вршење на обезбедување е постоењето на Центар за обезбедување и надзор. Центарот за обезбедување и надзор во основа е посебна просторија опремена со технички уреди за автоматски прием и обработка на алармни сигнали и други информации кои пристигнуваат од уреди и инсталации во објекти или возила инсталирани за таа намена. Овој Центар мора да има дежурство од 24 часа.

Обезбедувањето на транспорт и пренос на пари и други вредносни пратки претставува обезбедување на превоз и пренос на пари, злато, скапоцени камења, уметнички дела, хартии од вредност и на други вредносни пратки што се врши со работници за приватно обезбедување и посебни возила.

Во последно време актуелна е и нужна потребата за заштита на превозот, односно преносот на пари, скапоцености и други вредносни пратки од евентуални грабежи што се вршат со употреба на огнено оружје, во една предсмислени акции од маскирани лица во кои напади може покрај кражбата на имотот да има за последица и смрт на лицата што ги превезуваат, односно пренесуваат скапоценостите. Превозот на скапоценостите, најчесто на условно речено подолги дестинации се врши со посебно опремено возило за транспорт што мора да исполнува прецизно утврдените законски услови како што се: да има блиндирана каросерија, стакла и гуми; да има вграден механички сигурносен сеф, да има вграден уред на глобален систем (ГПС уред) за сателитско следење и далечински мониторинг од центар за обезбедување и надзор и слично. За разлика од превозот на скапоцености, преносот се врши без посебно опремено возило, од страна на работници за обезбедување со сигурносен куфер чија конструкција е така изработена да може да спречи насилно отворање и отуѓување на содржината, а обидот за насилно отворање да го алармира или дојави со звучен, светлосен или друг сигнал. При тоа, за вршење на преносот потребно е да бидат исполнети и други законски утврдени услови.

Обезбедувањето на јавни собири и други настани е обезбедувањето што се врши со работници за приватно обезбедување и со употреба на технички средства заради одржување на јавниот ред на јавни собири, спортски натпревари, културни, забавни, верски, хуманитарни, социјални, политички, економски и други настани.

Сведоци сме на современо живеење кога потребата за обезбедување е се поактуелна и неминовна. Имено, речиси секое одржување на било каков и да е вид на јавно собирање од спортски, културен, забавен или сличен карактер не може да се замисли без ангажирање на приватното обезбедување во интерес на мирот и безбедноста на сите учесници и присутни лица и сведување на минимум на ризикот за евентуално нарушување на јавниот ред и мир, евентуалните повреди и оштетувања на имотот.



4.2. ОПШТИ УСЛОВИ ЗА ФИЗИЧКО ЛИЦЕ ЗА ВРШЕЊЕ НА ПРИВАТНО ОБЕЗБЕДУВАЊЕ (ЛИЦЕНЦА И ЛЕГИТИМАЦИЈА ЗА ОБЕЗБЕДУВАЊЕ)

Физичко лице може да врши приватно обезбедување само доколку е вработено во правно лице кое има дозвола за приватно обезбедување и доколку поседува:

- лиценца за приватно обезбедување и
- легитимација за приватно обезбедување.

Лиценцата за приватно обезбедување претставува овластување со кое физичкото лице кое ги исполнува законски утврдените услови се стекнува со право да врши приватно обезбедување на лица и имот.

Легитимацијата за приватно обезбедување е исправа што е издадена од Комората на Република Македонија за приватно обезбедување со која работникот за приватно обезбедување го докажува своето службено својство.

Формата и содржината на лиценцата за приватно обезбедување и на легитимацијата за приватно обезбедување се пропишани со посебни подзаконски прописи што ги донесува министерот за внатрешни работи и се објавуваат во „Службен весник на Република Македонија“.

Лиценцата за приватно обезбедување може да му се издаде на физичко лице како:

- лиценца за физичко обезбедување и
- лиценца за техничко обезбедување.

И двата вида на лиценци се издаваат само ако тоа физичкото лице-барател на лиценцата ги исполнува следниве законски утврдени услови:

1. е државјанин на Република Македонија,
2. има живеалиште во Република Македонија,
3. има наполнето 18 години,
4. поседува општа психофизичка здравствена способност, што го докажува со соодветно лекарско уверение кое не смее да биде постаро од три месеци,
5. не е осудено со правосилна судска пресуда или против него не се води кривична постапка за кривично дело за кое се гони по службена должност,
6. има завршено најмалку средно образование,
7. оспособено е за физичко обезбедување лица и имот ако бара да се стекне со лиценца за физичко обезбедување, односно оспособено е за техничко обезбедување лица и имот ако бара да се стекне со лиценца за техничко обезбедување и
8. има положено стручен испит за физичко обезбедување ако бара да се стекне со лиценца за физичко обезбедување, односно има положено стручен испит за техничко обезбедување ако бара да се стекне со лиценца за техничко обезбедување.

За оние лица кои завршиле високо образование од областа на безбедноста и криминалистиката, со оглед на природата на овој вид образование и совладаните наставни содржини, законот утврдува дека можат да го полагаат стручниот испит во рок од десет години од денот на стекнувањето со диплома за завршено соодветно високо образование без претходно оспособување за приватно обезбедување.

Исполнување на условите за соодветно оспособување и полагање на стручен испит како услов за стекнување на лиценца, не се однесува на лицата кои најмалку три години извршувале работи и работни задачи како овластено службено лице во Министерството за внатрешни работи или Министерството за одбрана. Овој исклучок законодавецот го утврдил како резултат на спроведената анализа и утврдена оценка за теоретското и практичното искуство кое го стекнува таа категорија на работници во тој временски период како и на положениот соодветен испит за работа на тие работни места во наведените Министерства со оглед на нивниот законски утврден делокруг на надлежности.

Оспособувањето, како еден од претходно наведените законски услови за стекнување со лиценца го организира Комората на Република Македонија за приватно обезбедување, а го вршат посебни комисии и тоа комисија која врши само оспособување за физичко обезбедување и комисија што врши само техничко оспособување. И двете комисии ги формира министерот за внатрешни работи, а се составени од претставници на Министерството за внатрешни работи и Комората, во законски утврден сооднос. Трошоците за оспособување се на товар на барателот на лиценцата за приватно обезбедување.

И стручните испити, како и оспособувањето, се полагаат пред посебни комисии и тоа комисија за спроведување на стручен испит за физичко обезбедување и комисија за спроведување на стручен испит за техничко обезбедување, кои ги формира министерот за внатрешни работи од претставници на Министерството за внатрешни работи и Комората, во законски утврден сооднос. За проверка на оспособеноста за ракување со огнено оружје како дел од стручниот испит за физичко обезбедување се формира посебна комисија на Министерството за внатрешни работи.

Оспособувањето и спроведувањето на стручниот испит се врши согласно посебна Програма која е утврдена во подзаконски пропис што согласно Законот за приватно обезбедување го донесува министерот за внатрешни работи. Со Програмата е утврдено дека оспособувањето и полагањето стручен испит за техничко обезбедување се состои од Теоретски дел и Практичен дел. Теоретскиот дел е составен од повеќе наставни содржини при што оспособувањето се врши во траење од вкупно 40 часа.

Како лиценцата и легитимацијата за приватно обезбедување се издава како:

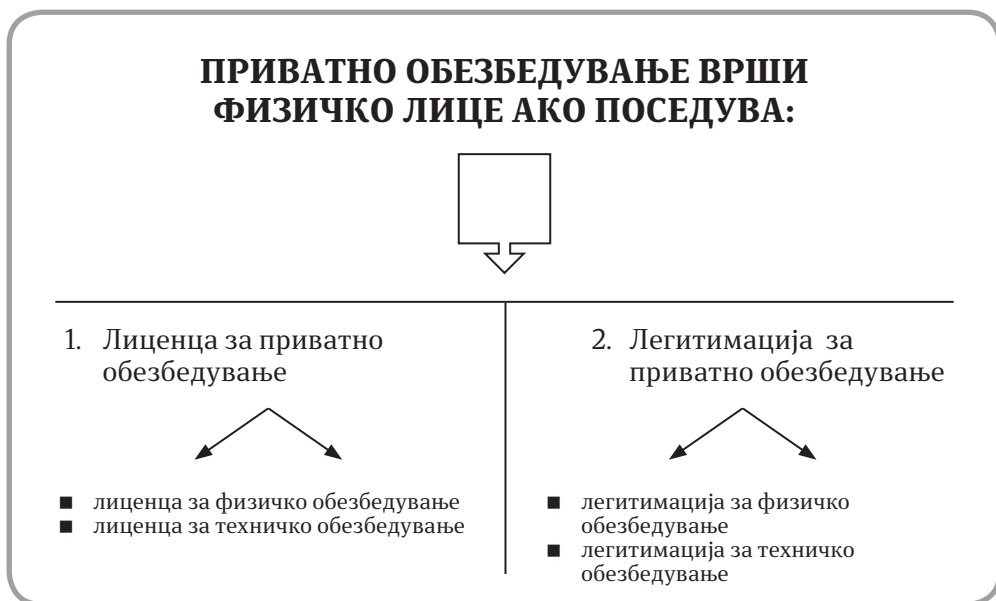
- Легитимација за физичко обезбедување и
- Легитимација за техничко обезбедување.

Легитимацијата се издава на правно лице кое врши приватно обезбедување, при што истата се издава за физичкото лице кое:

- Има лиценца за физичко, односно техничко обезбедување,
- Има засновано работен однос во правното лице кое врши приватно обезбедување во вид на давање на услуги, односно во правното лице кое врши приватно обезбедување за сопствени потреби,
- Здравствено и психофизички е способно и
- Со правосилна пресуда или со правосилна одлука на прекршочен орган не му е изречена казна или прекршочна санкција забрана за вршење професија, дејност или должност.

Секое правно лице е должно да поднесе барање за издавање легитимација за приватно обезбедување до Комората во рок од 30 дена од

засновање на работниот однос со работникот. Кога пак работникот, во текот на траење на работниот однос, престане да исполнува еден од претходно наведените услови за стекнување легитимација, правното лице ја одзема легитимацијата од работникот и ја доставува за поништување до Комората во рок од 30 дена сметано од денот кога е констатирано дека работникот не го исполнува условот. Доколку пак правното лице не во можност да го стори тоа, во истиот рок е должно да ја извести Комората за неисполнувањето на условот од страна на работникот и веднаш да ја огласи легитимацијата за неважечка во „Службен весник на Република Македонија“. На барање на правното лице, работникот е должен да ја врати легитимацијата за приватно обезбедување.



4.3. ВРШЕЊЕ НА ТЕХНИЧКО ОБЕЗБЕДУВАЊЕ

Техничкото обезбедување претставува обезбедување на лица и имот со примена на технички средства и уреди, нивно проектирање, инсталирање и одржување.

Употребата на технички средства и уреди се врши заради спречување на противправни дејствија насочени кон лица и имот, а особено за заштита од:

1. Недозволен пристап во објекти и простории што се обезбедуваат,
2. Неовластено користење и отуѓување на предмети што се обезбедуваат,
3. Неовластено внесување на огнено оружје, експлозивни, радиоактивни, запаливи и отровни материи,
4. Провалување, диверзија или насилен напад на објектот што се обезбедува,
5. Неовластен пристап до податоци и документација,
6. Напад на возила за транспорт на пари и други вредносни пратки и
7. Напад на работници за обезбедување кои вршат пренос на пари и други вредносни пратки.

Техничките средства и уреди може да бидат поврзани во систем на техничка заштита.

Работите на техничко обезбедување согласно закон може да се вршат:

- Само во објектот што се обезбедува,
- До границата на просторот што се обезбедува,
- Во текот на транспорт и пренос на пари и други вредносни пратки и
- За време на вршење на телесна заштита на лица.

За да се почитуваат ограничувањата утврдени во законот во однос на овој вид на обезбедување, потребно е при секојдневното работење да нема дилеми, односно истите да се сведат на минимум. Во таа насока, во законот се дефинирани и употребените поими:

- границата на простор што се обезбедува е дефинирана како линија што ги опфаќа недвижностите и површините што се составен дел на имотот што се обезбедува,
- телесната заштита е физичко обезбедување со кое работниците за приватно обезбедување непосредно ги обезбедуваат лицата и имотот.

4.4. ЗАШТИТА НА ПРИВАТНОСТА И ИЗВЕСТУВАЊЕ ЗА ВРШЕЊЕ НА ВИДЕОНАДЗОРОТ

Живееме во ера кога значењето и потребата за заштита на приватноста е мошне актуелна. Сведоци сме дека последните години на ова прашање му се посветува се поголемо внимание. Имајќи ги предвид можностите на техничките средства и методи со помош на кои се врши приватното техничко обезбедување, несомнено е дека законодавецот утврдил децидна забрана. Имено, техничките средства и уреди не смеат да се користат на

начин на кој надвор од објектот што се обезбедува или надвор од границата на просторот што се обезбедува, се нарушува приватноста на други лица.

Во случај пак, кога обезбедувањето на одреден објект или просторија кои се користат за јавна употреба, се врши со технички средства и уреди за видеонадзор, правното лице кое го врши обезбедувањето е должно на видливо место да истакне известување за тоа дека се врши видеонадзор, согласно со прописите за заштита на личните податоци.

Материјата за заштита на личните податоци е регулирана со посебен закон, а надзорот над почитувањето на одредбите на тој закон и подзаконските прописи од таа област го врши Дирекцијата за заштита на лични податоци, како самостоен и независен државен орган со својство на правно лице.

4.5. КВАЛИТЕТ И ИСПРАВНОСТ НА ТЕХНИЧКИТЕ СРЕДСТВА И УРЕДИ

Правните лица кои имаат дозвола за вршење приватно техничко обезбедување се должни обезбедувањето да го вршат согласно со важечките стандарди на Република Македонија кои се однесуваат на квалитетот и исправноста на средствата и уредите за техничко обезбедување. Кога не постојат пропишани стандарди во Република Македонија обврската постои за почитување на меѓународните технички стандарди. Затоа едно од круцијалните обврски во работата на одговорните лица во правните лица кои го вршат овој вид на дејност е континуирано следење на оваа материја.

Правното лице кое врши приватно техничко обезбедување е одговорно за исправноста на вградените технички средства и уреди, нивното редовно одржување и поправка, согласно со писмениот договор што се склучува со корисникот на услугата. Имено, правното лице кое врши приватно техничко обезбедување, обезбедувањето го врши врз основа на договор за приватно обезбедување што го склучува со корисникот на услугата во писмена форма. Договор кој не е склучен во писмена форма или е склучен со правно лице кое нема дозвола за приватно обезбедување се смета за ништовен. Вршењето на обезбедување без писмен договор има за последица прекршочна одговорност на правното лице за прекршок за кој е утврдена глоба од 3.500 до 4.000 евра во денарска противвредност и изрекување прекршочна санкција забрана за вршење на дејноста во траење од шест месеци до пет години. За истиот прекршок утврдена е и глоба во износ од 1.500 до 1.800 во денарска противвредност и за одговорното лице во правното лице.

4.6. ЛЕГИТИМИРАЊЕ НА РАБОТНИКОТ ЗА ПРИВАТНО ОБЕЗБЕДУВАЊЕ

Легитимацијата за приватно обезбедување, како што е и претходно истакнато, претставува исправа која е издадена од Комората на Република Македонија за приватно обезбедување со која работникот за приватно обезбедување го докажува своето службено својство. Поседувањето на легитимацијата е еден од условите што треба да ги исполни едно физичко лице, доколку сака, односно треба да врши приватно обезбедување.

