VALSTYBĖS ĮMONĖS TURTO BANKO

TECHNINIO STANDARTO

PRIEDAS AS
(apsauginės signalizacijos)

2025 m.

TURINYS

1. ĮVADAS

Šiame standarte nustatyti bendrieji reikalavimai, keliami Turto banko valstybei nuosavybės teise priklausančio nekilnojamojo turto, administruojamų, valdomų ir prižiūrimų objektų apsaugos užtikrinimui.

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 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. TIKSLAS

Dokumento tikslas – sukurti organizacinius, teisinius ir techninius pagrindus, užtikrinant saugumą ir nepertraukiamą veiklą objektuose nuo projektinių išorinių grėsmių: pašalinių asmenų, trečiųjų asmenų. Apsaugos standartas apima visą Turto banko administruojamą bešeimininkį, konfiskuotą, valstybės paveldėtą, valstybei perduotą nekilnojamąjį turtą. Standartu siekiama nustatyti apsaugos bendruosius ir specialiuosius reikalavimus skirtingo apsaugos lygio objektams, kas leis užtikrinti ekonomiškesnę, veiksmingesnę, efektyvesnę Turto banko valdomų pastatų, patalpų ir statinių apsaugą. Šiame standarte pateikiama detalizuota informacija, būtina projektuojant ir įrengiant elektronines saugos sistemas, mechanines apsaugos priemones bei organizuojant ir vykdant objektų fizinę apsaugą. Standarte apsaugos organizavimo reglamentavimas užtikrins, kad turtas būtų valdomas veiksmingai, efektyviai, ekonomiškai, užtikrinant visuomenės interesų tenkinimą.

Apsaugos užtikrinimo principai

Objektų saugos sistema projektuojama, jos veikla organizuojama ir prižiūrima vadovaujantis šiais principais:

- **teisiniu saugos organizavimo ir veiklos pagrįstumu.** Objektų saugos procesas organizuojamas ir veikia griežtai laikantis Lietuvos Respublikos įstatymų bei kitų teisės aktų, vidaus tvarkomųjų dokumentų reikalavimų.
- **objektų saugos sistemos adekvatumu (proporcingumu).** Objekto saugos sistema projektuojama atsižvelgiant į projektines grėsmes ir galimą žalą bei priemonių pakankamumą šioms žaloms.
- **bendradarbiavimu.** Užtikrinant objektų apsaugą privaloma bendradarbiauti su teritorinėmis policijos įstaigomis, užtikrinant viešąją tvarką, administracinių teisės nusižengimų ir nusikalstamų veikų prevenciją ir atskleidimą.
- **apsaugos priemonių diferenciacija.** Objektų skirstymas pagal svarbą, galimą žalą ir atitinkamo objekto priskyrimas apsaugos lygiui leis pasiekti maksimalius rezultatus.
- **apsaugos priemonių kompleksiškumu.** Efektyvi objektų apsauga turi būti vykdoma panaudojant skirtingas apsaugos priemones, maksimaliai suderinant jų poveikį.

3. STANDARTIZUOTAS OBJEKTŲ SKIRSTYMAS Į APSAUGOS LYGIUS.

Šiuolaikinės objektų apsaugos sistemos uždavinys išspręsti specifines vykdančių turto valdymą ir naudojančių turtą saugumo problemas apsaugos priemonėmis. Atlikdami objekte vykdomos administracinės veiklos ir apsaugos priemonių analizę, nustatėme apsaugos standarto mato vieneto kriterijų, projektinę grėsmę („Design Basis Threat“ DBT), t.y. pašalinių ir trečiųjų asmenų galimą poveikį valdomam turtui. Vadovaudamiesi Turto banko parengtu pastatų, statinių ir jų priklausinių eksploatacinės techninės priežiūros paslaugų standartu padidinto saugumo valdomas, parduodamas turtas, laikinai neeksploatuojamas turtas, nenaudojamas, bešeimininkis turtas (toliau - objektai), buvo suskirstyti į penkis apsaugos lygius. Inicijuodami veiklos apsaugos srityje gerinimo iniciatyvas ir galimybę objektuose sumažinti saugumo pažeidžiamumus, įvertinę pašalinių, trečiųjų asmenų keliamą riziką objektams, nustatėme skirtingas (fizines, mechanines, inžinerines ir elektroninės) apsaugos priemones.

3.1. SAUGOMŲ OBJEKTŲ APSAUGOS LYGIAI

1. **Penktas objektų apsaugos lygis.** Padidinto saugumo objektai, valdomas turtas, kuriuose saugoma ir dirbama su įslaptinta informacija, valstybinės institucijos (ministerijos, kt.).
2. **Ketvirtas objektų apsaugos lygis**:
   - **2.1.** Valdomas turtas, kuris yra apskričių centrų miestų teritorijose ir naudojamas pilnu intensyvumu. Kuriame nuolatos būna naudotojai/lankytojai (jei objekte yra keli nuomininkai ar klientų aptarnavimo skyriai, padidinto saugumo patalpos (serverinės, archyvai, kt.), turi būti numatytos papildomos apsaugos priemonės;
   - **2.2.** Valdomas turtas, kuris yra laikinai nenaudojamas pagal paskirtį, nedaro įtakos kitų turtų eksploatacijai.
   - **2.3.** Valdomas turtas, kuris yra laikinai nenaudojamas pagal paskirtį, daro įtaką kitų turtų eksploatacijai, numatomos papildomos apsaugos priemonės patekimo apribojimui.
3. **Trečias objektų apsaugos lygis**. Nenaudojamas, naudojamas pagal paskirtį parduodamas turtas. Objekte įrengiamos tik būtiniausios apsaugos priemonės, papildomai investuojama į apsaugos priemones tik pagal atskirą pritarimą.
4. **Antras objektų apsaugos lygis**. Nenaudojamas arba nenaudojamas pagal paskirtį, dalinės nuosavybės, bešeimininkis parduodamas turtas. Objekte įrengiamos tik būtiniausios apsaugos priemonės, nereikia elektroninės įeigos kontrolės ir kitų saugos sistemų.
5. **Pirmas objektų apsaugos lygis**. Avarinės būklės požymių turintis turtas - numatomos apsaugos priemonės užkertančios pašalinių asmenų patekimui į objektą.

4. PAGRINDINĖS GALIOJANČIUOSE TEISĖS AKTUOSE IR ŠIAME STANDARTE NAUDOJAMOS BEI SUSIJUSIOS SĄVOKOS, TERMINAI, APIBRĖŽTYS IR SANTRUMPOS.

