



VALSTYBĖS ĮMONĖS TURTO BANKO

TECHNINIO STANDARTO

PRIEDAS AS (apsauginės signalizacijos)

1. BENDROSIOS NUOSTATOS

Apsaugos signalizacijos, vaizdo stebėjimo ir praėjimo kontrolės sistemos turi būti valdomos per vieną centralizuotą darbo vietą pastate – vieną serverį ar kompiuterį – montuojamą techninėje patalpoje arba apsaugos poste (jeigu yra). Projektuojant sistemas negali būti naudojama įranga, kuri atsakingų Lietuvos Respublikos, Europos sąjungos arba NATO institucijų yra pripažinta kaip nesaugia arba galinti kelti grėsmę dėl duomenų saugumui. Šioms sistemoms taip pat negali būti naudojama įranga, iš šalių, kurios Lietuvos Respublikos Vyriausybės, Seimo ar kitų atsakingų institucijų priimtais teisės aktais ar išleistomis rekomendacijomis yra pripažintos nepatikimomis. Turi būti vengiama naudoti abejotinos reputacijos gamintojų įranga – dėl įrangos gamintojų ir tiekėjų būtina derintis su Užsakovu.

Apsaugos signalizacijos, vaizdo stebėjimo ir praėjimo kontrolės sistemos turi būti atviro kodo principo. Sistemose turi būti galimybė be papildomų gamintojo apribojimų licencijavimui ir pan. komponuoti skirtingų gamintojų įrangą. Turto bankui turi būti suteikiami visi prisijungimai prie sistemų laisvam sistemų konfigūravimui ir nustatymų keitimui pagal sistemų galimybes. Sistemų ar jų komponentų gamintojai ar tiekėjai neturi pasilikti jokių išskirtinių teisių ir galimybių sistemų valdymui ir konfigūravimui, kurios apribotų laisvą sistemų naudojimą pagal Turto banko poreikius.

2. Apsaugos signalizacija

Apsaugos centralės:

Naudojamos adresinės, lengvai plečiamos ir programuojamos apsaugos centralės ir išplėtimo moduliai. Apsaugos centralės turi būti apjungiamos su gaisrinės saugos signalizacijos ir praėjimo kontrolės sistemomis pavojaus signalų priėmimui ir išsiuntimui į išorinį centralizuotą apsaugos postą. Įranga turi suteikti galimybę tiksliai nustatyti pažeidimo vietą pastate.

Apsaugos centralės montuojamos apsaugos poste arba kitoje su Užsakovu suderintoje vietoje.

Valdymo klaviatūros:

Apsaugos signalizacijos valdymo centralės diegiamos prie visų išėjimų iš pastato, įskyrus techninius išėjimus. Taip pat valdymo klaviatūros gali būti montuojamos pastato viduje šalia patekimo į atskiras pastato funkcines zonas (pvz.: konkretaus nuomininko patalpas, sandėliavimo patalpas ir pan.). Klaviatūra montuojama ant sienos akių lygyje, greta įėjimo durų.

Jutiklių išdėstymas:

Apsauginei signalizacijai įrengti naudojami judesio jutikliai, magnetiniai kontaktai ir stiklo dūžio jutikliai. Magnetiniai kontaktai montuojamos ant visų cokolinio ir pirmo aukšto langų ir įėjimo durų. Taip pat magnetiniai kontaktai montuojami ant kitų langų, kurių atstumas nuo apatinio lango angokraščio iki paviršiaus, ant kurio galima užlipti be specialių priemonių, yra mažesnis nei 3,5 m.

Judesio jutikliai ir stiklo dūžio jutikliai montuojami visose cokolinio ir pirmo aukšto patalpose besiribojančiose su išorinėmis atitvaromis ir turinčiose langų arba įėjimo iš lauko durų.

Apsaugos signalizacija turi būti jungiama į "TB tinklą" įrengiant reikiamus ryšio perdavimo sprendimus ir turėti galimybę įrengtais ryšiais perduoti informaciją apie įrangos veikimo statusą (suveikimus, gedimus, prisijungimus ir t.t).

Turi būti užtikrintas nenutrūkstamas sistemos veikimas, užtikrinantis veikimą ne mažiau kaip 2 val. nutrūkus centralizuotam elektros maitinimui.

3. Vaizdo stebėjimo sistema

Vaizdo stebėjimo sistema projektuojama ir įrengiama pastato perimetrai ir pagrindinio įėjimo į pastatą stebėjimui. Tuo tikslu projektuojamos IP spalvoto vaizdo kameros su infraraudonųjų spindulių pašvietimu. Pagrindinio įėjimo stebėjimui projektuojama vaizdo kamera šalia pagrindinio įėjimo durų.

Suderinus su Užsakovu, papildomos vaizdo kameros gali būti projektuojamos pagrindinio įėjimo hole nukreiptos į pagrindinio įėjimo durų stebėjimą.