Имено, во случај кога едно физичко лице заснова работен однос во правно лице кое врши приватно техничко обезбедување, за работно место работник за приватно обезбедување, правното лице е должно до Комората да поднесе барање за издавање на легитимација за тоа лице во рок од 30 дена сметано од денот на засновање на работниот однос на лицето. Формата и содржината на образецот на легитимацијата, начинот на нејзиното издавање и употреба е пропишано со посебен подзаконски пропис што го донесува министерот за внатрешни работи и се објавува во „Службен весник на Република Македонија„.

За време на вршењето на приватното обезбедување работникот е должен да ја носи легитимацијата и секогаш кога се повикува на своите работи и работни задачи е должен истовремено и да ја покаже, бидејќи со неа пред други лица го докажува своето службено својство. Но, легитимацијата работникот е должен да ја покаже и на барање на овластено службено лице на Министерството за внатрешни работи. Ова пред се бидејќи надзорот над спроведувањето на одредбите на овој закон и прописите донесени врз основа на него го вршат овластени службени лица на Министерството за внатрешни работи.

Неносењето на легитимација за приватно обезбедување во вршењето на приватно обезбедување има за последица прекршочна одговорност на физичкото лице за прекршок за кој е утврдена глоба во износ од 600 до 700 евра во денарска противвредност. За овој прекршок е утврдено да се изрече и прекршочна санкција забрана за вршење на дејноста на физичкото лице во траење од една до пет години.

4.7. ПОСТАПУВАЊЕ ПО НАРЕДБА

Министерството за внатрешни работи како орган на државната управа, врши работи што се однесуваат на остварување на системот на јавната и државната безбедност во државата. Надзорот над спроведувањето на Законот за приватно обезбедување и на прописите донесени врз основа на овој закон, вршат овластени службени лица на Министерството за внатрешни работи. Во таа насока, овластените службени лица, согласно своите законски овластувања преземаат мерки и активности, меѓу кои е и издавањето на наредби, односно наредувањето.

Наредбата овластеното службено лице може да ја издаде кога согласно закон тоа е потребно за да се заштити животот и личната сигурност на луѓето и имотот, да се спречи извршување на кривично дело или прекршок, да се обезбедат траги од кривично дело и предмети што можат да послужат како доказ во кривична или прекршочна постапка, да се одржи или спречи нарушување на јавниот ред и мир, како и за воспоставување на јавен ред и мир, контрола, регулирање и безбедноста во сообраќајот на патиштата и друго. Наредувањето овластените службени лица го вршат на јасен, недвосмислен и разбирлив начин.

Работникот за приватно обезбедување е должен да постапи по наредба на овластено службено лице на Министерството за внатрешни работи. Работникот не смее да ја изврши наредбата на тоа лице, ниту пак наредбата на својот претпоставен доколку со тоа би извршил кривично дело.

Со Законот за приватно обезбедување утврдена е глоба во износ од 900 до 1000 евра во денарска противвредност за физичко лице кое нема да постапи по наредба на овластено службено лице на Министерството. За овој прекршок, на физичкото лице ќе му се изрече и прекршочна санкција забрана за вршење на дејноста во траење од една до пет години.

4.8. РАБОТНА ОБЛЕКА И ОЗНАКА НА РАБОТНИЦИТЕ ЗА ПРИВАТНО ОБЕЗБЕДУВАЊЕ

За да може едно правно лице да се стекне со дозвола за приватно обезбедување, потребно е да исполни повеќе законски утврдени услови. Еден од нив е да поседува акт со кој се пропишуваат изгледот на работната облека на работниците за приватно обезбедување и знакот на правното лице. Со тој акт се пропишува видот, составот, бојата и кројот на работната облека. Правното лице без исклучок мора да води сметка дека пропишаната

работна облека и ознака мора да се разликува од униформата и ознаките на Полицијата, Армијата на Република Македонија, Царинската управа, како и од униформите и ознаките на други државни органи. Ова е потребно меѓу другото и од практичен аспект за отстранување на било каква веројатност од предизвикување заблуди и забуни пред се кај граѓаните во однос на нивното постапување.

Правното лице кое има дозвола за приватно обезбедување е должно во текот на своето работење во континуитет да ги исполнува сите законски услови што се пропишани за издавање на дозволатата, вклучувајќи го и овој услов за актот за работната облека и ознака.

Покрај постоењето на актот за пропишување на работната облека и ознаката, правното лице мора да ја обезбеди така пропишаната работна облека со ознака за работниците за приватно обезбедување.

По правило, работникот за приватно обезбедување обезбедувањето го врши во работна облека. По исклучок, истата не мора да ја носи, но во секој случај без исклучок секогаш мора да ја има ознаката на правното лице.

Обврската за носење на работната облека е само во текот на работното време, како и при доаѓање и враќање од работа.

Работната облека или делови од неа и ознаката на правното лице не смеат да ги носат, односно користат лица кои не се овластени за тоа.

Непочитувањето на одредбите за работната облека и ознаката на правното лице повлекува прекршочна одговорност.

4.9. ПРЕКРШОЧНИ ОДРЕДБИ

Непочитувањето на законските одредби од страна на оние субјекти на кои се однесуваат има за последица спроведување на соодветна постапка за утврдување на одговорност и изрекување соодветни санкции од страна на овластените субјекти за тоа, суд или прекршочен орган. Во случајов, непочитувањето на одредбите од Законот за приватно обезбедување предизвикува спроведување на прекршочна постапка, пропишана со Законот за прекршоците и Законот за приватното обезбедување.

Изрекување прекршочна санкција е последица на сторен прекршок. Што е прекршок?

Прекршок е противправно дело кое со закон е определено како прекршок, чии обележја се определени со закон и за кое е пропишана прекршочна санкција.

На пример, во Законот за приватното обезбедување има посебна одредба со која е пропишано дека работникот за приватно обезбедување е должен за време на вршење на обезбедувањето да носи легитимација за обезбедување. Со истиот закон е утврдено дека глоба во износ од 600 до 700 евра во денарска противвредност ќе му се изрече за прекршок на физичко лице ако во вршењето на приватното обезбедување не носи легитимација за обезбедување. Покрај глобата, утврдено е дека за тој прекршок на физичкото лице ќе му се изрече и прекршочна санкција забрана за вршење на дејноста приватно обезбедување во траење од една до пет години. Надзор над спроведување на овој закон вршат овластени службени лица на Министерството за внатрешни работи. Доколку при таквиот надзор определено овластено службено лице утврди дека определен работник при вршење на обезбедувањето не носи легитимација ги презема сите мерки и дејствија заради утврдување на прекршочна одговорност на тој работник и изрекување соодветна прекршочна санкција од страна на надлежен суд.

Со Законот за приватно обезбедување пропишани се одредби за одговорност на правното лице, одговорното лице во правното лице и на физичкото лице, односно работникот за приватно обезбедување. Одговорно лице во правното лице е она лице во правното лице кое со оглед на неговата функција или врз основа на посебно овластување во правното лице му е доверен определен круг на работи што се однесуваат на извршување на законските прописи или на прописите донесени врз основа на закон или општ акт на правното лице во управувањето, користењето и располагањето со имот, раководењето со производниот или некој друг стопански процес или надзорот над нив.

Со истиот Закон пропишани се два вида на прекршочни санкции и тоа глоба и забрана за вршење на дејност. За полесните прекршоци пропишани се пониски износи на глоба, а за потешките и повисоки износи на глоба. Значи законодавецот направил извесна градација во тој поглед, бидејќи нема иста тежина прекршокот на пример ако работник за обезбедување за време на обезбедувањето не ја носи легитимацијата, со прекршокот на работникот за физичко обезбедување, кој е овластен за употреба на средства на присилба, а кој употреби средства на присилба спротивно на законски утврдените ограничувања, што може да предизвика мошне сериозни пооследици, дури и по животот на граѓаните.

Со Законот за приватно обезбедување пропишани се следните санкции:

■ За правно лице

Глоба - износ од 900 до 1000 евра

И од 3.500 до 4.000 евра и забрана за вршење на дејноста во траење од шест месеци до пет години

- За одговорно лице во правно лице -
Глоба- износ од 400 до 500 евра
Од 1.500 д 1.800 евра и
Од 1.200 до 1.500 евра
- За физичко лице -
Глоба- износ од 600 до 700 евра
И од 900 до 1.000 евра
Со прекршочна санкција забрана за вршење на дејноса во траење од една до пет години

Во случај кога овластеното службено лице ќе констатира прекршок и утврди дека се исполнети законските услови за спроведување на прекршочна постапка, поднесува барање за поведување на прекршочна постапка до надлежниот суд за утврдување на прекршочна одговорност. Но она што е од суштинско значење е дека секогаш, без исклучок, овластеното службено лице е должно претходно, пред да поднесе барање за прекршочна постапка, да му предложи на сторителот на прекршокот постапка за порамнување. Целта на постапката за порамнување е да се постигне согласност на сторителот на прекршокот и надлежниот орган - Министерството за внатрешни работи, да се спречи повторното вршење на прекршокот и да се избегне водење на прекршочна постапка пред надлежниот суд.

Во постапката за порамнување се преземаат следниве активности:

- Овластеното службено лице составува записник, во кој меѓу другото внесува: битни елементи на дејствијето од кое произлегува правното обележје на прекршокот, времето, местото и начинот на сторување на прекршокот, дава опис на дејствијето и лицата кои се затегнати на самото место. Записникот го потпишува овластеното службено лице и сторителот
- На сторителот на прекршокот му издава платен налог во кој изрекува глоба за сторениот прекршок во висина што е еднаква на минимумот од глобата што е утврден во законот за тој прекршок
- Ако сторителот го прими платниот налог, го потпишува истиот и издавањето на платниот налог се забележува и во записникот
- Се смета дека сторителот на прекршокот со потписот на приемот на платниот налог се согласува да ја плати глобата
- Законски утврдениот рок за плаќање на глобата изречена во платниот налог е осум дена сметано од денот на приемот на платниот налог.

Она што е од суштинско значење за платниот налог, односно за оваа постапка за порамнување е дека во тој рок, врз основа на издадениот платен налог се плаќа само половина од изречената глоба. Ако сторителот не ја плати глобата во тој рок, се поднесува барање за поведување на прекршочна постапка до надлежниот суд за сторениот прекршок.

5

ТЕОРЕТСКИ ДЕЛ

Закон за заштита на лични податоци

- 5.1. Правилник за техничките и организациските мерки за обезбедување на безбедност и заштитата на обработката на личните податоци **149**
- 5.2. Правилник за видео надзор **163**

2 ЧАСА



5.1. ПРАВИЛНИК ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

I. Вовед

Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија“ бр.38/09 и 158/10), преку неговата целосна и правилна примена ја обезбедува сигурноста на личните податоци како еден најважен сегмент од поширокиот поим „заштита на личните податоци“. Со примената на овој Правилник, односно преку примената на соодветни технички и организациски мерки се обезбедува заштита на личните податоци од секако случајно или незаконско уништување на личните податоци, или нивно случајно губење, преправање, неовластено откривање или пристап, особено кога обработката вклучува и пренос на податоците преку мрежа, како и заштита од какви било незаконски облици на обработка.

Во Законот за заштита на личните податоци е утврдено дека за да се обезбеди тајност и заштита на обработката на личните податоци на субјектот, контролорот и обработувачот мора да применат соодветни технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци, како и да донесат и применат соодветна документација со опис на техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци. Содржината пак на самата документација е пропишана од страна на Дирекцијата за заштита на личните податоци.

Во насока на подобро разбирање на одредбите на Правилникот најнапред треба да се појасни значењето на изразите во Правилникот при што одделени изрази следново значење:

1. **Авторизиран пристап** е овластување доделено на овластеното лице за обработка на личните податоци, за користење на одредена информатичко комуникациска опрема или за пристап до одредени работни простории на контролорот;
2. **Администратор на информацискиот систем** е лице овластено за пла-нирање и за применување на технички и организациски мерки, како и за контрола на обезбедувањето тајност и заштита на обработката на личните податоци;
3. **Документ** е секој запис кој содржи лични податоци и истиот може да биде во електронска или хартиена форма, да се чува на медиум и во информатичко комуникациската опрема која се користи за

обработка на податоците, да се доставува преку пошта или да се пренесува преку електронско комуникациска мрежа.

4. **Идентификација** е постапка за идентификување на овластеното лице на информацискиот систем;
5. **Информатичка инфраструктура** е целата информатичко комуникациска опрема на контролорот, во рамките на која се собираат, обработуваат и чуваат личните податоци;
6. **Информациски систем** е систем со кој може да се обработуваат личните податоци со цел да бидат достапни и употребливи за секој кој што има право и потреба да ги користи;
7. **Инцидент** е секоја аномалија која влијае или може да влијае на тајноста и заштитата на личните податоци;
8. **Контрола на пристап** е операција за доделување на пристап до личните податоци или до информатичко комуникациската опрема со цел проверка на овластеното лице;
9. **Овластено лице** е лице вработено или ангажирано кај контролорот кое има авторизиран пристап до документите и до информатичко комуникациската опрема;
10. **Лозинка** е доверлива информација составена од множество на карактери кои се користат за проверка на овластеното лице;
11. **Медиум** е физички уред кој се користи при обработка на личните податоци во информацискиот систем, на кој податоците можат да бидат снимени или од кој истите можат да бидат повторно вратени;
12. **Офицер за заштита на личните податоци** е лице овластено од контролорот за самостојно и независно вршење на работите во смисла на член 26-а од Законот за заштита на личните податоци;
13. **Проверка** е постапка за верификација на идентитетот на овластеното лице на информацискиот систем;
14. **Сигурносна копија** е копија на личните податоци содржани во електронските документи, кои се зачувани на медиум за да се овозможи нивно повторно враќање.

Одредбите од Правилникот се применуваат и при обработката на личните податоци од страна на обработувачот на збирка на лични податоци.

Одредбите од овој правилник се применуваат за:

- целосно и делумно автоматизирана обработка на личните податоци и
- друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.

Нивоа на технички и организациски мерки и нивна примена

Техничките и организациските мерки треба да се применуваат на начин кој ќе обезбеди тајност и заштита на обработката на личните податоци, соодветно на природата на податоците кои се обработуваат и ризикот при нивната обработка. При тоа, техничките и организациските мерки согласно нивната природа и ризикот при нивната обработка се класифицираат во три нивоа: основно, средно и високо.

За сите документи задолжително се применуваат технички и организациски мерки кои се класифицирани на основно ниво.

За документите кои содржат лични податоци што се однесуваат на: кривични дела, изречени казни, алтернативни мерки и мерки на безбедност за извршени кривични дела, задолжително се применуваат технички и организациски мерки кои се класифицирани на основно и средно ниво.

За документите кои содржат: посебни категории на лични податоци, лични податоци кои се обработуваат за полициски цели и лични податоци кои се обработуваат заради заштита на интересите на државната безбедност и одбраната на Република Македонија, задолжително се применуваат технички и организациски мерки кои се класифицирани на основно, средно и високо ниво.

За документите кои содржат матичен број на граѓанинот задолжително се применуваат технички и организациски мерки кои се класифицирани на основно и средно ниво.

За документите кои се пренесуваат преку електронско комуникациска мрежа, а содржат посебни категории на лични податоци и/или матичен број на граѓанинот задолжително се применуваат технички и организациски мерки кои се класифицирани на основно, средно и високо ниво.