Objekto apsaugos postas - stacionari patalpa, kurioje pagal sudarytą grafiką budi apsaugos darbuotojai. Patalpoje įrengta elektroninės saugos sistemos valdymo, kontrolės ir atvaizdavimo įranga (centralės, apsaugos valdymo įrenginiai, vaizduokliai), kurios pagalba formuojami aktualių įvykių pranešimai susiję su objekto elektroninėmis saugos sistemomis ir perduodanti signalus GSM ryšiu į CSP.

Atitvaras – inžinerinė apsaugos priemonė, ribojanti asmens (-ų) ir/ar transporto priemonės (-ių) judėjimą.

Atsparumas (angl. *resilience*) – pavojų paveiktų elektroninių saugos sistemų ir mechaninių apsaugos priemonių techninis gebėjimas pasipriešinti neteisėtam fiziniam poveikiui laiku ir efektyviai, užtikrinant veiklą ir pagrindinių funkcijų išsaugojimą.

Atitvarinės konstrukcijos – patalpos sienos, grindys, perdengimai.

Apsauginė signalizacija – tai komponentų ir elementų visuma, įrengta pagal atitinkamą konfigūraciją ir galinti registruoti bei indikuoti nesankcionuotą patekimą.

Aktyvinis infraraudonųjų spindulių barjeras (IR barjeras) – sudaro poroje veikiantys infraraudonųjų spindulių siųstuvas ir imtuvas. Abu elementai orientuoti taip, kad siųstuvo siunčiami infraraudonieji spinduliai patektų į imtuvo aktyviąją zoną (langą). Kertant ar uždengus siųstuvo spindulį, įvyksta pavojaus signalo generavimas imtuvo signalo formavimo trakte.

Adresiniai gaisro detektoriai – šie temperatūriniai ir dūmų detektoriai analogiški paprastiems, tik papildomai savyje turi skaitmeninio elektroninio adreso priskyrimo modulį.

Centralė – tai elektroninis mikroprocesorinis įrenginys, kontroliuojantis elektrinės grandinės, prijungtos prie centralės įėjimo gnybtų, elektrinę būseną ir atitinkamai reaguojantis į tos būsenos pasikeitimą, suformuodamas atitinkamus programiškai priskirtus išėjimo signalus.

Centralizuoto stebėjimo pultas (CSP) – elektroninis mikroprocesorinis įrenginys, specializuotas kompiuteris, darbo sotis – serveris ar jų sistema, į kurį/kuriuos ryšių linijomis priimami pavojaus ir techniniai informaciniai pranešimai iš objektų saugos sistemų (suveikus saugomo objekto signalizacijai, perduodant/priimant objekto saugos sistemą stebėjimui į/iš CSP ir pan.). CSP 24 val./parą dirba operatorius(iai), kuris (ie) vadovaudamiesi vidinėmis veiklos instrukcijomis priima sprendimus dėl greitojo reagavimo grupės (GRG), apsaugos darbuotojo, objekto atsakingų asmenų ar kitų organizacijų ar asmenų informavimo apie įvykį, reikalingo fizinės saugos, GRG ar kitų specialiųjų pajėgų koordinavimo šalinant ar užkardant neteisėtus fizinius veiksmus, ekstremaliųjų ar ypatingųjų situacijų atvejais.

Dvigubo veikimo stiklo dūžio detektoriai – analizuoja aukšto ir žemo dažnio garsines bangas. Aukšto dažnio - atitinkančias dūžtančio stiklo spektrą, žemo dažnio - 2Hz- 20Hz smūginės bangos spektrą. Suveikimas įvyksta užregistravus abu signalus tuo pačiu metu.

Detektorius – aktyvūs elektroniniai įrenginiai ar pasyviniai mechaniniai prietaisai, fiksuojantys nustatyto parametro pokytį, pokyčio ribą ar faktą, ko pasekoje generuojamas signalas ar sujungiami gnybtai ar formuojamas elektrinės aktyvinės ar reaktyvinės varžos, šviesos radijo bangų atspindžio pokytis, kurie perduodami į kontrolinį priėmimo-perdavimo prietaisą.

Judesio detektorius – tai prietaisas, registruojantis fizinių kūnų mechaninius judesius jo kontroliuojamoje erdvėje ir formuojantis atitinkamą signalą.

Inžinerinės perimetrinės kliūtys – tai iš skirtingų medžiagų pagamintos tvoros.

Įeigos kontrolės sistema – tai techninių ir elektroninių įrenginių ar jų grupės bei programinių priemonių visuma, turinti duomenų valdiklį su skaitytuvu, kuris nustato asmens tapatybę surenkant kodą arba iš tam tikrų informacijos laikmenų - identifikatorių (brūkšninio kodo, magnetinės, radijo banginės RF-ID („radio frequency identification“), lustinės identifikacinės kortelės, RF-ID žetonai ir pan.) nuskaitydamas koduotą informaciją, arba pagal asmens individualius biometrinius parametrus, arba aukščiau išvardintų veiksmų ir priemonių kombinacija bei suteikia galimybę jam patekti į tam tikras teritorijas, patalpas arba jos nesuteikia.

Gaisro pavojaus mygtukai (rankiniai gaisriniai signalizatoriai) – skirti signalui apie gaisrą sukelti. Analoginiai-konvenciniai ir analoginiai-adresiniai. Analoginiai-konvenciniai gaisro mygtukai naudojami analoginės-konvencinės centralės signalizaciniame spindulyje, analoginiai-adresiniai naudojami adresinės centralės kilpoje su jam priskirtu adresu.

Gaisro aptikimo ir signalizavimo sistema – tai techninė apsaugos priemonė, susidedanti iš gaisro detektoriaus (-ų), centrinio įrenginio, valdymo modulio ir/ar kitų priemonių, skirta gaisro aptikimui ir signalizavimui.

Elektroninė apsauga – saugomo objekto apsauga naudojant signalizacijos priemones, kai elektroninėmis priemonėmis gauti pranešimai apie signalizacijos suveikimą perduodami greitojo reagavimo ekipažui.

Mechaninės apsaugos priemonės – mechaniniai įrenginiai, kuriuos sudaro perimetriniai inžineriniai užtvarai, tvoros, vartai, pastatų perimetrinės dalies ir svarbiausių vidinių patalpų apsaugos priemonės skirtos įsibrovėlio užlaikymui, durys, jų tvirtinimas pagal atskirus durų elementus, įskaitant staktas, vyrius, spynos, apsauginės plėvelės ir plastikas, grotos, langų žaliuzės, kt.

Magnetinis kontaktas (MK) – poliarizuoti hermetiniame korpuse esantys sausi kontaktai, susijungiantys/atsijungiantys veikiant pastoviam magnetiniam laukui.