Turi būti užtikrintas nenutrūkstamas sistemos veikimas, užtikrinantis veikimą ne mažiau kaip 2 val. nutrūkus centralizuotam elektros maitinimui.

Vaizdo įrašymo įrenginys įrengiamas apsaugos poste (jeigu toks yra) arba ryšio patalpoje komutacinėje spintoje. Turi būti sudaryta galimybė prie vaizdo įrašymo įrenginio prisijungti iš nutolusios darbo vietos WEB sąsajos pagalba. Nutolusios darbo vietos vartotojams turi būti galimybė nustatyti skirtingas vartotojo teises (administratorius, naudotojas ir pan.).

Iš nutolusios darbo vietos turi būti galimybė realiu laiku stebėti vaizdo kameromis stebimą aplinką, valdyti vaizdo kameras, atsukti vaizdą, keisti nustatymus, daryti vaizdo įrašų kopijas.

Ant objekto sienos, kuriame vykdomas vaizdo stebėjimas, pakabinti lentelės su užrašu „Asmenų ir turto apsaugos tikslu patalpose vykdomas vaizdo stebėjimas“, nurodant įmonę, įmonės kodą, telefoną, atsakingo už asmens duomenų apsaugą elektroninį paštą ir telefono numerį, kuriuo galima kreiptis norint gauti informacijos ir sužinoti savo teises šiais klausimais.

4. Praėjimo kontrolės sistema

Praėjimo kontrolės sistema pastatuose diegiama tarp skirtingų pastato zonų (pvz. patekimui į skirtingų nuomininkų patalas, patekimui į padidintos saugumo zonas ir pan.), patekimams į pastatą, patekimo į uždarytą teritoriją vartų valdymui, turniketams ir pan. Praėjimo kontrolės diegimo apimtis kiekvienu atveju derinama su Užsakovo atstovu.

Sistema gali būti realizuojama per autonomiškai veikiančias belaides spynas, bei wireless ryšiu veikiančias belaides spynas arba sistemą valdomą per centrinį kontrolerį ir tarpinius išplėtimo kontrolerius. Sistema turi veikti RFID pagrindu, naudojant atstumines korteles arba žetonus. Bendruoju atveju sistemą sudaro:

- Programinė įranga;
- Kontroleriai (atsižvelgiant į sistemos tipą);
- Kortelių skaitytuvai;
- Atstuminės RFID kortelės (arba žetonai);
- Durų atidarymo mygtukai;
- Elektroninės spynos.

Programinė įranga turi užtikrinti tokius funkcionalumus:

- turėti galimybę prisijungti prie sistemos ir ją valdyti iš nutolusios darbo vietos per WEB sąsają;
- turi būti galimybė vienos sistemos lango pagalba valdyti visos pastato praėjimo kontrolės sistemos kontrolerių, kortelių ir kitų sistemos įrenginių bei vartotojų nustatymus – pridėti ir ištrinti vartotojus, keisti jiems suteiktas teises, keisti vartotojų duomenis, prie sistemos pridėti naujas įėjimo korteles;
- turi turėti galimybę nustatyti skirtingus programinės įrangos operatorius, suteikiant jiems skirtingas valdymo teises;
- turi turėti galimybę nustatyti skirtingus sistemos darbo režimus pagal pasirinktus kalendorinius ir laiko grafikus;
- Svečio funkcija – trumpalaikių leidimų suteikimas, kuriuo galiojimas baigiasi po nustatyto laikotarpio;
- Eksportavimo funkcija – duomenų (kas, kur kada ėjo) eksportavimas .xls arba .csv formatais.

Praėjimo kontrolės sistema turi būti lengvai plečiama ir turėti konkurencingą licencijavimo ir sistemos palaikymo kainodarą.

Turi būti užtikrintas nenutrūkstamas sistemos veikimas, užtikrinantis veikimą ne mažiau kaip 2 val. nutrūkus centralizuotam elektros maitinimui.

Praėjimo kontrolės sistemos išplėtimo (tarpiniai) kontroleriai montuojami virš pakabinamų lubų arba kitose lengvai nepasiekiamose vietose, tačiau turi būti užtikrinamas priejimas jų techniniam aptarnavimui. Centrinis kontroleris turi būti montuojamas apsaugos poste (jeigu toks yra) arba ryšio patalpoje šalia kitos apsaugos sistemos įrangos. Valdymas turi būti užtikrinamas iš nutolusios darbo vietos pastate ir už pastato ribų.

Praėjimo kontrolės sistema turi būti jungiama į "TB tinklą" įrengiant reikiamus ryšio perdavimo sprendimus ir turėti galimybę įrengtais ryšiais perduoti informaciją apie įrangos veikimo statusą (gedimus, prisijungimus ir t.t.), suteikti prieigą prie duomenų bazės ir ją koreguoti (įvesti vartotojus, korteles ir t.t.).