Обработката на личните податоци надвор од работните простории на контролорот може да се врши врз основа на обезбедено писмено овластување од страна на контролорот и во согласност со соодветното ниво на технички и организациски мерки кои се применувале за обработка на податоците содржани во документите.

Контролорот треба да ја евидентира и да ја чува целокупната документација за софтверските програми за обработка на личните податоци и за сите негови промени.

Физичките или правните лица кои вршат одржување на информацискиот систем на контролорот треба да ги применуваат прописите за заштита на личните податоци и донесената документација за технички и организациски мерки.

II. Основно ниво на технички и организациски мерки

Контролорот задолжително донесува и применува документација за технички и организациски мерки за овластените лица кои имаат пристап до личните податоци и до информацискиот систем која особено треба да содржи:

- План за создавање систем на технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци;
- Акт за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци;
- Правила за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема;
- Правила за пријавување, реакција и санирање на инциденти;
- Правила за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;
- Правила за начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите.

Технички мерки

Контролорот треба да обезбеди соодветни технички мерки за тајност и заштита на обработката на личните податоци и тоа:

1. единствено корисничко име;
2. лозинка креирана од секое овластено лице, составена од комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;
3. корисничко име и лозинка која овозможува пристап на овластеното лице до информацискиот систем во целина, на поединечни апликации и/или поединечни збирки на лични податоци потребни за извршување на неговата работа;
4. автоматизирано одјавување од информацискиот систем после изминување на определен период на неактивност (не подолго од 15 минути) и за повторно активирање на системот потребно е одново внесување на корисничкото име и лозинката;
5. автоматизирано отфрлање од информацискиот систем после три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на овластеното

лице дека треба да се побара инструкција од администраторот на информацискиот систем;

6. инсталирана хардверска/софтверска заштитна мрежна бариера (“фајервол”) или рутер помеѓу информацискиот систем и интернет или било која друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или пробивање на системот;
7. ефективна и сигурна анти-вирусна и анти-спајвер заштита на информацискиот систем, која постојано ќе се ажурира заради превентива од непознати и непланирани закани од нови вируси и спајвери;
8. ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови и
9. приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.

Организациски мерки

Контролорот треба да обезбеди и соодветни организациски мерки за тајност и заштита на обработката на личните податоци и тоа:

1. ограничен пристап или идентификација за пристап до личните податоци;
2. организациски правила за пристап на овластените лица до интернет кои се однесуваат на симнување и снимање на документи преземени од електронската пошта и други извори;
3. уништување на документи по истекот на рокот за нивно чување;
4. мерки за физичка сигурност на работните простории и на информатичко комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци и
5. почитување на техничките упатства при инсталирање и користење на информатичко комуникациската опрема на која се обработуваат личните податоци.

Вработеното лице кое ги врши работите за човечки ресурси кај контролорот, го известува администраторот на информацискиот систем за вработувањето или ангажирањето на секое овластено лице со право на пристап до информацискиот систем, за да му биде доделено корисничко име и лозинка, како и за престанок на вработувањето или ангажирањето за да му бидат избришани корисничкото име и лозинката, односно заклучени за натамошен пристап.

Физичка сигурност на информацискиот систем

Серверите на кои се инсталирани софтверските програми за обработка на личните податоци, треба да бидат физички лоцирани, хостирани и администрирани од страна на контролорот, а физички пристап до просторијата во која се сместени серверите може да имаат само лица посебно овластени од контролорот.

Во случај кога е неопходен пристап и на друго лице до просторијата и личните податоци зачувани на серверите, тогаш тоа лице треба да биде придружувано и надгледувано од страна на некое од веќе овластените лица.

Воедно, просторијата во која се сместени серверите треба да се заштити од ризиците во опкружувањето преку примена на мерки и контроли со кои се намалува ризикот од потенцијални закани (на пр. кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење).

Само по исклучок, серверите на кои се инсталирани софтверски програми за обработка на личните податоци, можат да бидат физички лоцирани, хостирани и администрирани надвор од просториите на контролорот во кој случај меѓусебните права и обврски на контролорот и правното, односно физичкото лице кај кое се физички лоцирани, хостирани и администрирани серверите се уредуваат со договор во писмена форма, кој задолжително ќе содржи технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци.

Информирање за заштитата на личните податоци

Лицата кои се вработуваат или се ангажираат кај контролорот, пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со донесената документација за технички и организациски мерки. При тоа за лицата кои се ангажираат за извршување на работа кај контролорот во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.

Лицата кои се вработуваат или се ангажираат кај контролорот, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци која задолжително содржи одредби дека лицата ќе ги почитуваат начелата за заштита на личните податоци пред нивниот пристап до личните податоци; дека ќе вршат обработка на личните податоци согласно упатствата добиени од контролорот, освен ако со закон поинаку не е уредено и дека ќе ги чуваат како доверливи личните податоци, како и мерките за нивна заштита. Вака потпишана изјава потребно е да се чува во досиејата на лицата кои се вработуваат или се ангажираат кај контролорот.

Обврски и одговорности на администраторот на информацискиот систем

Обврските и одговорностите на администраторот на информацискиот систем и на овластените лица, контролорот ги дефинира и утврдува во Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема. Во овие Правила задолжително се пропишува кој/кои лица се подведува/ат под поимот администратор на информацискиот систем, кои лице се сметаат за овластени лица и имаат пристап до информатичко комуникациската опрема, кои се обврските и одговорностите на администраторот на информацискиот систем, за вршењето на периодични контроли на неговата работа, како и за обврските и одговорностите на овластените лица кои имаат пристап до личните податоци и информатичко комуникациската опрема и за начинот на нивното информирање за техничките и организациските мерки кои се однесуваат на извршувањето на нивните обврски и одговорности.

Контролорот задолжително врши периодична контрола над работата на администраторот на информацискиот систем и изработува извештај за извршената контрола.

Евидентирање на инциденти

Во Правилата за пријавување, реакција и санирање на инциденти, контролорот го определува начинот на евидентирање на секој инцидент, времето кога се појавил, овластеното лице кое го пријавило, на кого е пријавен и мерките кои се преземени за негово санирање.

Идентификација и проверка

Контролорот задолжително води евиденција за овластените лица кои имаат авторизиран пристап до документите и информацискиот систем, како и воспоставува постапки за идентификација и проверка на авторизираниот пристап.

Кога проверката се врши врз основа на корисничко име и лозинка, контролорот секогаш ги применува правилата кои ја гарантираат нивната доверливост и интегритет при пријавување, доделување и чување на истите.

Лозинките треба автоматски да се менуваат по изминат временски период што не може да биде подолг од три месеци утврден во Актот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци, како и да се чуваат заштитени со соодветни методи, така што нема да бидат разбирливи додека се валидни.

Контрола на пристап

Овластените лица може да имаат авторизиран пристап само до личните податоци и информатичко комуникациската опрема кои се неопходни за извршување на нивните работни задачи при што се воспоставуваат механизми за да се оневозможи пристап на овластените лица до личните податоци и информатичко комуникациската опрема со права различни од тие за кои се авторизирани.

Администраторот на информацискиот систем кој е овластен со Актот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци може да доделува, менува или да го одзема авторизираниот пристап до личните податоци и информатичко комуникациската опрема само во согласност со критериумите кои се утврдени од страна на контролорот.

Управување со медиуми

Со медиумите треба да се овозможи идентификација и евидентирање на категориите на лични податоци и истите треба да се чуваат на локација до која пристап имаат само овластени лица утврдени во Актот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци.

Пренесување на медиумите надвор од работните простории може да се врши само со претходно писмено овластување од страна на контролорот.

Уништување, бришење или чистење на медиумот

По пренесувањето на личните податоци од медиумот или по истекот на определениот рок за чување, медиумот треба да се уништи, избрише или да се исчисти од личните податоци снимени на него.

Уништувањето на медиумот се врши со механичко разделување на неговите составни делови, при што истиот повторно да не може да биде употреблив.

Бришењето или чистењето на медиумот треба да се изврши на начин што ќе оневозможи понатамошно обновување на снимените лични податоци.

Сигурносни копии и повторно враќање на зачувани лични податоци

Контролорот е одговорен за проверка на примената на Правилата за

начинот на правење на сигурносна копија, архивирање и чување, како и за повторното враќање на зачуваните лични податоци во кои задолжително треба да се содржани постапките за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

При примената на основното ниво на технички и организациски мерки сигурносни копии задолжително се прават секој работен ден и на крајот од работната седмица, а само по потреба и секој последен работен ден во месецот.

Сигурносните копии задолжително се прават на начин со кој ќе се гарантира постојана можност за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

Сигурносните копии се чуваат надвор од просторијата во која се наоѓаат серверите и треба да се физички и криптографски заштитени, заради оневозможување на каква било модификација.

III. Средно ниво на технички и организациски мерки

Покрај наведените мерки во глава II, во случај на примена на средно ниво на технички и организациски мерки, во документацијата за технички и организациски мерки, задолжително треба да се содржани и постапки за вршење на периодични контроли, а заради следење на усогласеноста на работењето на контролорот со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки, како и за мерките кои треба да се преземат при користење на медиумите.

Во случај на средно ниво информацискиот систем и информатичката инфраструктура на контролорот задолжително подлежат на внатрешна и надворешна контрола со цел да се провери дали постапките и упатствата содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на личните податоци.

Надворешна контрола на информацискиот систем и информатичката инфраструктура се врши на секои три години од страна независно трето правно лице, а внатрешна контрола секоја година.

Во извештаите од извршената контрола задолжително треба да има и мислење за тоа во колкава мера постапките и упатствата содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на личните податоци, да се наведени констатираните недостатоци, како и предложените неопходни корективни или дополнителни мерки за нивно отстранување. Воедно, треба да се содржани и податоците и фактите врз основа на кои е изготвено мислењето

и се предложени мерките за отстранување на констатираните недостатоци. Вака изработениот извештајот се анализира од страна на офицерот за заштита на личните податоци, кој му доставува предлози на контролорот за преземање на потребните корективни или дополнителни мерки, за отстранување на констатираните недостатоци.

Евидентирање на авторизираниот пристап (логови)

Во случај на примена на средно ниво, контролорот треба да води евиденција за секој авторизиран пристап која треба да ги содржи особено следните податоци: име и презиме на овластеното лице, работна станица од каде се пристапува до информацискиот систем, датум и време на пристапување, лични податоци кон кои е пристапено, видот на пристапот со операциите кои се преземени при обработка на податоците, запис за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем. Во оваа евиденција се внесуваат и податоци за идентификување на информацискиот систем од кој се врши надворешен обид за пристап во оперативните функции или личните податоци без потребното ниво на авторизација.

Операциите кои овозможуваат евидентирање на податоците треба да се контролираат од страна на офицерот за заштита на личните податоци и истите да не може да се деактивираат.

Евиденцијата за авторизиран пристап треба да се чува најмалку пет години.

Контрола на физички пристап

Во случај на примена на средно ниво на ТОМ, во документацијата за технички и организациски мерки покрај наведеното за основно ниво, контролорот треба да определи критериуми и за овластените лица кои можат да имаат пристап до просториите каде е сместен информацискиот систем.

Управување со медиуми

Контролорот треба да воспостави систем за евидентирање на медиумите кои се примаат или испраќаат од страна на контролорот со цел да овозможи директна или индиректна идентификација на видот на медиумот кој е примен, датум и време на примање, испраќач, број на медиуми кои се примени, вид на документ кој е снимен на медиумот, начин на испраќање на медиумот, име и презиме на лицето овластено за прием на медиумот.

За пренесените медиуми надвор од работните простории на контролорот, треба да бидат преземени неопходни мерки за да се спречи неовластено обработување на личните податоци снимени на нив.

Евидентирање на инциденти

Во Правилата за пријавување, реакција и санирање на инциденти, контролорот ги определува постапките кои се применуваат за повторно враќање на личните податоци и начинот на евидентирање на овластените лица кои ги извршиле операциите за повторно враќање на личните податоци, категориите на личните податоци кои се вратени и кои биле рачно внесени при враќањето.

За повторното враќање на личните податоци, контролорот издава писмено овластување на овластените лица за да ги извршат операциите за враќање на податоците.

Сигурносни копии

Во случај на примена на средно ниво на ТОМ, сигурносните копии задолжително се прават секој работен ден, на крајот од работната седмица и секој последен работен ден во месецот при што истите треба да се чуваат надвор од објектот во кој се наоѓаат серверите или персоналните компјутери во кои се сместени збирките на лични податоци за кои се прави сигурносна копија. Во ваков случај сигурносните копии треба да бидат обезбедени со соодветни технички и организациски мерки, согласно документацијата за технички и организациски мерки при што меѓусебните права и обврски на контролорот и правното, односно физичкото лице каде се чуваат сигурносните копии, треба да бидат уредени со договор во писмена форма, кој задолжително ќе содржи технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци.

Тестирање на информацискиот систем

Контролорот задолжително врши тестирање на информацискиот систем пред неговото имплементирање или по извршените промени со цел да се провери дали системот обезбедува тајност и заштита на обработката на личните податоци согласно со документацијата за технички и организациски мерки и прописите за заштита на личните податоци при што тестирањето се врши преку обработка на документи кои содржат имагинарни лични податоци од страна на независно трето правно лице.

IV. Високо ниво на технички и оргъанизациски мерки

Сертификациони податоци

Во случај на примена на високо ниво на ТОМ покрај мерките од основното и средното, контролорот може да применува и други технички мерки за тајност и заштита на обработката на личните податоци, преку примена на сертификациони постапки согласно прописите за податоците во електронски облик и електронски потпис.

Пренесување на медиуми

Медиумите можат да се пренесуваат надвор од работните простории само ако личните податоци се криптирани или ако се заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи, при што само администраторот на информацискиот систем може да ги декриптира или лице овластено од него.

Пренесување на личните податоци преку електронско-комуникациска мрежа

Личните податоци можат да се пренесуваат преку електронско - комуникациска мрежа само ако се криптирани или ако се посебно заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи при преносот.

V. Рачна обработка на личните податоци

1. Основно ниво на технички и оргъанизациски мерки

Одредбите кои се однесуваат на обработувачот на збирки на лични податоци, класифицирањето на нивоата на организациски мерки, организациските мерки, информирањето за заштита на личните податоци и обврските на овластените лица (без администраторот) и евидентирањето на инциденти (членовите 3, 5, 6, 7, 10, 12, 14, 15 и 16 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на

обработката на личните податоци), соодветно се применуваат и при друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел на збирка на лични податоци.

Пристап до документите

Пристапот до документите треба биде ограничен само за овластени лица на контролорот при што за пристапувањето задолжително треба да се воспостават механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува.

Доколку е потребен пристап на друго лице до документите тогаш треба да бидат воспоставени соодветни процедури за таа цел во документацијата за техничките и организациските мерки.

Правило „чисто биро“

Контролорот задолжително го применува правилото „чисто биро“ при обработката на личните податоци содржани во документите за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Чување на документи

Чувањето на документите треба да се врши на начин што ќе се применат соодветни механизми за попречување на секое неовластено отворање. Во случај кога физичките карактеристики на документите не дозволуваат примена на ваквите мерки, контролорот треба да примени други мерки кои што ќе го спречат секој неовластен пристап до документите.