Mechaniniai kontaktai (K) – uždari ar atviri sausi mechaniniai kontaktai, jungtukai be padėties fiksacijos, skirti varstomų konstrukcijų atidarymo identifikavimui. Naudojami kaip komandiniai davikliai ar saugos zonų pažeidimo jutikliai.

Kombinuotas PIR+GB detektorius – viename korpuse sumontuoti PIR ir GB jutikliai.

Kombinuotas dvigubo veikimo detektorius PIR+MW – dvigubo veikimo pasyvus infraraudonų spindulių detektorius suderintas su aktyviu mikrobangų traktu. Suveikimo signalas išduodamas, kai suveikia abi dedamosios. Naudojamas klaidingu suveikimų mažinimui.

Optiniai dūmų detektoriai – panaudotas optinis siųstuvo - imtuvo traktas. Analizuoja oro skaidrumą ir, pasiekus kritinę ribą, generuoja suveikimo signalą.

Perimetras – tai saugomos teritorijos išorinis kontūras (riba);

Pavojaus signalizavimo priemonės – skambučiai, sirenos, optiniai signalizatoriai, šviesiniai tablo ir kt.

Pasyvus infraraudonųjų spindulių detektorius (PIR – „Passive Infrared“) – detektorius, kurio veikimo principas paremtas infraraudonų 700-1100nm ilgio bangų registravimu. Veidrodžio ar lęšio pagalba infraraudoni spinduliai iš aplinkos fokusuojami į IR imtuvą, kur generuojama elektros srovė. Jos padidėjimas, atsiradus šilumos šaltiniui, iššaukia pavojaus signalo atsiradimą.

Paprasto veikimo stiklo dūžio detektorius (GB – „Glass Break“) – tai prietaisas registruojantis ir analizuojantis aukšto dažnio garsinę bangą, atitinkančią dūžtančio stiklo spektrą ir formuojantis atitinkamą signalą.

Padidinto saugumo patalpos – serverinė, dokumentų saugykla (archyvas), techninės patalpos (elektros skydinės, dūmų šalinimo automatikos skydas, technologinės elektroninių ryšių komutacinės spintos, su laikoma įranga svarbia pastato valdymui ir vykdoma veiklai, patalpos.

Sabotažo (trikties, liesties) zona – tyčinio elektroninės saugos sistemos darbą trikdančios veikos (jungiamųjų kabelių pažeidimo, papildomų prietaisų nesankcionuoto prisijungimo, kontrolinės priėmimo-perdavimo įrangos ar jos komponentų, jutiklių ar signalizatorių ar kitų korpusų atidarymo) identifikavimo zona.

Sukamieji varteliai − elektromechaninis įrenginys, skirtas asmenų įleidimui/išleidimui iš Objekto. Sukamieji varteliai valdomi įeigos kontrolės sistema su identifikavimo priemonėmis (elektroninės įeigos kortelės, žetonai ir pan.).

Valdomas kelio užtvaras (šlagbaumas) − nuleidžiamas/pakeliamas barjeras, naudojamas reguliuoti transporto priemonių srautą per kontroliuojamą patekimo į objektą vietą. Užtvaras turi turėti aiškiai matomą perspėjimo švyturėlį, privalo būti automatizuotas, valdomas nuotoliniu būdu arba EĮKS.

Vaizdo stebėjimo sistema – saugos sistema ar sistemos dalis, skirta vaizdo informacijos fiksavimui vaizdo stebėjimo kameromis (juodai balto ar spalvoto vaizdo, stacionarių ar valdomų ir pan.), vaizdo informacijos apdorojimui (perjungimas, kvadratavimas, multipleksavimas, matricavimas ir pan.), apdorotos vaizdo informacijos kaupimui (įrašymui) skaitmeninėse laikmenose, vaizdo informacijos atvaizdavimui vaizduokliuose bei komunikacininių priemonių pagalba nuotoliniam perdavimui tikslu stebėti „gyvą“ vaizdą, peržiūrėti sukauptą vaizdo informaciją, informuoti apie aktualų įvykį arba kaupti (dubliuoti) aktualių įvykių vaizdo informaciją nutolusiose skaitmeninėse laikmenose bei vaizduokliuose.

Užpuolimo signalizavimo sistema – techninė apsaugos priemonė, susidedanti iš pavojaus mygtuko (-ų), valdymo modulio (-ų) ir/ar kitų priemonių, skirta nustatyti ir fiksuoti pavojaus mygtuko suveikimo įvykį bei perduoti signalą į vietinį ir (arba) centralizuotą stebėjimo pultą.

Užsklendimo įtaisas – tai mechanizmas, mechaninis įtaisas, kuris užrakina langą, duris ir jiems neleidžia atsidaryti, tačiau nebūtinai tai turi būti spyna.

Standarte naudojamos santrumpos:

- gaisro aptikimo ir signalizavimo sistema (GASS);
- apsauginė signalizacijos sistema (ASS);
- įeigos kontrolės sistema (ĮKS);
- vaizdo stebėjimo sistema (VSS);
- centralizuoto stebėjimo pultas (CSP);
- apsaugos postas (AP);
- apsaugos tarnyba (AT)
- Priešgaisrinės apsaugos ir gelbėjimo departamentas (PAGD)
- LST EN – Lietuvos ir Europos standartas.
- Nacionalinis standartas – nacionalinės standartizacijos institucijos priimtas visuomenei skirtas standartas.
- Tarptautinis standartas – tarptautinės standartizacijos organizacijos priimtas visuomenei skirtas standartas.