Уништување на документи

Уништувањето на документите се врши со ситнење или со друг начин, при што истите повторно да не можат да бидат употребливи, за што комисиски се составува записник кој ги содржи сите податоци за целосна идентификација на документот како и за категориите на личните податоци содржани во истиот.

2. Средно ниво на технички и организациски мерки

Контрола

Правилата за периодични контроли и контрола на информацискиот систем (членови 23 и 25 о Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци) треба соодветно се применуваат и при друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел на збирка на лични податоци.

Начин на чување на документите

Во случај на средно ниво, плакарите (орманите), картотеките или другата опрема за чување на документи задолжително треба да бидат сместени во простории заклучени со соодветни заштитни механизми. Просториите треба да бидат заклучени и за периодот кога документите не се обработуваат од овластените лица. Ако физичките карактеристики на просториите не дозволуваат примена на вакви мерки, контролорот треба да примени други мерки за да се спречи секој неовластен пристап до документите.

3. Високо ниво на технички и организациски мерки

Копирање или умножување на документите

Копирањето или умножувањето на документите може да се врши единствено со контрола на овластени лица определени со претходно писмено овластување од страна на контролорот.

Пренесување на документи

Во случај на физички пренос на документите контролорот задолжително презема мерки за нивна заштита од неовластен пристап или ракување со личните податоци содржани во документите кои е пренесуваат.

5.2. ПРАВИЛНИК ЗА ВИДЕО НАДЗОР

Вовед

Одредбите на Законот за заштита на личните податоци се применуваат и на обработката на личните податоци преку вршење на видео надзор. Законот за заштита на личните податоци утврдува дека контролорот кој врши видео надзор е должен да истакне известување кое мора да биде јасно, видливо и истакнато на начин што им овозможува на субјектите на лични податоци да се запознаат со вршењето на видео надзорот. Известувањето задолжително содржи информација:

- дека се врши видео надзор;
- за името на контролорот кој го врши видео надзорот и
- за начинот на кој може да се добијат информации за тоа каде и колку време се чуваат снимките од системот за видео надзор.

Контролорот може да врши видео надзор само на просторот кој е доволен за исполнување на целите за кои е поставен.

Снимките направени при вршење на видео надзор се чуваат до исполнување на целите за кои се врши, но не подолго од 30 дена, освен ако со друг закон не е предвиден подолг рок.

Видео надзор може да се врши во службени или деловни простории ако тоа е потребно за:

- заштита на животот или здравјето на луѓето;
- заштита на сопственоста;
- заштита на животот и здравјето на вработените поради природата на работата или
- обезбедување на контрола над влегувањето и излегувањето од службените или деловните простории.

Секој контролорот кој планира или воспоставил видео надзор е должен да го уреди начинот на вршењето на видео надзор со посебен акт.

Контролорот задолжително ги известува вработените за вршење на видео надзор во службени или деловни простории.

Видео надзорот не смее да се врши во гардероби, соблекувални, санитарни јазли, лифтови и други слични простории.

Законот утврдува дека директорот на Дирекцијата за заштита на личните податоци ги пропишува содржината и формата на актот за вршење

на видео надзор. Имајќи го во предвид овој факт Дирекцијата има донесено Правилник за содржината и формата на актот за начинот на вршење на видео надзор кој е објавен во „Службен весник на Република Македонија“ бр.158/2010. Со овој Правилник е пропишана содржината и формата на актот за начинот на вршење на видео надзор кој треба да го имаат донесено и да го применуваат сите контролори кои вршат обработка на личните податоци преку видео надзор. На овој начин се постигнува унифицирана примена на правилата за видео надзор.

Во овој Правилник е утврдено дека неговите одредби ќе се применуваат и при обработка на личните податоци преку вршење на видео надзор од страна на обработувачите на збирките на лични податоци. Имајќи во предвид дека согласно Законот за приватно обезбедување, правното лице кое дејноста приватно обезбедување ја врши во вид на давање на услуги, обезбедувањето го врши врз основа на договор за приватно обезбедување што го склучува со корисникот на услугата во писмена форма, произлегува дека правните лице кои вршат приватно обезбедување ќе се јавуваат (најчесто) како обработувачи и дека и за нив важат правилата утврдени во посочениот Правилник за содржината и формата на актот за начинот на вршење на видео надзор.

Оттука, подолу во овој текст се дадени одредбите кои задолжително треба да ги содржи секој акт со кој се уредува видео надзорот.

II. *Содржина и форма на актои за начини на вршење на видео надзор*

Актот за начинот на вршење на видео надзор задолжително треба да содржи: правен основ за неговото донесување, наслов на актот, основни одредби со опис на системот за вршење на видео надзор, цел, односно цели на обработка на личните податоци, категории на лични податоци, давање и пренос на лични податоци обработени преку системот за вршење видео надзор, технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци преку системот за вршење на видео надзор, овластени лица за обработка на лични податоци преку системот за вршење на видео надзор, изјава за тајност и заштита на обработката на личните податоци преку системот за вршење на видео надзор, рок на чување на снимките од видео надзорот, известување за вршење на видео надзор, технички спецификации на опремата, план каде е поставен системот за вршење на видео надзор и преодни и завршни одредби.

Во правниот основ за донесување на актот за начинот на вршење на видео надзор, се наведува членот од Законот за заштита на личните податоци (член 9-б став 2) или друг закон кој е основ за донесување на актот,

бројот на Службениот весник на Република Македонија каде е објавен законот, кој го донесува актот, како и датумот на неговото донесување.

Насловот на актот за начинот на вршење на видео надзор е „Правилник за начинот на вршење на видео надзор на _____ (назив на контролорот)“.

Во основните одредби се утврдува краток опис на содржината на актот за начинот на вршење на видео надзор со опис на системот за вршење на видео надзор (на пример: преку колку камери се врши видео надзорот, наративен опис каде и како се поставени камерите, каде се чуваат снимките, на каков медиум, колку време, кој има пристап до нив, се утврдува и целта, односно целите за обработка на личните податоци преку вршењето на видео надзор во смисла на одредбите од член 9-б став 1 од Законот за заштита на личните податоци и сл.).

Контролорот задолжително треба да има и изработена анализа на целта, односно целите за која се поставува видео надзорот пред започнување на процесот за воспоставување на систем за вршење на видео надзор. Анализата треба да ги содржи причините за поставување на видео надзорот со образложение на потребата за исполнување на целта, односно целите во смисла на одредбите од член 9-б став 1 од Законот за заштита на личните податоци, како и опис на недвижните и движните ствари кои ќе се заштитиуваат со поставувањето на видео надзорот.

III. Технички и орѓанизациски мерки за обезбедување тајноста и заштитата на обработката на личните податоци преку системот за вршење на видео надзор

Контролорот задолжително ги определува техничките и организационските мерки за обезбедување тајност и заштита на обработката на личните податоци преку системот за вршење на видео надзор, согласно Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци, со давање на опис за преземените технички и организациски мерки.

За пристапот и увидот до личните податоци обработени преку системот за вршење на видео надзор контролорот задолжително води евиденција, која ги содржи следните податоци:

- Име и презиме на овластеното лице;
- Датум и време на пристапување;
- Цел за пристапување;
- Датум и час на направената снимка кон која се пристапува;
- Датум и време, назив и седиште на корисникот на кого му е дадена

снимката од видео надзорот;

- Вид на медиумот во кој е содржана снимката од видео надзорот и
- Други податоци согласно член 27 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци.

Пристап и увид до личните податоци обработени преку системот за вршење на видео надзор можат да имаат само овластени лица од страна на контролорот кои пред нивното отпочнување со работа треба своерачно да потпишат изјава за тајност и заштита на обработката на личните податоци преку системот за вршење на видео надзор.

Снимките направени при вршење на видео надзорот можат да се чуваат до исполнување на целта, односно целите за кои се врши, но не подолго од 30 дена при што истите по истекот на рокот автоматски треба да се бришат од медиумот на кој што се чуваат. Снимките од видео надзорот може да се чуваат подолго од 30 дена ако тоа е потребно согласно закон, но не подолго до исполнување на целта, односно целите.

Контролорот на видливо и јасно место истакнува известување дека се врши видео надзор во смисла на одредбите на член 9-а од Законот за заштита на личните податоци кое е составен дел на актот за начинот на вршење на видео надзор.

Техничката спецификација на опремата со која ќе се врши видео надзор, особено бројот на камерите, резолуцијата и квалитетот на сликата, видот на камерите, бројот и идентификацијата на работните станици со кои се пристапува до системот за видео надзор, како и бројот и идентификацијата на опремата со која се врши видео надзорот, треба задолжително да се наведе во актот за видео надзор.

Воедно во Планот каде е поставен системот за вршење на видео надзор графички треба да се прикаже начинот на поставеност на видео камерите, просторот каде се врши видео надзорот, аголот на покриеност на просторот опфатен со видео надзорот, како и карта со локациите на местата каде што се поставени камерите.

IV. Обрасци**Образец 1**

Врз основа на одредбите од Законот за заштита на личните податоци („Службен весник на Република Македонија“ бр. 7/05, 103/08, 124/10 и 135/11), на ден _____ 20__ година ја давам следнава

ИЗЈАВА**за тајност и заштита на обработката на личните податоци преку
системот за спроведување на видео надзор**

Јас, долу потпишаниот/ата, _____ (име и презиме) на работно место / во улога на _____ (назив на работното место/улогата) во _____, согласно со Правилникот за начинот на спроведување на видео надзор во _____, се обврзувам дека:

- ќе ги применувам правилата за заштита на личните податоци во текот на спроведувањето на видео надзорот;
- ќе ги применувам техничките и организациските мерки за обезбедување на тајност и заштита на обработката на личните податоци и дека ќе ги чувам личните податоци и мерките за нивна заштита како доверливи;
- ќе ги применувам техничките и организациските мерки за пристап и увид во личните податоци кои се обработени преку системот за спроведување на видео надзор со кои се оневозможува неовластен и неевидентен пристап и увид во снимките од системот за видео надзор;
- ќе извршувам обработка на личните податоци во согласност со упатствата на контролорот;
- на трети лица, освен на контролорот, како и на други лица на контролорот нема да му откријам било каков личен податок од снимката на видео надзорот или било каков друг личен податок кој ми е достапен и кој што го дознав или ќе го дознам во текот на спроведувањето на видео надзорот во Министерството, освен ако со закон не е поинаку предвидено.

Име и презиме:

Потпис

Врска: Овластување број _____ / 20__.

Потпишаната Изјава се приложува и се чува заедно со референтното овластување.

Образец 2

Известување за спроведување на видео надзор



**Објектот е под
видео надзор**

Контролор: _____

Информации: +389 2 _____

Образец 3

Врз основа на одредбите од член ____ од Правилникот за начинот на вршење на видео надзор во _____, на ден _____ 20__ година _____ го дава следново:

О В Л А С Т У В А Њ Е**за пристап и увид во снимките направени и обработени преку системот за вршење на видео надзор**

Се овластува, *(име и презиме)*, на работно место/во улога на *(назив на работното место/улогата)* во _____, во согласност со Правилникот за начинот на вршење на видео надзор во _____, за пристапување и увид во снимките направени и обработени преку системот за вршење на видео надзор, заради:

(причина за давање на овластувањето и можни дојолнишелни овластувања)

Овластувањето се дава за период: од _____ 20__ до _____ 20__ година.

Број на овластувањето: _____ / 20__.

Управител:

Администратор на системот:

Потпис

Датум и потпис

6

ПРАКТИЧЕН ДЕЛ

Планирање и инсталирање на системи за техничко обезбедување

- 6.1. Систем за детекција и дојава на најраник, кражба, напад и
паника **197**
- 6.2. Системи за детекција, дојава и гасење на пожар **205**
- 6.3. CCTV практичен водич **213**
- 6.4. Основен водич за планирање и изведба на систем за
контрола на пристап **221**



6.1. СИСТЕМ ЗА ДЕТЕКЦИЈА И ДОЈАВА НА НАТРАПНИК, КРАЖБА, НАПАД И ПАНИКА

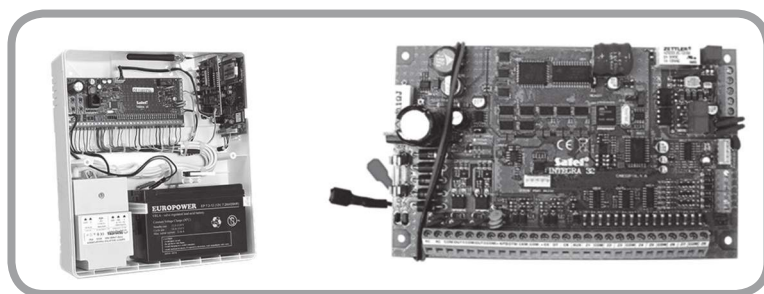
Уредите или помагалата за детекција на натрапник, кражба се составени од повеќе различни компоненти поврзани помеѓу себе и образуваат таканаречен **-СИСТЕМ ЗА ДЕТЕКЦИЈА-** или повеќе познат како систем за алармирање, односно Алармен Систем.

Основни компоненти на системот се:

6. Микропроцесорска алармна централа.
7. Тастатура- шифратор.
8. Детектори – сензори.
9. Сирена
10. Мрежно и резервно напојување
11. Инсталација – кабли
12. Медиум за комуникација (телефонска линија, интернет, радио врска, GSM мрежа).

Микропроцесорска алармна централа.

Алармната централа е уред кои ги обединува – поврзува сите компоненти на системот и е еден од најзначајните делови на истиот.

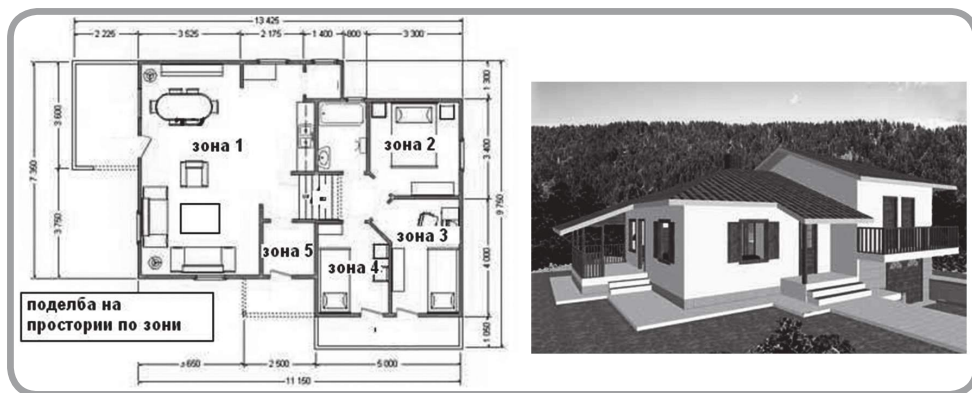


Слика 6.105.

Во светот постојат повеќе производители на алармни централи, а тие се разликуваат според нивните основни карактеристики и големина и тоа :

1. Број на зони.

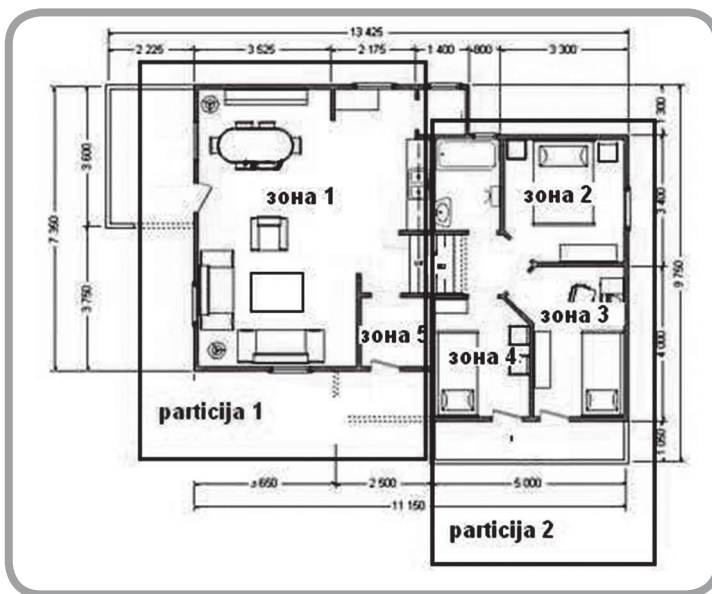
Зона е однапред определен простор што се штити/обезбедува, може да биде канцеларија, соба , дел од магациски простор, влез, ходник или друго во кој се поставува детектор/сензор означен со истиот број на зоната .



Слика 6.106.

2. Број на џарџиции (можносџ за џоделба на џовеке независни делови).

Алармната Централа може да се подели во две, четири, осум шеснаесет, тريسет и две и повеќе независни делови кој можат различно да се управуваат активираат, деактивираат со различни кодови/шифри во различно време.



Слика 6.107.

На сликата 6.3. е означена поделбата на зони по партиции, што значи зона 5 и зона 1 сме ги групирале во партиција 1, а зона 2,3 и 4 сме ги групирале во партиција 2.

3. Број на шифри/корисници

Алармните центри се разликуваат и по бројот на шифри/кодови што можат да се користат. Секоја централа има различен број на кодови, а според техничките карактеристики се врши и избор на која централа ќе се вгради во објектот.

Тастатура – шифратор

Овој уред е составен дел на системот, а преку него со помош на код/шифра се активира-вклучува или деактивира-исклучува централата. Тастатурата користи и за програмирање на централата, на нејзе има вградено и сигнализација за одреден статус. Во зависност дали сигнализацијата е со LED диода или LCD дисплеј, така е и поделбата на видот/типот на тастатурата.



Слика 6.108.

Детектори – Сензори

Уреди кои ќе ни помогнат да откриеме или детектираме:

- отварање на врата или прозор,
- вибрации од механички удари,
- кршење на стакло,

- присуство на топло крвно суштество-човек,
- појава на дим и или зголемување на температура над 60°C,
- присуство или надојдување на вода,
- промена на температура (температурен) сензор,
- и често се произведуваат комбинирани сензори на некој од горе наведените два или три во еден сензор.

ги нарекуваме детектори или сензори, а тие можат да бидат :

магнетен сензор



гласбрејк сензор



вибро сензор



PIR сензор (пасивен инфра црвен)



димно оптички сензор



сензор за вода



температурен сензор

паник тастер



Сирени

Уреди за звучно известување или сирена се дел од алармен систем. Тие се делат на два типа :

- Надворешни сирени, со и без резервно напојување – батерија.



- Внатрешни сирени со и без резервно напојување – батерија.



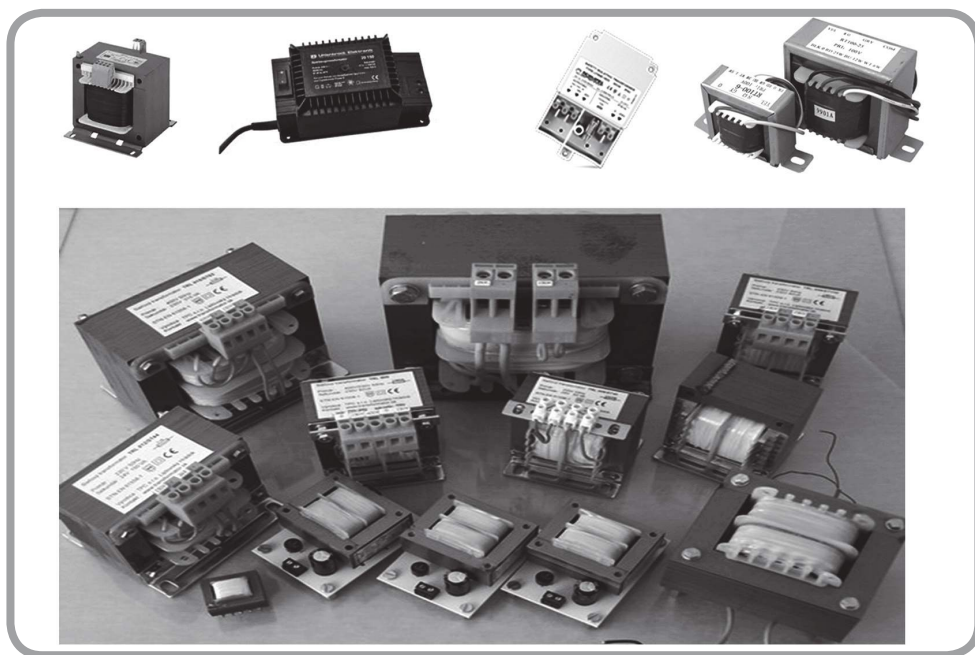
Постојат и сирени со вградено трепкачко светло – флешер, кои служи да го означат објектот што се обезбедува.

Мрежно и резервно напојување.

Еден од најважните и неопходни фактори за да функционира еден безбедносен систем е електрична енергија. Што значи дека објектот во кој треба да се изгради – инсталира безбедносен систем мора да поседува прописен електричен мрежен приклучок 220-240 волти.

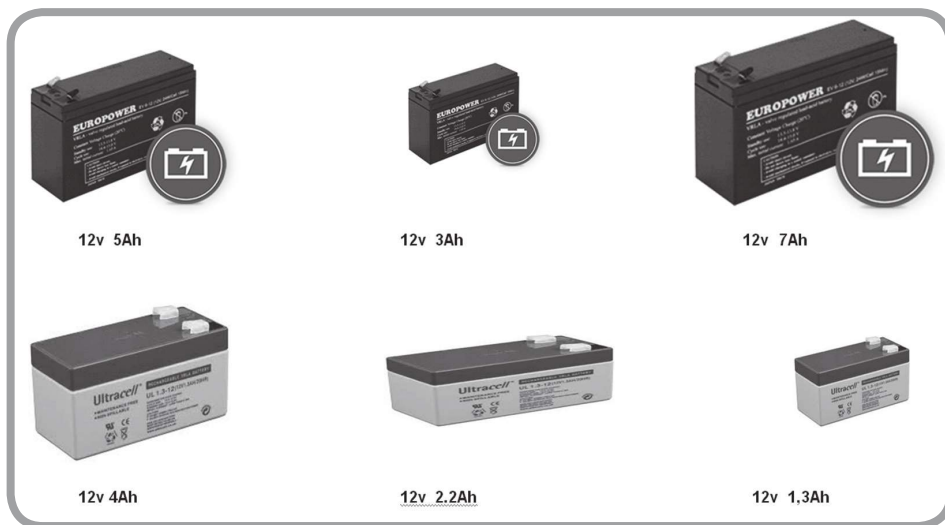
Алармните системи се слабострујни потрошувачи кој работат на 16-18 волти , па за таа цел се користат трансформатори за да го трансформираат напонот од 220-240 волти на 16-18 волти.

НАПОМЕНА:(секој производител дефинира на колкав напон работи неговата централа)



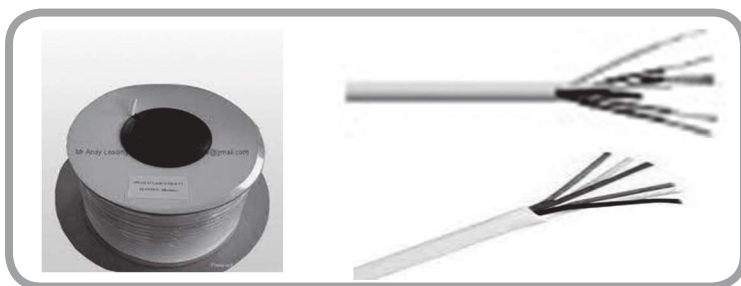
Во случај кога има недостаток или одреден дефект на мрежното напојување производителите на системите предвиделе можност за резервно напојување со акумулатори - батерии .

Акумулатори - Батерии



Инсталации – Кабли

За да можат сите составни делови на еден систем да си разменуваат информации, статус, состојба, напони, контакти и др. треба меѓусебно да се поврзано со проводник – кабел – инсталација. Најчесто во алармните системи се користи 6 (шест) жилен кабел за поврзување на компонентите/сензорите и 3 (тро) жилен кабел за мрежно напојување.



На пазарот постојат и безжични алармни системи кои не користат кабли за меѓусебно поврзување.

Медиум за комуникација (телефонска линија, интернет, радио врска, GSM мрежа).

Еден алармен систем за да може да се поврзе, односно за да испрати информација до мониторинг центар на Агенцијата за Обезбедување потребно е некаков начин односно медиум, неколку од нив се :

1. Телефонска линија PSTN.
2. GSM мобилна мрежа.
3. Интернет TCP/IP
4. Радио врска

На објекти со поголем ризик се користат истовремено или како резервен два и повеќе начини за комуникација

6.2. СИСТЕМИ ЗА ДЕТЕКЦИЈА, ДОЈАВА И ГАСЕЊЕ НА ПОЖАР

Уредите или помагалата за детекција на оган, дим, покачување на температура се составени од повеќе различни компоненти поврзани помеѓу себе и образуваат таканаречен **-СИСТЕМ ЗА ДЕТЕКЦИЈА НА ПОЖАР-** или повеќе познат како **ПРОТИВ ПОЖАРЕН** систем, скратено **ПП систем**.

Основни компоненти на системот се:

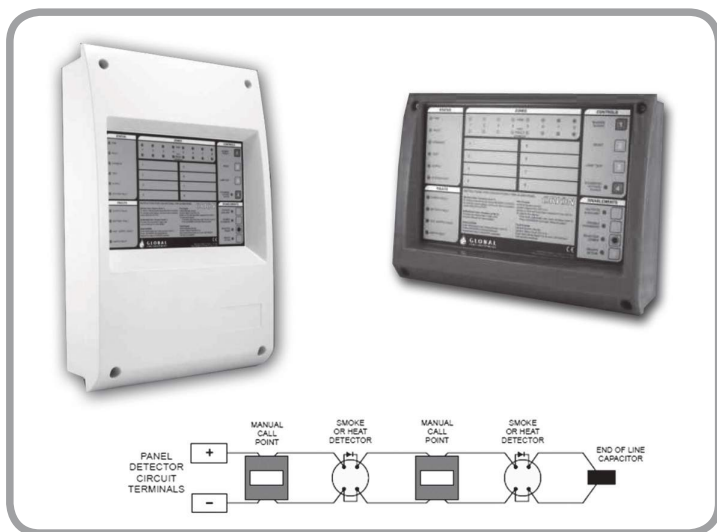
13. Против Пожарна централа..
14. Детектори – сензори – рачни јавувачи.
15. Сирени
16. Мрежно и резервно напојување
17. Инсталација – кабли
18. Медиум за комуникација (телефонска линија, интернет, радио врска, GSM мрежа).

Против Пожарна централа

ПП централа е уред кои ги обединува – поврзува сите компоненти на системот и е еден од најзначајните делови на истиот.

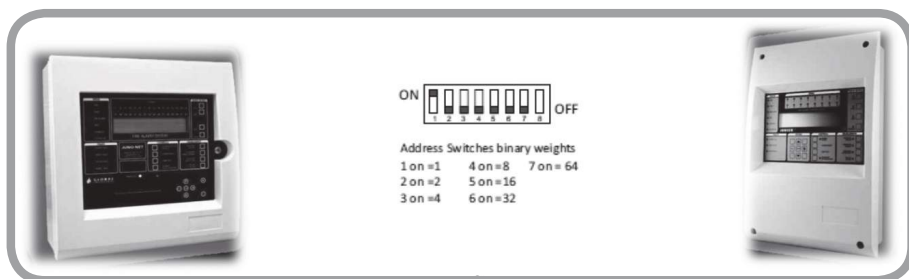
Во светот постојат повеќе производители на ПП центри, а тие се разликуваат според нивните основни карактеристики и големина, а се делат на:

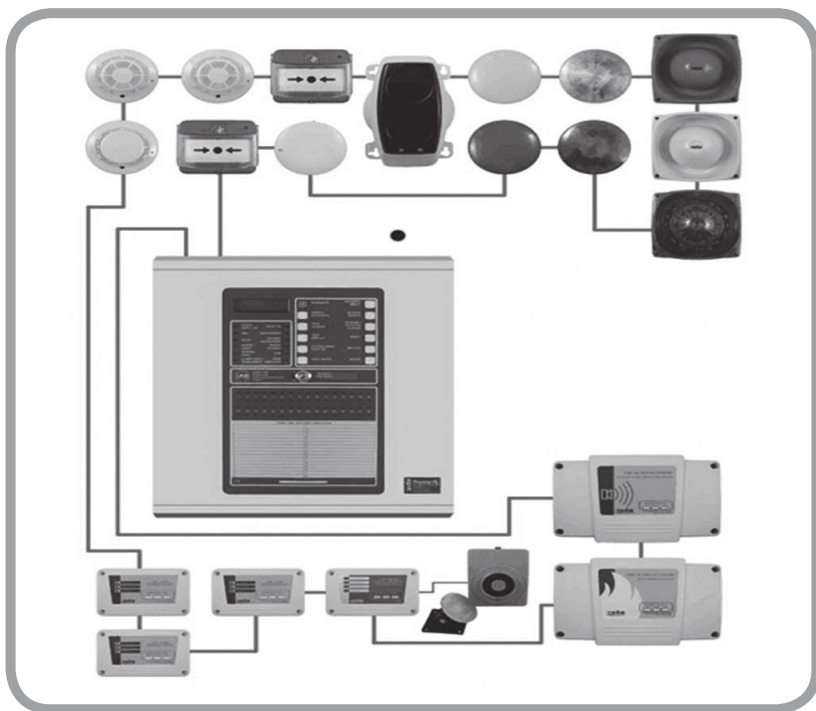
- Конвенционална ПП централа.
 - (оваа централа може да има 2,4,8 или повеќе зони, а во една зона можат да се поврзат околу 27-30 детектори – сензори. Било кој од сензорите во една зона ако се активира ќе ја отвори таа зона – што значи дека локацијата за настанатиот пожар е потешко да се лоцира).



■ Аналогно адресабилна ПП централа

- (ова централа за разлика од Конвенционалната може да биде со 1,2,3,4 и повеќе јамки (лупови) на кој можат да се поврзат околу 125-127 детектори појамка. Сите сензори имаат своја адреса и многу лесно може да се лоцира неговата местоположба).





Детектори – Сензори – Рачни јавувачи

Уреди кои ќе ни помогнат да откриеме или детектираме:

- појава на дим – ДИМНО ОПТИЧКИ
- појава на оган – светлина
- зголемување на температура над 60°C – ТЕРМИЧКИ.
- Детекција на гасови
- комбинирани сензори , комбинација на некој од горе наведените два или три типа во еден сензор.
- Рачни јавувачи

ги нарекуваме Против Пожарни детектори - сензори, а тие се делат на :

- Аналогно адресабилни ПП детектори и
- Конвекционални ПП детектори.

Според шийот на централата на која треба да се поврзи.