5. BENDRIEJI REIKALAVIMAI APSAUGOS PRIEMONIŲ PROJEKTAVIMUI IR ĮRENGIMUI.

1. Objektuose projektuojamos ir įrengiamos elektroninės saugos sistemos ir kitos apsaugos priemonės turi atitikti šios srities privalomų ir normatyvinių dokumentų, įstatymų, LST EN standartų, CE ir statybos techninių reglamentų ir šio apsaugos standarto reikalavimus.
2. Pasirenkant techninės ar programinės įrangos gamintojus, priežiūrą ir palaikymą vykdančius ar juos kontroliuojančius asmenis, kurie nelaikomi patikimais, vadovautis Lietuvos Respublikos Vyriausybės 2022 m. kovo 30 d. nutarimu Nr. 280. Galiojanti suvestinė redakcija (nuo 2022-12-30).
3. Projektuojant ir įrengiant GASS vadovaujamasi PAGD prie VRM 2007 m. vasario 22 d. Nr.1-66 su pakeitimais, 2012 m. birželio 29 d. direktoriaus įsakymu Nr.1-186 patvirtintais normatyviniais statinio saugos dokumentais. „Stacionariųjų gaisrų gesinimo sistemų projektavimo ir įrengimo taisyklės“.
4. Projektuojant ir įrengiant GASS vadovaujamasi PAGD prie VRM direktoriaus 2010 m. gruodžio 7 d. įsakymu Nr.1-338 patvirtintais “gaisrinės saugos pagrindiniai reikalavimai”.
5. Projektuojant ir įrengiant GASS vadovaujamasi PAGD prie VRM direktoriaus 2010 m. liepos 27 d. įsakymo Nr. 1-223 nauja redakcija „Bendrosios gaisrinės saugos taisyklės“.
6. Projektuojanti ir įrenginėjanti įmonė turi parengti techninį darbo ar darbo projektą vadovaujantis Statybos techniniu reglamentu STR 1.04.04:2017 „Statinio projektavimas, projekto ekspertizė”. Suvestinė redakcija 2020-09-22.
7. Projektavimo darbai turi būti vykdomi vadovaujantis galiojančiais teisės aktais, statybos techniniais reglamentais, valstybės valdymo institucijų patvirtintais reikalavimais ir šiuo apsaugos standartu.
8. Įrengiant objekte apsaugos priemones Turto banko inžinieriai atsakingi už savo objektus turi parengti techninę užduotį projektavimui.
9. Elektroninės įeigos kontrolės, vaizdo stebėjimo sistemos jungiamos į šioms sistemoms sukurtą uždarą, kompiuterinį tinklą, kurį valdo, administruoja ir prižiūri nuomininkas (vartotojas).
10. Visa techninė dokumentacija ir slaptažodžiai turi būti saugomi Granlund manager sistemoje ir prieinama tik objektą prižiūrinčiam inžinieriui, bei aptarnaujančiai įmonei.
11. Elektroninių saugos sistemų objektuose valdymui sukuriami kelių lygių vartotojai su savo slaptažodžiais. Administratoriaus, „master, instaler“ lygio sistemos vartotojai žinomi tik Turto banko atsakingam asmeniui, arba sukuriami laikini, tokio lygio slaptažodžiai – technines apsaugos sistemas prižiūrinčiai įmonei (pasibaigus sutarčiai, slaptažodžiai turi būti pakeisti), paprasto vartotojo lygio – nuomininko atstovui.
12. Jei nuomininkui perduodamas sistemų administravimas ir suteikiama tokio lygio prieiga prie sistemų valdymo, pasirašomas sutarties priedas su Turto banku dėl duomenų tvarkymo.
13. Objektuose, kuriuose dirbama su įslaptinta informacija elektronines saugos sistemas turi projektuoti įmonės, turinčios UAB Statybos produkcijos sertifikavimo centro (SPSC) išduotus ir galiojančius kvalifikacijos atestatus ir jų teisės pripažinimo dokumentus, suteikiančius teisę eiti jiems priskirtas pareigas, Valstybinės energetikos reguliavimo tarybos išduotą kvalifikacinį atestatą elektros įrenginių iki 1000 V įrengimo darbams.
14. Kvalifikacijos atestatus turinčių įmonių darbuotojams turi būti suteikta teisė eiti ypatingo statinio projekto dalies vadovo, ypatingo statinio projekto dalies vykdymo priežiūros vadovo pareigas. Projekto dalys: apsauginės signalizacijos, gaisrinės signalizacijos, procesų valdymas ir automatizacija. Specialieji statybos darbai: procesų valdymo ir automatizavimo sistemų įrengimas; statinio apsauginės signalizacijos, gaisrinės saugos (signalizacijos) inžinerinių sistemų įrengimas.
15. Objektuose, kuriuose saugoma įslaptinta informacija arba dirbama su įslaptinta informacija, teritorijos apsauga, pastato, patalpų apsaugos priemonių įrengimas vykdomas vadovaujantis LRV 2018 m. rugpjūčio 13 d. nutarimu Nr. 820 „Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo įgyvendinimas“ ir priedais Nr.2, Nr.3.
16. Visi elektrotechninėms bei automatikos sistemoms perduodami valdymo signalai turi būti suderinti su automatikos bei elektros projektų dalimis.
17. Įžeminimas ir viršįtampių apsauga projektuojama vadovaujantis Elektros įrenginių bendrųjų taisyklių reikalavimais.
18. VSS tinklo konfigūravimo ir papildymo aktyviąją telekomunikacinę įrangą konkrečiame objekte derinti su Užsakovu.
19. Objektuose skirtingas apsaugos (elektronines, fizines, mechanines, organizacines) priemones taikyti ir naudoti kartu.
20. Objektuose įrengtų elektroninių saugos sistemų aliarminių suveikimų pranešimai turi būti perduodami į vietinį apsaugos postą ir nutolusį apsaugos tarnybos CSP arba mobiliąją aplikaciją (debesis) dviem nepriklausomais GSM, IP ryšio kanalais.

21. Įrengiami komutatoriai turi atitikti LST EN standarto 50136-1, 50136-6 (Pavojaus signalizavimo sistemos. Pavojaus signalų perdavimo sistemos ir įranga) reikalavimus ir gebėti objektuose įrengtų elektroninių saugos sistemų aliarminių suveikimų pranešimus perduoti bevieliu ryšiu į vieną arba du apsaugos tarnybų CSP pultus kartu, arba į vieną pultą ir mobiliąją aplikaciją (debesis).
22. Objektų apsaugą turi vykdyti sutartiniu pagrindu veikianti apsaugos tarnyba ir apsaugos darbuotojai, turintys atitinkamą kvalifikaciją ir reglamentuojančiais teisės aktais suteiktą teisę vykdyti neginkluotą asmens ir turto apsaugą.
23. Atsižvelgus į Nacionalinio saugumo strategiją penkto ir ketvirto apsaugos lygio objektuose, valstybės institucijose ir nacionalinio saugumo požiūriu svarbiuose sektoriuose, įskaitant 5G infrastruktūrą, nebūtų naudojamos valstybių ar teritorijų, kurių tiekėjai, jų subtiekėjai, ūkio subjektai, kurių pajėgumais yra remiamasi, gamintojai, techninės ar programinės įrangos priežiūrą ir palaikymą vykdantys asmenys ar juos kontroliuojantys asmenys nelaikomi patikimais, o būtų naudojama Europos Sąjungos ir draugiškose NATO šalims gamintojų pagaminta techninė ar programinė įrangos.
24. Organizuojant ir vykdant viešuosius pirkimus vadovautis Lietuvos Respublikos Vyriausybės 2022 m. kovo 30 d. nutarimu Nr. 280. Suvestinė redakcija 2022-12-30.
25. Įrengiant vaizdo stebėjimo ir elektroninės įeigos kontrolės sistemas vadovautis Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo, Europos Sąjungos Bendrojo duomenų apsaugos reglamento (ES) 2016/679 reikalavimais.
26. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 820 patvirtintame „Įslaptintos informacijos fizinės apsaugos reikalavimų ir jų įgyvendinimo tvarkos apraše“ nustatyta tvarka. Patalpų, kuriose dirbama su įslaptinta informacija ar ji yra saugoma, apsaugos priemonių grupės atsparumo įsilaužimui balas nustatomas atsižvelgiant į patalpos sienų, perdangų, durų, langų, grotų, apsauginių žaliuzių, užraktų atsparumo įsilaužimui balą, šių priemonių įrengimo ypatybes, užraktų raktų apsaugos procedūras.
27. Dokumentų saugyklos (archyvai), kuriose laikomi neterminuoto ar terminuoto saugojimo dokumentai, įrengiamos vykdant Lietuvos vyriausiojo archyvaro 2011 m. gruodžio 28 d. įsakymu Nr. V-157 patvirtintas „dokumentų saugojimo taisykles“ ir šiuos reikalavimus patalpoms, langams, durims, spynoms.
28. Padidinto saugumo patalpose apsauginė 412 mkm storio plėvelė ant stiklo turi būti klijuojama langų gamybos metu ir tvirtinama prie lango rėmo juostomis.
29. Įrengiant serverinės patalpas, būtina atsižvelgti į bendruosius fizinės apsaugos reikalavimus ir šiuos kriterijus:
    - patalpa turi būti izoliuota nuo taršos šaltinių;
    - turi būti tinkamas priėjimas prie patalpos ir reikiamo pločio durys, kad į serverinę įnešti techninę įrangą;
    - pasirinkti vietą, kur yra užtikrinama pastato zonos apsauga;
    - pasirinkti vietą, kur galima ekonomiškai įrengti oro kondicionavimo sistemą;
    - pasirinkti vietą, kur mažai tikėtina, kad artimiausioje aplinkoje galimi statybos, remonto, patalpų rekonstravimo darbai;
    - pasirinkti vietą, kur būtų potenciali galimybė praplėsti serverinę, jeigu to prireiktų, nes plėtimo atveju pigiau išplėsti esančią, negu įrengti naują serverinę;
    - vengti vietų kur galimi skysčių nutekėjimai – vandentiekio ir kanalizacijos vamzdynai, kt.
    - serverinės patalpa projektuojama kaip uždara, padidinto saugumo zona, neturėtų būti langų;
    - įrangos įnešimui į serverinę numatomas durų plotis 100 cm, aukštis – 210 cm.
    - visos durys, per kurias įranga gabenama į serverinę turi turėti nemažesnius išmatavimus, o koridoriai – 150 cm pločio;
    - grindys turi būti padengtos neslidžia, atsparia padidintoms apkrovoms danga.
    - patalpos saugumo padidinimui gali būti konstruktyviai sustiprintos. Tokiu atveju sustiprinimas atliekamas taip: sienos, grindys, lubos neplonesnės, kaip 25 cm iš fero-betono, plytų ar panašios reikiamo stiprumo medžiagos;
    - jeigu tokių sienų nėra, sienos sustiprinamos geležiniais strypais (armatūra), nemažesnio diametro, kaip 12 mm, horizontaliai ir vertikaliai, sujungiant ties kiekvienu susikirtimu ir įtvirtinant grindyse, lubose, sienose nemažiau, kaip 10 cm gylyje,
    - langų dydis nemažesnis, kaip 15x15 cm, jeigu jie yra, jie turi būti sustiprinti vertikaliais ir horizontaliais geležiniais strypais (armatūra), nemažesnio diametro, kaip 12 mm, horizontaliai ir vertikaliai, sujungiant ties kiekvienu susikirtimu ir įtvirtinant grindyse, lubose, sienose;
    - langų stiklai turi būti dvigubi, langai uždengiami užuolaidomis ar žaliuzėmis, kad nepraleistų šviesos.

20. Reikalavimai įrengiant padidinto saugumo patalpų duris, spynas:
    20.1. Įrengiamos padidinto saugumo patalpų durys gali būti vienvėrės arba dvivėrės, varstymo kryptis ir būdas, vienos krypties, pasukant apie vertikaliąją staktos dalį vieną iš ašių, stacionariai fiksuojant vienoje durų staktos pusėje.
    20.2. Pastato vidinių patalpų durys gali būti priešgaisrinės, metalinės arba medienos pakaitalų kompozicinės padidinto saugumo, atitinkančios 2 saugumo klasę.
    20.3. Pagal konstrukciją durų varčiai, staktai ir jų medžiagoms keliami 2-3 saugumo klasės reikalavimai.
    20.4. Sertifikuota cilindrinė, plokštelinė spyna ir spynos plokštelė bei tam tikrais atvejais sertifikuoti durų sutvirtinimo komplektai turi atitikti 3 saugumo klasę.
    20.5. Priešgaisrinės ir evakuacinės durys turi atitikti STR 2.01.04:2002 „Gaisrinė sauga. Pagrindiniai reikalavimai“ normatyvinius reikalavimus.
    20.6. Priešgaisrinės durys turi atitikti EI-30, EI-45, EI-60 durų gaisrinės saugos klasę, turi būti įrengiamos elektromechaninės motorinės spynos, atitinkančios 3 saugumo klasę, suderintą su evakuacinių išėjimų įranga.
    20.7. Sertifikuota elektromechaninė motorinė spyna turi atitikti LST EN 12209, LST EN 1303 arba LST EN 12320 standartų 3 saugos klasės reikalavimus: sertifikuotas korpusas, šerdis ir užrakto plokštelė bei tam tikrais atvejais sertifikuota vidinė durų arba pakabinama spyna su sertifikuota furnitūra.
    20.8. Svarbių veiklai patalpų durų elektromechaninės spynos ir įeigos kontrolės sistemos komutaciniai laidai, jungiantys elektroninę ir mechaninę įrangą turi būti apsaugoti įleidžiama laido šarvo apsauga, staktos ir varčios briaunose (uždarytoje durų padėtyje, laido šarvo apsaugos vizualiai negali matytis).
    20.9. Durų uždarymo užtikrinimui turi būti naudojami pritraukėjai atitinkantys durų svorį, gabaritus, LST EN 1154 standarto reikalavimus, gamintojo pateiktas CE kokybės sertifikatas.
    20.10. Priešgaisrinėse duryse naudojamų spynų bei uždarymo įtaisų atsparumo ugniai klasė turi būti ne žemesnė, negu pačių durų atsparumo ugniai klasė.
    20.11. Evakuacinių išėjimų iš pastatų durys pagal STR 2.01.04:2002 „Gaisrinė sauga. Pagrindiniai reikalavimai“ nuostatas, privalo turėti užraktus arba uždarymo mechanizmus, atidaromus iš vidaus ir atitinkančius LST EN 1125 arba LST EN 179 standartų reikalavimus.
    20.12. Evakuacinių ir avarinių išėjimų duryse, privaloma tvarka, turi būti montuojami tik sertifikuoti įtaisai pagal standartų reikalavimus: LST EN 179, kuris reglamentuoja atsarginio išėjimo įtaisų, valdomų sverto rankena arba nuspaudžiamuoju strypu, naudojimą ir LST EN 1125, kuris reglamentuoja avarinio išėjimo įtaisų, valdomų horizontaliu strypu, naudojimą.
21. Objekto apsaugos posto patalpa, kurioje pagal sudarytą grafiką budi apsaugos darbuotojai, turi būti įrengta elektroninės saugos sistemos valdymo, kontrolės ir atvaizdavimo įranga (centralės, apsaugos valdymo įrenginiai, vaizduokliai).
    21.1. Šios valdymo įrangos sumontuotos stacionariame poste stebėjimas turi būti vykdomas visą parą, stebint su objekto elektroninėmis saugos sistemomis susijusią informaciją, kuriose suformuoti aktualių įvykių pranešimai susiję su informaciją apie jų būklę, perduodami GSM ryšiu į CSP.
    21.2. Patekimo kontrolė į apsaugos postą turi būti vykdoma įrengus elektroninę įeigos kontrolės sistemą, suteikus prieigą tik šiame poste dirbantiems apsaugos darbuotojams.