ПП сензори и подножје за истите

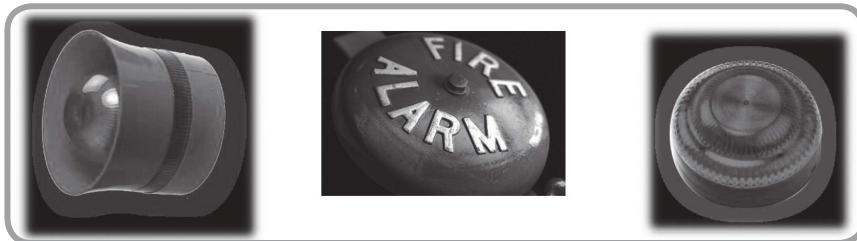


Рачни Јавувачи

Сирени

Уреди за звучно известување или сирена се дел од Против Пожарен систем. Тие се делат на два типа :

- Внатрешни сирени со и без резервно напојување – батерија.



- Надворешни сирени, со и без резервно напојување – батерија.



Постојат и сирени со вградено трепкачко светло – флешер, кои служи да го означат објектот што се обезбедува.

Мрежно и резервно напојување.

Еден од најважните и неопходни фактори за да функционира еден безбедносен систем е електрична енергија. Што значи дека објектот во кој треба да се изгради – инсталира безбедносен систем мора да поседува прописен електричен мрежен приклучок 220-240 волти.

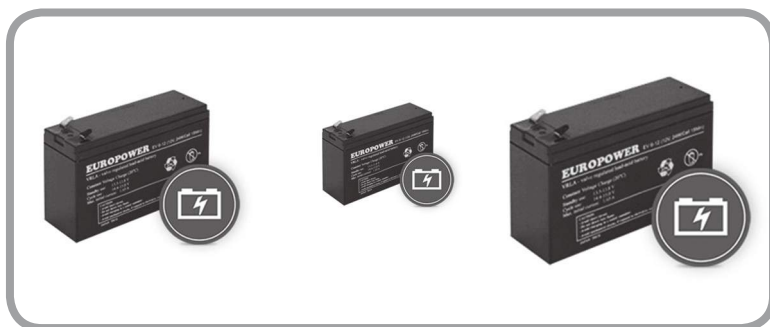
Системи се слабо струјни потрошувачи кој работат на 12- 24 волти , па за таа цел се користат трансформатори за да го трансформираат напонот од 220-240 волти .

НАПОМЕНА: (секој производител дефинира на колкав напон работи неговата централа)



Во случај кога има недостаток или одреден дефект на мрежното напојување производителите на системите предвиделе можност за резервно напојување со акумулатори - батерии .

Акумулатори - Батерии



Инсѝалации – Кабли

За да можат сите составни делови на еден систем да си разменуваат информации , статус , состојба, напони, контакти и др. треба меѓусебно да се поврзано со проводник – кабел – инсталација. Најчесто во системи се користи 2 (дво) и 4 (четири) жилен кабел, тешко горечки или незапалив за поврзување на компонентите/сензорите и 3 (тро) жилен кабел за мрежно напојување.



Медиум за комуникација (телефонска линија, интернет, радио врска, GSM мрежа).

Еден систем за да може да се поврзе, односно за да испрати информација до мониторинг центар на Агенцијата за Обезбедување потребно е некаков начин односно медиум, неколку од нив се :

1. Телефонска линија PSTN.
2. GSM мобилна мрежа.
3. Интернет TCP/IP
4. Радио врска

На објекти со поголем ризик се користат истовремено или како резервен два и повеќе начини за комуникација.

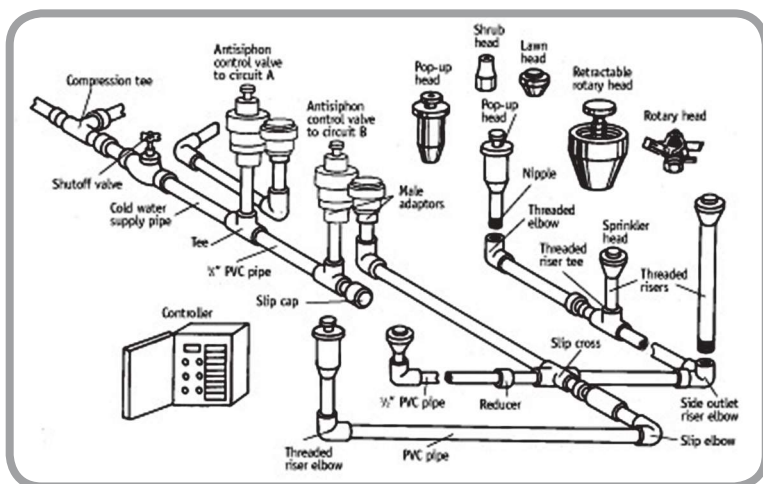
Гасење на Пожар

После извршената дојава за настанат пожар на одредена локација, треба да се пристапи кон негово гасење рачно или автоматизирано .

Рачното гасење нормално во зависност од неговата јачина и големина може да биде со помош на вода, песок, ткаенина кебе за удушвање со противпожарен апарат ,како на сликата подолу. Автоматското гасење може да биде со систем на вода со инсталирани цевки и распрскувачи на температура или електрични вентили, испустање на пена , гас, прав.



Системи за автоматско гаснење



6.3. CCTV ПРАКТИЧЕН ВОДИЧ

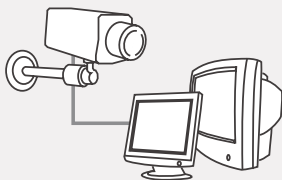
Изборот на вистинскиот тип на CCTV систем за видео надзор може да биде збунувачки на почетокот. Овој водич ќе ви одговори на повеќето ваши прашања.

- | | |
|---|------------------------------|
| 1 | Цели на системот |
| 2 | Избор на CCTV камери |
| 3 | Опрема за контрола и снимање |
| 4 | Мониторинг |
| 5 | Додатоци |

1. ОДЛУКА ЗА ЦЕЛИТЕ НА CCTV СИСТЕМОТ ЗА ВИДЕО НАДЗОР

САМО НАДЗОР

Ви треба да надгледувате една или повеќе камери на екранот



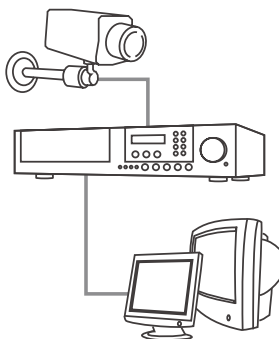
Госпоѓата X е стара и живее сама. Нејзе и е потребен CCTV систем за да види кој е пред вратата или долу пред влезот

Господинот и госпоѓата уживаат во гледањето на притице. Тие изградиле куќичка за прици на крајот од нивната градина и потребен им е CCTV систем за нивно надгледување

На младиот брачен пар им е потребен безжичен CCTV систем за да ги надгледуваат нивните деца во градината.
Потребни им е да ги надгледуваат на преносен монитор или да ги гледаат на нивниот ТВ приемник

НАДЗОР И СНИМАЊЕ

Потребно е да надгледувате една или повеќе камери и да снимате

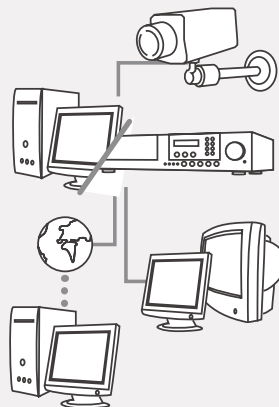


Инвеститор отворил продавница,магазин или услужна компанија и потребен му е CCTV систем за надзор над работата на вработените или однесувањето на клиентите. Исто така потребно е да му се обезбеди пристап до докази и евидентиран материјал заради понатамошни дејствија или соработка со полициската екипа за криминал

Семејството поседува сопствена кука,стан, возило или друг објект. Нивниот имот е вадализиран или има реални можности за Тоа. Потребен им е CCTV систем за надзор за да се фатат прекршителите, или потенцијалните натрапници во времето кога семејството не е присутно на имотот.

НАДЗОР, СНИМАЊЕ И ДАЛЕЧИНСКО СЛЕДЕЊЕ

Потребно е да надгледувате една или повеќе камери, да снимате и да им пристапите преку Internet мрежата



Инвеститор отворил ланец од магазини,продавници, салони или експозитивно повеќе места.
Потребен му е CCTV систем за надзор на сите простори, локално и далечински за да има сознание какво е работењето на вработените како клиентите се услужени кога тој не е присутен. Тој истото сака да го следи и на својот лап-топ или мобилен телефон.

Вашiot клиент патува многу често надвор од своето на живеење. Тој сака да да има постојан надзор над својот дом, сака да биде известен и во тек со целосната сигурност на својот имот.
Сака да има увид и во моментите кога има дојава од упад на натрапници во просторот.

ИЗБОР НА СООДВЕТНИ КАМЕРИ

3. Избор на соодветни камери

Многу е важно да ја одберете вистинската - соодветна - камера за да се постигне индивидуалната работа. Следат повеќе фактори кои ќе ви помогнат во правиот избор на соодветна CCTV камера.

Надзор и контрола



Препознавање



Детекција



Идентификација



Вашите CCTV барања-услови за видео надзорот ќе одредат кои перформанси се потребни за вашите камери.

Најчести поплаки и разочарувања од karakteristikите на многу CCTV системи за видео надзор вклучуваат:

- субјектот е премногу мал, или не е во видното поле доволно долго време
- сликите се јасни и се надвор од фокусот или подвижните објекти се замаглени
- камерите не ја покриваат соодветната зона

Одбирате традиционална аналог или понов тип digital network (IP) камери конектирани директно на вашата LAN мрежа.

Формат на сликата

Најчест формат на сликата е КОЛОР PAL/NTSC во зависност од стандардот

Црно/Бела камера се одбира кога се работи за амбиент со многу слаба светлост а исто така се користат и камери со вградени Инфра Црвени диоди .

Day/Night Камерите се гледање во колор во текот на денот а црно/бело во текот на ноќта.

Инфра/црвените диоди I-R LEDs можат да осветлат различно растојание.

Постави си прашање:

Дали треба да се следи во текот на ноќта?

Дали условите на светло се менуваат често и многу?

Кој тип на светло има на објектот (ако постои)?

(на пример: Неонско, Халоген, Лед ...)

Намена

Што ќе следи камерата

Што сакате да опфати

Перформанси

Надзор и контрола на генералната состојба

☐

Детекција на личности и објекти

☐

Препознавање на личности

☐

Идентификација на личности

☐

Препознавање на бројот на регистарски таблички

☐

Тип

Аналог

☐

IP (Internet Protocol)

☐

Околина

Внатрешна

сува и стабилна собна температура

☐

Надворешна

влажно и променлива температура

☐

Отпорна на удар и саботажа

места со висок ризик на оштетување

☐

Начин на монтажа

Сидна

☐

Плафонска

☐

Останато

Формат на сликата

Колор

☐

Црно/Бела

☐

Inra Red/ Day/Night:

☐

Максимално растојание на видно поле потребно во мрачни услови(m) —



g Формат на камерата

Класична BOX	☐
Куполна / Dome	☐
Вртлива Pan/Tilt Dome	☐
Моторизирана Pan/Tilt/Zoom Dome	☐

h Тип на објективот
Видно поле на сликата

Фиксен објектив	☐
Променлив објектив	☐

Димензија на објективот:

Потребна максимална ширина (m) _____

Потребно максимално растојание(m) _____

i Видливост на камерата

Видлива/Робусни	☐
Скриена	☐
Мала/Дискретна	☐

i Квалитет на сликата

Стандардна/ под 420 TVL	☐
Висока/ над 420 TVL	☐

k Поврзување

Безжична	☐
Жичана :	
Оптички со конвертори	☐
Коаксијален кабел RG59	☐
Cat 5; Cat6 / LAN	☐

Растојание на каблите до опремата за контрола?
(на пр. до TV , DVR или NVR) _____

Тип на објективот:

Помала димензија на објектив, поширок агол на видно поле. Поголема дим. на објектив потесен агол

На пр. 3.6mm објектив = широк агол на гледање
12mm објектив = тесен агол на гледање

Што е аголот поширок , толку се помали објектите
Со потесен агол на гледање ќе бидат прикажани поголеми објекти.

Постави си прашање:

Кое е максималното видно растојание кое треба да биде фокусирано.
Која е максималната видна ширина во која треба да се обсервира во тој смер.

Видливост на камерата:

Видливи/Робусни CCTV
камери кои вообичаено се робусни во големо кукиште кои имаа визуелна доминација на објектот.

Скриени / Мали
многу мали или минијатурни вградени камери во друг предмет како во ПИР детектор ПП детектор, часовник, рамка...)
Мали дискретни камери
Камери со комплетарен дизајн со амбиентот обично се со средна големина. Тие се идеални за резидентни објекти или за канцелариски простори.

Постави си прашање:

Каде ќе биде поставена камерата?
Дали треба да биде скриена заради постигнување на совата цел?
Дали ќе го нарушува изгледот на амбиентот

Квалитет на сликата:

TVL (Телевизиски Линии) се број на хоризонтални линии генерирани од сигурносната камера и е мерка за резолуција на сликата или нејзината чистина. Повеќе TVL, подобар квалитет на сликата.

Постави си прашање:

Кој квалитет на слика е потребен за целта за која се поставува камерата?
Дали целта бара добра слика или генерално следење на околината?
Дали се потребни подоцнежни доказни слики и детали ?

Поврзување:

Постојат 4 начини за поврзување на CCTV камерите.

Безжична - Wireless преку 2.4 GHz аналог или преку LAN. Напомена : Комерцијаните уреди и камери засновани на ваквата конекција се нестабилни, со мал домет и несигурни.

Жичани,

- со поставување на инсталација со коаксијален кабел RG 59 (најчесто употребувани)

- со мрежен кабел Network Cat5 или Cat6 -

- понекогаш се користи и паричен кабел со употреба на специјални конвертори на импеданси -video balun

- Или најново со оптички кабел и конвертори

Постави си прашање:

Коку е едноставно да се постави инсталација?
Дали видливоста за врска или амбиентот ќе биде проблем?

ИЗБОР НА ОПРЕМА ЗА КОНТРОЛА И СНИМАЊЕ

3. Избор на опрема за контрола и снимање

→ единечно подесување
на камера

→ подесување на повеќе
камери

Опремата за контрола е потребна ако имате потреба да мониторирате повеќе од една камера или да снимате. Следуваат повеќе медиуми за снимање на видео сликите од камерите:

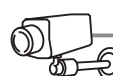
- 1 Video/DVD Recorder
- 2 Digital Video Recorder
- 3 PC Based Software
- 4 IP Camera Software

ССТV СИСТЕМ СО ВИДЕО / DVD РЕКОРДЕР

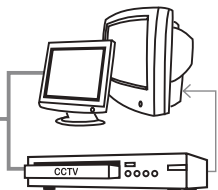
Една камера

Едноставно поврзете ја вашата камера (жичано или безжично) на видео рекордерот или DVD рекордерот/или мониторот.

Жичана врска



Безжична врска



3.1 УПОТРЕБА НА VIDEO/DVD РЕКОРДЕР

Употреба на Video /DVD Recorder или time lapse video recorder

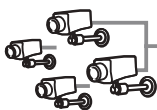
За употреба на Видео / ДВД или time lapse рекордерите потребно е да се приклучат и специјални префрлувачи (switcher) , квад уреди. (quad processor) или мултиплексери (multiplexer) за да се снимаат повеќе од една камера. Овие уреди снимаат со временски мултиплекс.