6. APSAUGOS PRIEMONIŲ SKIRTINGO APSAUGOS LYGIO OBJEKTUOSE SUVESTINĖ LENTELĖ.

Eil. Nr.	Priemonės pavadinimas	Objektų apsaugos lygiai								
		V		IV			III	II	I	Pastabos
		Padidinto saugumo objektai, valdomas turtas, kuriuose saugoma ir dirbama su įslaptinta informacija, valstybinės institucijos (ministerijos, kt.).		Valdomas turtas naudojamas pilnu intensyvumu	Valdomas turtas, kuris yra laikinai nenaudojamas pagal paskirtį, nedaro įtakos kitų turtų eksploatacijai	Valdomas turtas, kuris yra laikinai nenaudojamas pagal paskirtį, daro įtaką kitų turtų eksploatacijai	Nenaudojamas, naudojamas pagal paskirtį parduodamas turtas	Nenaudojamas, nenaudojamas pagal paskirtį, dalinės nuosavybės, bešeimininkis parduodamas turtas	Avarinės būklės požymių turintis turtas	
		Privalomos priemonės	Rekomenduojamos priemonės	Privalomos priemonės	Privalomos priemonės	Privalomos priemonės	Privalomos priemonės	Privalomos priemonės	Privalomos priemonės	
1.	**Apsauginė įsibrovimo signalizacija (vidinė)**									
	PIR judesio	+		+	+	+	+	+		
	Magnetokontaktiniai	+		+	+	+	+	+		
	Stiklo dūžio	+		+						
	PIR judesio su antimaskavimu	+								
	Užpuolimo pavojaus signalizavimo sistema (pavojaus mygtukai)	+		+						
2.	**Apsauginė įsibrovimo signalizacija (lauko)**									
	Mikrobanginiai		+							
	PIR pasyviniai, aktyviniai		+							
	Radijobanginiai		+							
3.	**Elektroninė įeigos kontrolės sistema, patekimo kontrolė**									

	EĮKS su darbinio dažnio 125 kHz bekontakčiais „smart“ technologijos skaitytuvais	+		+		+	+			Patekimas į objektą
	EĮKS „B“ patekimo klasė su darbinio dažnio 125 kHz bekontakčiais „smart“ technologijos skaitytuvais	+								Patekimas į padidinto saugumo patalpas
	EĮKS „B“ patekimo klasė su bekontakčiais darbinio dažnio 13,56 Mifare technologijos kortelių skaitytuvais, kodine spyna arba biometrine priemone.	+								Dirbama su įslaptinta informacija
	Kodinė spyna arba telefonspynė				+	+		+		
4.	**Vaizdo stebėjimo sistema**									
	VSS numatant 3-ią kokybės lygį, su judesio detekcija, jungiama į uždarą vidinį tinklą, su numerių atpažinimo sistema	+								
	VSS užtikrinanti vaizdo stebėjimą ir įrašymą realiu laiku			+						
5.	**Gaisro aptikimo ir signalizavimo sistema**									
	Įrengiama konvencinė GSS					+	+	+		
	Įrengiama adresinė	+		+	+					

	GSS									
	Gaisrinė signalizacija įrengiama su vietiniu garsiniu žmonių perspėjimu pastate							+		
6.	**Elektroninių saugos sistemų pranešimų perdavimas**									
	Vykdomas pranešimų perdavimas į vidinį apsaugos postą ir nuotolinį CSP	+								
	Vykdomas pranešimų perdavimas į nuotolinį CSP			+	+	+	+	+		
	Vykdomas vietinis garsinis žmonių perspėjimas objekte							+		
7.	**Elektroninių saugos sistemų valdymas**									
	Vidiniame apsaugos poste įrengtos valdymo centralės	+								
	Objekto viduje įrengtoje serverinėje patalpinta centralė			+						
	Objekto viduje rakinamoje ir signalizuotoje spintoje patalpinta centralė				+	+	+	+		
	Naudojamas bendras apsaugos įrenginys skirtingų elektroninių saugos sistemų valdymui		+							
8.	**Reagavimas į saugos sistemų pažeidimus, aliarminius suveikimus**									
	AT apsaugos darbuotojai ir greito reagavimo ekipažas	+								
	AT greito reagavimo ekipažas			+	+	+	+	+		
9.	**Objekto fizinė apsauga**									

	Apsaugos darbuotojas dirbantis 7/24	+								Nuomininkui reikalaujant
	Apsauginninkas, administracijos darbuotojas dirbantis darbo valandomis			+						
10.	**Periodinių stebėjimų apsilankant objektuose vykdymas**									
	Objektų periodinė vizualinė apžiūra				+	+	+	+	+	
	Objektų periodinė vizualinė apžiūra su parengtu reglamentinių darbų sąrašu	+		+						
11.	**Inžinerinės perimetrinės apsaugos priemonės (tvoros)**									
	Teritorijos perimetrinė metalinių strypų arba segmentinė tvora		+							
	Teritorijos aptvėrimui naudojami laikini tvoros segmentai 2x3 metrų.								+	
12.	**Mechaninės perimetrinės apsaugos priemonės (vartai)**									
	Mechaniniai arba automatizuoti įvažiavimo vartai		+							
	Valdomas kelio užtvaras (šlagbaumas) su EĮKS	+		+						
13.	**Pastato mechaninės apsaugos priemonės**									
	Rakinamos durys, užsandarinamos objekto varstomos dalys				+		+	+	+	
14.	**Padidinto saugumo patalpos**									

	Padidinto 3-čio saugumo klasės durys	+		+						
	Langai su užsklendimo įtaisu ir apsaugine plėvele	+		+						
	Sertifikuotos 3 saugos klasės spynos	+		+						
15.	**Vykdomų funkcijų, privalomų teisės aktais, dokumentavimas**									
	Nustatytas leidimų režimas	+		+						
	Parengti ir pildomi privalomi teisės aktais nustatyti registracijos žurnalai	+		+	+					

7. PRIVALOMOS APSAUGOS PRIEMONĖS PENKTO APSAUGOS LYGIO OBJEKTUOSE.

Užtikrinant penkto apsaugos lygio objektų apsaugą, įrengiamos įsibrovimo pavojaus signalizavimo sistemos turi sugebėti aptikti įsibrovėlį, parodyti, pro kurią perimetrinę pastato dalį ar į kurias patalpas bando patekti pažeidėjas. Šis apsaugos lygis turi užtikrinti, kad į įslaptintos informacijos saugojimo ar kitas svarbias vykdomai veiklai patalpas patektų darbuotojas, kuriam yra suteikta prieiga. Turi būti įrengtos mechaninės apsaugos priemonės, galinčios užlaikyti pažeidėją arba sustabdyti nesankcionuotą patekimą į administracinę erdvę, iki atvyks, gavę aliarminį pavojaus signalą, apsaugos poste budintys apsaugos darbuotojai ar greito reagavimo ekipažas. Šio apsaugos lygio objektuose, priklausomai nuo galimo pavojaus, rizikos vykdomai veiklai, turi būti įrengtos arba naudojamos šios apsaugos priemonės:

- Apsauginė (įsibrovimo) pavojaus signalizavimo sistema;
- Gaisro aptikimo ir signalizavimo sistema;
- Įeigos kontrolės sistema;
- Uždara vaizdo stebėjimo sistema;
- Elektroninės saugos sistemos informacinių pranešimų perdavimas.
- Mechaninės apsaugos priemonės (tvoros ir vartai, durys, langai, spynos).
- Fizinė apsauga (apsaugos darbuotojai).

7.1. Apsauginė (įsibrovimo) pavojaus signalizavimo sistema

Įvertinus objekto vietą, atvirų teritorijų ir perimetrinės dalies ilgį, prieigų prie pastato apsaugos galimybes bei saugomo pastato dydį ir veiklos jame intensyvumą, gali būti įrengiama lauko perimetrinė apsauginė signalizacija. Prieigų prie pastato ir vidinėje teritorijos dalyje esančių statinių, pastato vidinių erdvių apsaugai turi būti naudojami skirtingo veikimo principo elektroninės saugos sistemos detektoriai. Įrengiamos apsauginės signalizacijos sprendiniai turi atitikti ne žemesnį negu 3 saugumo lygmenį pagal standartą LST EN EN50131-1.

1. Įvertinus prieigų prie pastato ir vidinių teritorijų bei artimos kaimynystės saugumo pažeidžiamumų rizikas nesankcionuotai patekti į objekto teritoriją ir galimą pažeidėjo neigiamą poveikį lauke saugomai įrangai (dyzeliniai elektros generatoriai, telekomunikacijų įvadų vietos), įrengti lauko mikrobanginius, radijobanginius ar PIR pasyvinius, aktyvinius infraraudonųjų spindulių detektorius.
2. Įrengiamos pavojaus signalizavimo sistemos (standartas LST EN 50131-1) turi būti klasifikuojamos pagal: autorizavimo, prieigos lygį, veikimo būdą, signalų apdorojimo tipą, detekcijos pobūdį, pranešimų siuntimo būdą, maitinimo šaltinio tipą, lietimo (sabotažo) saugos lygį, vidinio ryšio kontrolę, įvykių įrašymo ir išsaugojimo galimybę.
3. Įrengiamas kontrolės pultas (centralė) ir kiti apsaugos sistemos įrenginiai, turi būti sertifikuoti pagal EN50131-1 GR3 (3-ią apsaugos klasę) arba jam lygiavertį, turėti padidintą apsaugą nuo įsilaužimo. Apsaugos sistemos centrale (ir jos išplėtimo modulių) komutacinės dėžutės turi būti papildomai apsaugotos antisabotažiniais davikliais.
4. Apsaugos sistemos pilnas funkcionalumas turi būti prieinamas be papildomų licencijų įsigijimo.
5. Techninė užduotis projektavimui parengiama įvertinus objekto dydį, išplanavimą, apskaičiavus kontroliuojamų įėjimų (zonų) skaičių, numatant galimo išplėtimo zonų skaičių su privalomu zonų rezervu sistemoje, įvertinti įvykių atminties skaičių.
6. Parengus objekto techninę užduotį rengiamas techninis darbo projektas, įvertinus prietaisų kiekį ir galimą grupavimą, pagal funkcinę signalizacijos naudojimo ir valdymo paskirtį, suskaičiuojamas atskirų signalinių spindulių kiekis, parenkami kontroliniai priėmimo-perdavimo prietaisai pagal zonų skaičių, sugrupavimo poreikius, išėjimo ir įėjimo signalų kiekybiniai ir kokybiniai parametrai.
7. Įrengtų elektroninių saugos sistemų kontrolei ir valdymui, pastate įrengiama vieninga apsaugos sistema. Poreikiui esant, skaidoma į atskiras, nepriklausimas sritis.
8. Apsaugos signalizacija turi turėti ne mažiau 10 nepriklausomų sričių, vienoje sistemoje.
9. Objekto apsaugos poste įrengtos elektroninės saugos sistemos valdymo programinės įrangos paketai turi būti su valdymo ir vizualizacijos funkcionalumu, skirta grafiniam sistemos būsenos atvaizdavimui su žemėlapių ir prietaisų piktogramų įkėlimu bei interaktyviu valdymu. Šios programinės įrangos licencijos bei jos atnaujinimai turi būti nemokami.
10. Pirmame aukšte apsaugos signalizacija įrengiama pilnai perimetro apsaugai. Patalpose montuojami infraraudonųjų spindulių PIR judesio davikliai, ant visų pirmo aukšto langų ir durų turi būti sumontuoti magnetiniai kontaktai, patalpoje, kur yra langas, dar papildomai įrengiamas stiklo dūžio detektorius arba kombinuotas judesio ir stiklo dūžio detektorius.