-Префрлувачот (Switcher) овозможува автоматски да се префрлува видео влезот на рекордерот помеѓу сите поврзани камери. Постојат и свичеви со аларм влезови што овозможува автоматско префрлање на снимањето на соодветен аларм влез адресиран на соодветна камера.

-Quad processors едноставно го дели екранот на 4 еднакви делови. Камерите можат да бидат истовремено снимани и следени на екранот.

-Multiplexers -от овозможува секое поле од камерите да биде следено самостојно или мултиплексно , со повеќе камери на екранот. Исто така може да овозможат секоја камера да се снима поединечно а во исто време да се гледа во живо, мултиплексно или поединечно.

Жичана врска



Безжична врска



Switcher
или Quad Processor
или Multiplexer

Постави си прашање:

Дали е потребно да се гледаат сите камери одеднаш
Дали треба да се следат сликите на цел екран поединечно?

- ☒ Едноставен за употреба
- ☒ Идеален за мали комерцијални системи

a Потребен е уред за контрола

- Префрлувач/Switcher ☐
- Квад спред/Quad Processor ☐
- Мултиплексер/Multiplexer ☐

b Каблирање

Растојание за каблирање
(вкупно помеѓу уредите) _____

3.2 CCTV СИСТЕМ СО ДИГИТАЛЕН ВИДЕО РЕКОРДЕР

- ☒ Решение се во едно
- ☒ Снимање на повеќе камери
- ☒ Претење на камерите во живо
- ☒ Лесна репродукција на снимки

a Број на видео влезови

- До 4 ☐
- До 8 ☐
- До 9 ☐
- До 12 ☐
- До 16 ☐

b Потребно време на снимање

Потребни пресметки :

- Големина на HDD ☐
- Број на камери ☐
- Брзината на слики во секунда на DVR от ☐
- Резолуција ☐
- Квалитет на снимката ☐
- Употребен метод на компресија ☐

c Дополнителни можности

- Детекција на движење ☐
- Motion Detection ☐
- Снимање само кога DVR софтверот детектира движење
- Вас-уп и опции на снимките
- Поврзување на DVR ☐
- USB поврзување со PC ☐
- Вграден CD/DVD writer ☐
- Мрежно ☐
- Removable Pen-drive ☐
- Далечинско следење ☐
- Аларм влезови/излези ☐

DVR приклучен на локална мрежа или Internet мрежа со опција за дополнително снимање

Жичана врска

Безжична врска

Забелешка

DVR-от е возможно да се следи и подесува локално приклучен на монитор (BNC или VGA) приклучок, или далечински преку мрежната и интернет врска

Потребно време на снимање

Должината на времето на снимање определено е од :

Големината на Hard Drive
DVR ите снимаат директно на хард дискот. Изборот на капацитетот на хард дискот тоа колку долго треба да се чува снимениот материјал (најмалку 7 дена , највеќе 30 дена)
Обично DVRите се подесуваат да ги преснимуваат новите снимки над старите за да се овозможи постојана архива на снимен материјал од определениот период.
Број на камери: Повеќето DVR уреди имаат 4, 8/9, или 16 видео влезови за камери

Број на слики во секунда Frame Rate
(fps - frames per second): 25 fps е нормална жива слика која се емитува на ТВ уредите Бројот на слики во секунда прикажана во карактеристиките на DVR уредите се дели на бројот на приклучените камери.
На пример 4 канален DVR со 100Fps овозможува 25 слики во сек. за секоја камера Со намалување на сликите во секунда се заштедува капацитетот на хард дискот. Резолуција и квалитет на снимање:
Колку е поквалитетна сликата, толку е поголем потребниот капацитет на хард дискот за зачувување на снимениот материјал.

Метод на компресија:

JPEG, MPEG, MPEG4, H-264

Метод со поголема компресија овозможува поголемо време за снимање на хард дискот

Постави си прашање:

Колку долго треба да се чуваат снимките за да се прегледа снимениот материјал?
Дали постои можност за back-up на снимениот материјал.

Далечинско следење

Следење на сликите од вашите камери преку Интернет мрежата или LAN возможно со DVRи кои имаат ethernet (RJ45) конектор_ и кои имаат вграден WEB Server .



Локација Локација 2

Забелешка:

Софтверот за далечински надзор вообичаено се испорачува од производителот на DVR уредите

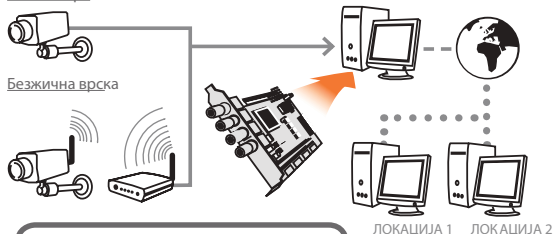
3.3 CCTV СИСТЕМ СО PC БАЗИРАНИ ИНТЕРФЕЈСИ И СОФТВЕРИ

CCTV Видео Надзор базиран на софтвер и вграден интерфејс во соодветна компјутерска конфигурација со орција на Интернет / LAN
Во ова варијанта CCTV сликите и снимките со употреба на постоечки PC. Интерфејсот (PC board) е инсталиран во соодветен слот во PC конфигурацијата и со помош на CD се инсталира софтверот за следење и снимање.

Вие можете да ги гледате вашите слики на екранот од PCто, да ги снимате на хард дискот и да ги прегледувате снимките. Исто така со креирање на серверска апликација на PCто до сликите и снимениот материјал може да пристапувате преку LAN/ Internet конекцијата.

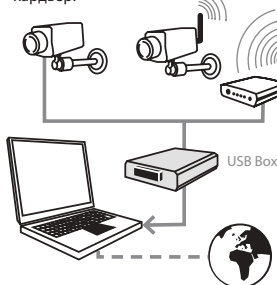
Жичана врска

Безжична врска



Со користење на Laptop ги гледате или го снимате снимениот материјал

За следење и снимање на сликите на Laptop потребно е да имате USBured без потреба да инсталирате дополнителен хардвер.



Дополнителни опции

PC Based -ПЦ базираните софтвери се со различни можности во зависност од производителот.

- Хибриден систем: Функција која поддржува и аналогни и IP камери • Прилагодливост за бројот на слики и резолуција за секоја камера • детекција на движење • Целосна контрола за време на репродукцијата: напред, враќање на снимката брзо и спор преглед, дигитален зум од било која зона на снимката • автоматско скенирање • Pan / Tilt / Zoom контрола • Интелигентно пред-снимање Pre-motion снимање • Повеќекратно маскирање зони
- Авто пребришување на складирање меморијата • Централно управување со конзоли
- Далеинско снимање и репродукција • Целосна контрола на снимките • следење на PDA и мобилен уред • Симултана репродукција во реално време • снимање и вмрежување
- Интелигентно пребарување • Визуелни пребарувања, ПОС, интеграција • E-mapping
- Email и звучна дојава на аларм • Лесен за употреба графички кориснички интерфејс
- ажурирање на софтвер онлајн и повеќе ..

- ☒ Решение се во едно
- ☒ Снимање на повеќе камери
- ☒ Следење на камерите во живо
- ☒ Лесно прегледување на снимките
- ☒ Употреба на постоечко PC или laptop за снимање на сликите
- ☒ Поевтина инсталација
- ☒ Одлична функционалност

a ПОДЕСУВАЊЕ НА СИСТЕМОТ

Преку Desktop PC

Преку Laptop PC

b БРОЈ НА ВИДЕО ВЛЕЗОВИ

- До 4 ☐
- До 8 ☐
- До 12 ☐
- До 16 ☐

c Потребна верзија

Мора да внимавате на:

- Бројот на камерите ☐
- Потребни број на слики во секунда ☐
- Барање за аудио снимка ☐
- Можностите на софтверот ☐

d Дополнителни фактори

Проверете го вашиот PC/Laptop за:

- Минимум барања на системот ☐
- Големината на Хард дискот и капацитет за снимање ☐
- CD/DVD снимач ☐
- Можноста на мрежата ☐

3.4 CCTV СИСТЕМ СО IP КАМЕРИ И IP МРЕЖНИ БАЗИРАНИ СНИМАЧИ

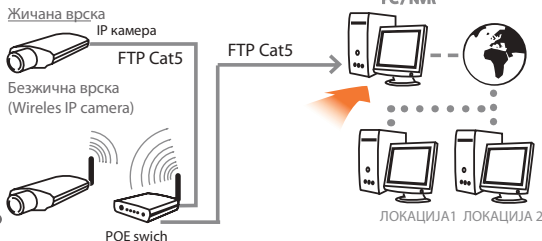
- ☒ Решение се во едно
- ☒ Снимање на неограничен број на камери и со многу поголем квалитет на снимките
- ☒ Следење на камерите во живо локално и далечински
- ☒ Лесно прегледување на снимките
- ☒ Употреба на постоечко PC или laptop за снимање на сликите и неограничен капацитет
- ☒ Одлична функционалност

а Број на камери во мрежата

Број на камери кои треба да се снимаат со софтверот или NVRot.

CCTV видео надзор со IP камери

Кога се употребуваат IP камери потребно е да се инсталира соодветен софтвер на PC конфигурација или да се употреби NVR (Network Video Recorder)



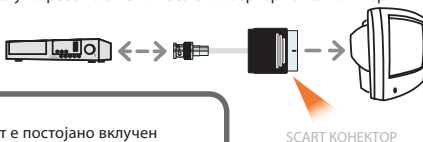
4 ИЗБОР НА МОНИТОР

а Опции

- Телевизор ☐
- CCTV Монитор ☐
- VGA / PC LCD Монитор ☐

Телевизиски монитор

Една камера може да биде приклучена на RCA(пин)или Scart конектор на вашиот телевизор.



Ако мониторот е постојано вклучен се препорачува да се употребат професионални монитори (CRT или LCD) кои се дизајнирани за подолга употреба 24/7

VGA / PC LCD

Ако DVRот има вграден VGA излез, тогаш тој се приклучува директно на PC мониторот.

Доколку нема VGA излез а сакате да го приклучите DVRот на PC мониторот тогаш користете BNC на VGA конвертор



Постави си прашање:

Која големина на екранот ви се бара?
Која резолуција на екран е потребна?
Каков влез за каков сигнал е потребен за да се приклучат уредите за снимање: BNC, RCA, SCART, VGA/PC?

Дали ви се бара дополнителен уред за следење на камерите и со каков приклучок?

ИЗБОР НА CCTV ДОДАТОЦИ

5. Избор на соодветни додатоци



Каблирање

Безжичен систем (2.4 GHz) ☐
Потребен е само напоен кабел

Жичен аналоген систем :
Коаксијален кабелRG59
(75 Ohm) +напоен кабел
PP/L 2x0.75mm ☐

Жичен IP систем :
FTP Cat 5 / LAN ☐

Растојание за каблирање
помеѓу:
-камерите и опремата
за снимање и контрола и
-помеѓу контролата ,рекордерот
и мониторот

Тип на напојни единици

Поединечни ☐

Заеднички/збирни ☐

Тип на држачи

Дополнителни барања за нив
Поедини камери се испора-
чуваат со соодветен држач

Потребно е соодветно
кукиште -надворешно
или внатрешно

Потребен е греач и вентилатор

Предупредувачки знаци

Да се постават на соодветно
место потребниот број на
знаци/налепници

Каква камера кој држач

Стандардна BOX камера ☐

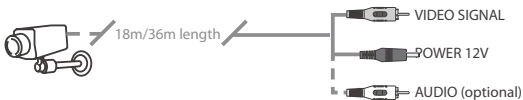
Куполна PTZ камера ☐

Надворешна камера ☐

Напојување и каблирање на системите

-Доколку безжичните системи се напојуваат на дистрибутивната
мрежа , за нив е потребен само кабел за напојување и тоа во
зависност од видот на камерата

- Кај жичените аналогни системи се употребува и комбиниран кабел
со кој истовремено се пренесува видео сигнал, аудио сигналот
и се напојува камерата . На завршетокот сите имаат соодветни конектори.
Вообичаената должина на ова каблирање е до 36 м.



- Најчесто употребувано каблирање кај аналогните жичани системи е
коаксијалниот кабел RG59 со кој може да се постигнат и растојанија до
300 м. За напојување кај помали должини се употребува напоен кабел
PP/L 2x0.75mm, а за поголеми должини и напоен кабел со поголем пресек.
Во продажба се наоѓа и комбиниран RG59+2x0.75mm кабел.

-Кабелот FTP Cat 5/LAN се употребува во CCTV IP системите. Вообичаено
овие камери се напојуваат преку FTP кабелот , но доколку не се поставува
дополнителен напоен кабел

Напојни единици на системите

-Поединечните напојни единици (адаптери)
се користат за напојување на камерите
кога се работи за помал број на камери,
или кога камерата се напојува локално
на местото каде се поставува.

-Кога се изведува систем со повеќе камери
и кога за камерите е потребно да се обез-
беди резервно напојување се употребуваат
заеднички/ збирни напојни единици
сместени во специјални напојни кутии со
поединечни осигурувачи за секоја камера

Постави си прашање

Дали е изводливо да со постави напојниот
кабел од секоја камера до централното
збирно место каде би можело да се постави
напојната кутија

Ознаки за предупредување налепници

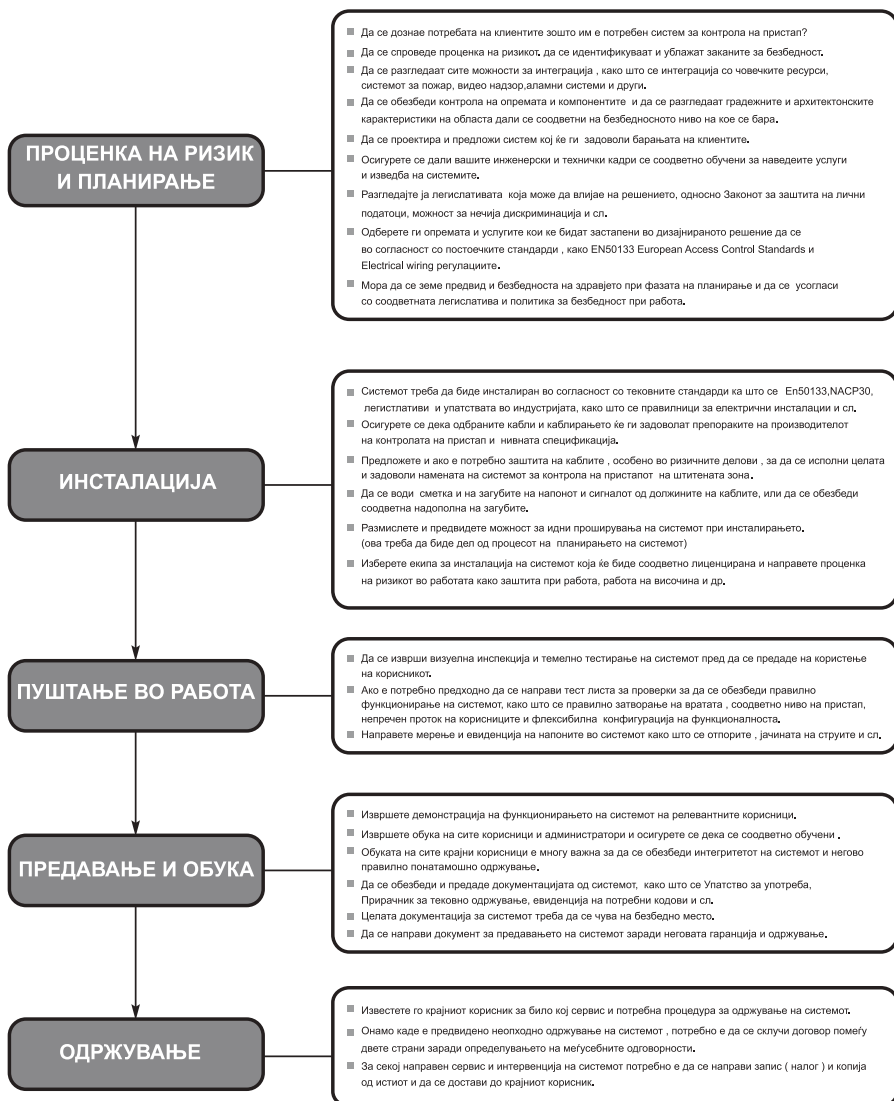
Заради заштита на личните
податоци знаците за поставен
систем за видео надзор реба да
бидат прикажани на јавни места
со сите потребни детали.

Потребен е правиот избор
на држач наспроти типот на
камерата и нејзината
местоположба

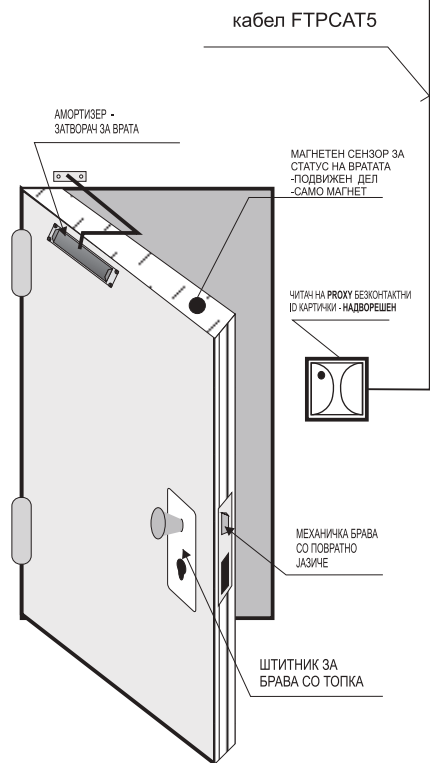
6.4. ОСНОВЕН ВОДИЧ ЗА ПЛАНИРАЊЕ И ИЗВЕДБА НА СИСТЕМ ЗА КОНТРОЛА НА ПРИСТАП

Контрола на пристап е значаен елемент на секој систем за физичка заштита. Општата цел на контролата на пристап е да се осигура дека само авторизираните и правилно најавените корисници, возила, и материјали ќе добијат пристап во областите и ќе излезат од областите за кои се бара заштита. За да се обезбеди ефективност на физичката заштита, контролата на пристап треба да се интегрира со други компоненти ка што се: физички бариери, детекција на упад и натрапници, системско откривање, проценка и процеси на пребарување. Заради тоа е потребно да постават и анализираат специфични услови за спроведување на мерките и технологијата за контрола на пристап.

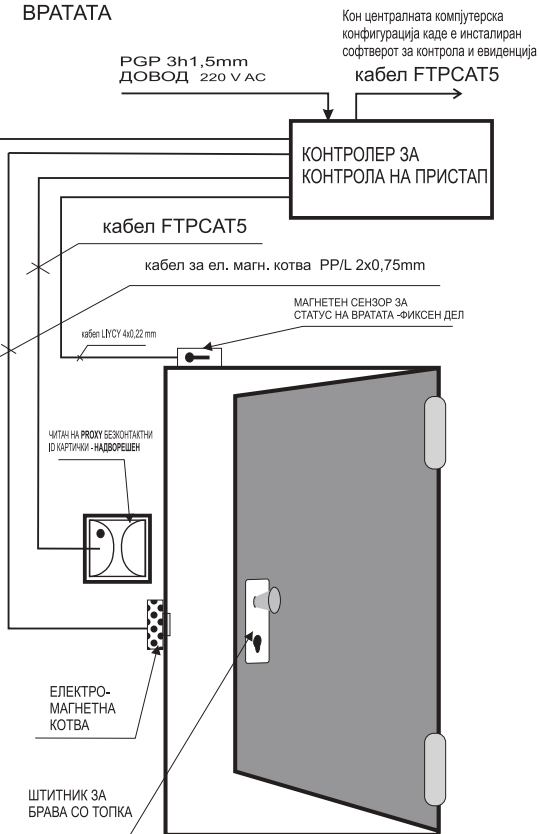
За да се контролира пристапот ефикасно, заштитените области мора прво да се идентификуваат. Откако овие области се идентификувани, неопходна е употреба на физички бариери на периметарот на идентификуваните области, треба да се спрени или одложи неовластен пристап и да се обезбедат средства за откривање и набљудување на сите обиди за неовластен пристап на персоналот, возила, и материјали надвор овие физички бариери. За да се обезбеди поддршка на овие операции и ги се задоволат барањата на системот за контрола на пристап, системите за физичка бариера треба да бидат дизајнирани за канализирање на движењето на лицата, возилата и материјалите за одредени локации на кои таков режим за работа се доделува. Следат дел од процедурите и правилата за изведба на системи за контрола на пристап.



ПОСТАВЕНОСТ НА ЕЛЕМЕНТИТЕ ОД НАДВОРЕШНА СТРАНА НА ВРАТАТА



ПОСТАВЕНОСТ НА ЕЛЕМЕНТИТЕ ОД ВНАТРЕШНА СТРАНА НА ВРАТАТА



НАЧИН НА ОТВОРАЊЕ НА ВРАТАТА - РАБОТЕН РЕЖИМ

- ОД НАДВОРЕШНАТА СТРАНА ПРИСТАПОТ Е МОЖЕН САМО СО ВАЛИДНА PROXY ID КАРТИЧКА
- ОД ВНАТРЕШНАТА СТРАНА ИЗЛЕГУВАЊЕТО Е МОЖНО САМО СО ВАЛИДНА PROXY ID КАРТИЧКА
- ВО СЛУЧАЈ НА ДЕФЕКТ НА СИСТЕМОТ ОТВОРАЊЕТО НА ВРАТАТА Е МОЖНО СО СООДВЕТЕН КЛУЧ ОД ЦИЛИНДЕРОТ СО ПОВЛЕКУВАЊЕ НА ЈАЗИЧЕТО

Напомена:

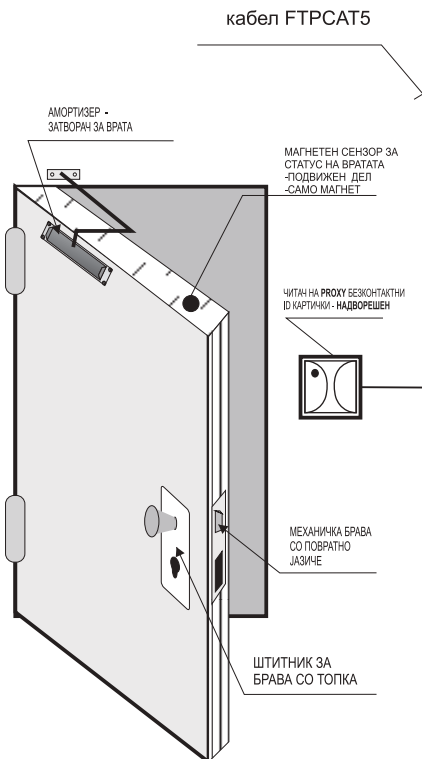
Во овој случај се евидентира секое влегување и излегување на корисниците на картичките во базата на централниот софтвер.

ПОСТАВЕНОСТ НА ЕЛЕМЕНТИТЕ НА СИСТЕМОТ ЗА КОНТРОЛА НА ПРИСТАП НА ВРАТАТА -ТИП 1

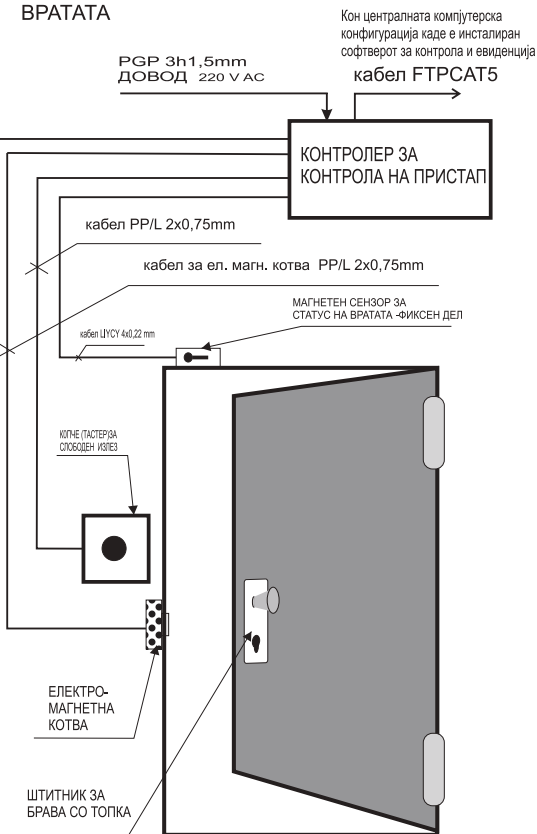
ПЛАНИРАЊЕ И ИНСТАЛИРАЊЕ НА СИСТЕМИ ЗА ТЕХНИЧКО ОБЕЗБЕДУВАЊЕ

Основен водич за планирање и изведба на систем за контрола на пристап

ПОСТАВЕНОСТ НА ЕЛЕМЕНТИТЕ ОД НАДВОРЕШНА СТРАНА НА ВРАТАТА



ПОСТАВЕНОСТ НА ЕЛЕМЕНТИТЕ ОД ВНАТРЕШНА СТРАНА НА ВРАТАТА



НАЧИН НА ОТВОРАЊЕ НА ВРАТАТА - РАБОТЕН РЕЖИМ

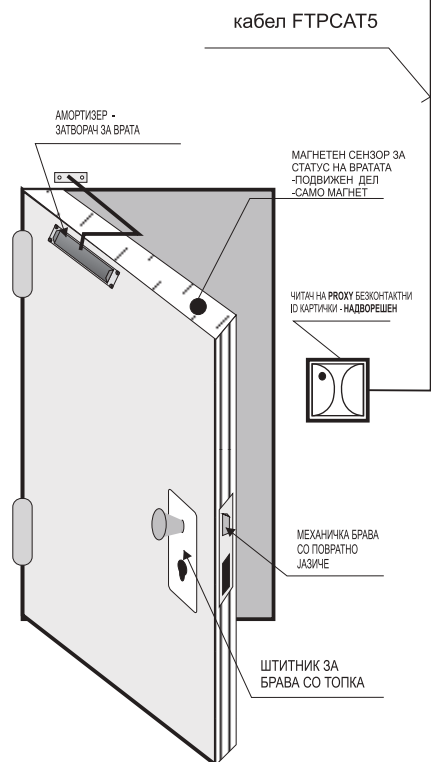
- ОД НАДВОРЕШНАТА СТРАНА ПРИСТАПОТ Е МОЖЕН САМО СО ВАЛИДНА PROXY ID КАРТИЧКА
- ОД ВНАТРЕШНАТА СТРАНА ИЗЛЕГУВАЊЕТО Е ОВОЗМОЖЕНО СО ПРИТИСКАЊЕ НА КОПЧЕ (ТАСТЕР) ЗА СЛОБОДЕН ИЗЛЕЗ
- ВО СЛУЧАЈ НА ДЕФЕКТ НА СИСТЕМОТ ОТВОРАЊЕТО НА ВРАТАТА Е МОЖНО СО СООДВЕТЕН КЛУЧ ОД ЦИЛИНДЕРОТ СО ПОВЛЕКУВАЊЕ НА ЈАЗИЧЕТО

Напомена:

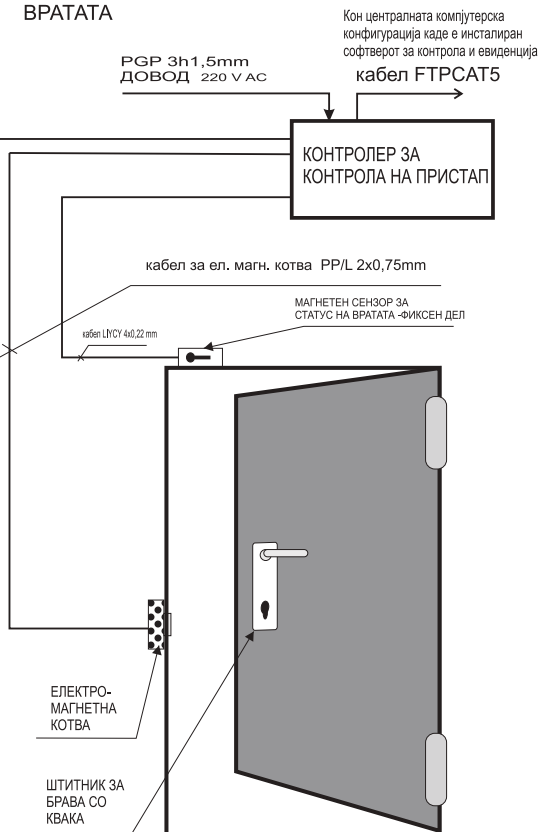
Во овој случај се евидентира само влегувањето на корисниците на картичките во базата на централниот софтвер. При излегување со притискање на тастерот за излез во базата се запишува секое притискање.

ПОСТАВЕНОСТ НА ЕЛЕМЕНТИТЕ НА СИСТЕМОТ ЗА КОНТРОЛ НА ПРИСТАП НА ВРАТАТА - ТИП 2

ПОСТАВЕНОСТ НА ЕЛЕМЕНТИТЕ ОД НАДВОРЕШНА СТРАНА НА ВРАТАТА



ПОСТАВЕНОСТ НА ЕЛЕМЕНТИТЕ ОД ВНАТРЕШНА СТРАНА НА ВРАТАТА



НАЧИН НА ОТВОРАЊЕ НА ВРАТАТА - РАБОТЕН РЕЖИМ

- ОД НАДВОРЕШНАТА СТРАНА ПРИСТАПОТ Е МОЖЕН САМО СО ВАЛИДНА PROXY ID КАРТИЧКА
- ОД ВНАТРЕШНАТА СТРАНА ИЗЛЕГУВАЊЕТО Е СЛОБОДНО СО ПОВЛЕКУВАЊЕ НА КВАКАТА.

- ВО СЛУЧАЈ НА ДЕФЕКТ НА СИСТЕМОТ ОТВОРАЊЕТО НА ВРАТАТА Е МОЖНО СО СООДВЕТЕН КЛУЧ ОД ЦИЛИНДЕРОТ СО ПОВЛЕКУВАЊЕ НА ЈАЗИЧЕТО

Напомена:

Во овој случај се евидентира само влегувањето на корисниците на картичките во базата на централниот софтвер. При излегување во базата на настани не се евидентира ништо.

ПОСТАВЕНОСТ НА ЕЛЕМЕНТИТЕ НА СИСТЕМОТ ЗА КОНТРОЛ НА ПРИСТАП НА ВРАТАТА -ТИП 3

Основен водич за планирање и изведба на систем за контрола на пристап