11. Kituose aukštuose judesio davikliai montuojami tik bendro naudojimo patalpose, koridoriuose (nebent yra specialus poreikis arba galima rizika dėl artimos kaimynystės atsirandanti nuo šalia esančių pastatų ar priestatų).
12. Informaciniai pranešimai iš objekte įrengtų elektroninių saugos sistemų turi būti perduoti į nutolusį centrinį stebėjimo pultą GSM ryšio pagalba. Apsaugos sistemos centralė turi sąveikauti su trečių gamintojų GSM modeliais.
13. Objektuose, parengus aiškią pavojaus mygtukų išdėstymo struktūrą ir įvertinus poreikį, įrengti bevielius (stacionarius, nešiojamus) užpuolimo pavojaus signalizavimo sistemos pavojaus mygtukus.
14. Apsaugos signalizacija turi turėti galimybę pajungti elektroninę įeigos kontrolės sistemą.
15. Patekimo į objekto perimetrinės pastato dalies varstomos dalys (durys, liukai, stoglangiai ir pan.) blokuojamos atskirais apsauginės signalizacijos spinduliais.
16. Lengvo patekimo vietos, kurias galima pasiekti užlipus ant stogo, patenkant į pastato rūsį iš gatvės pusės ir kt. iki 4 m aukštyje virš žemės paviršiaus - turi būti su įrengta signalizacija.
17. Padidinto saugumo patalpose (serverinės, ryšių patalpos, dokumentų saugojimo patalpos) įrengti dvigubo veikimo stiklo dūžio detektorius, jei yra langai – PIR pasyvinius infraraudonųjų spindulių detektorius su antimaskavimu. Šioms patalpoms apsaugoti turi būti sukurta atskira sritis apsaugos sistemoje su atskiru valdymo kodu.
18. Įslaptintos informacijos saugojimo ir darbo su įslaptinta informacija patalpose, vadovų kabinetuose įrengta apsauginė (įsibrovimo) signalizacija PIR judesio detektoriai turi turėti antimaskavimo funkciją.
19. Įrengta elektroninė saugos sistema nuo galimo išorinio poveikio turi turėti apsaugą nuo viršįtampių.
20. Turi būti parengtas ir pildomas apsauginės signalizacijos, elektroninės įeigos ir vaizdo stebėjimo sistemų techninės priežiūros, gedimų ir pažeidimų registracijos žurnalas.
21. Apsaugos signalizacijos sistema turi turėti automatinio signalizacijos pridavimo ir atjungimo funkciją pagal pasirenkamą laiko grafiką (auto-arm ir disarm).
22. Turi būti galimybė valdyti, stebėti apsaugos sistemos įvykius per mobilią aplikaciją (apps).

7.2. Gaisro aptikimo ir signalizavimo sistema.

Gaisro aptikimo ir signalizavimo sistema projektuojama taip, kad aptiktų gaisrą ankstyvojoje stadijoje ir perduotų reikiamus valdymo ir pavojaus signalus darbuotojams bei kitoms inžinerinėms sistemoms. Gaisro aptikimo sistema, detektoriams analizuojant kontroliuojamų patalpų būseną, turi sureaguoti į dūmų ir temperatūros pokyčius bei perduoti pavojaus signalą taip greitai, kad būtų užkirstas kelias gaisro židinio plitimui. Visi gaisro signalizacijos detektoriai turi būti programiškai suskirstomi į atitinkamas adresines zonas, atsižvelgiant į patalpų funkcinę paskirtį, gaisro kilimo priežastį, pastato architektūrinį paveldą bei evakuacijos kelius.

1. Gaisro aptikimo ir signalizavimo sistema įrengiama vadovaujantis galiojančiais teisės aktais, privalomais ir normatyviniais dokumentais.
2. Gaisrinė signalizacija turi būti įrengta apsaugos poste, nesujungiant jos kartu su apsaugine signalizacija ir įjungta į bendrą pastato patalpų apsaugos, stebėjimo ir valdymo sistemą.
3. Šio apsaugos lygio pastato patalpose, nustatant gaisro židinio (vietos) tikslumą, įrengti adresinę gaisrinės signalizacijos sistemą.
4. Įvertinus patalpų paskirtį, degumo klasę/medžiagas ir galimo gaisro kilimo pobūdį įrengti optinius dūminio ar temperatūrinio tipo detektorius.
5. Pastate turi būti naudojama vieninga gaisrinės signalizacijos sistema. Jei įrengtos kelios gaisrinės signalizacijos centralės, jos turi būti apjungtos, kad nustačius vienoje sistemoje gaisro aliarmą, jis būtų perduotas kitoms.
6. Turi būti numatyta galimybė gaisrinės signalizacijos sistemą valdyti per programinę įrangą su vizualizacijos funkcionalumu (grafiniam sistemos būsenos atvaizdavimui su žemėlapių ir prietaisų piktogramų įkėlimu bei interaktyviu valdymu). Šios programinės įrangos licencijos bei jos atnaujinimai turi būti nemokami.
7. Visas pastato zonas, tame tarpe pastoges, turi apimti gaisro aptikimo ir signalizavimo sistema, kuri prijungiama prie pastato apsaugos poste įrengtos centralės ir perduodama GSM belaidžio ryšio kanalu į apsaugos tarnybos CSP.
8. Pastato viduje turi būti numatytas lankytojų su negalia informavimas apie gaisrą šviesa ir garsu.
9. Gaisrinę signalizaciją turi projektuoti įmonės turinčios kvalifikacinius atestatus darbui ypatingos svarbos objektuose, Valstybinės energetikos reguliavimo tarybos išduotą kvalifikacinį atestatą elektros įrenginių iki 1000 V įrengimo darbams.

10. Turi būti parengta ir dokumentuota aiški tvarka, kaip pranešti priešgaisrinei gelbėjimo tarnybai apie gaisrą.
11. Pastato išorėje prie pagrindinių įėjimų į pastatą arba jo dalį (-is) turi būti įrengtos lauko sirenos 95 dB su blykstėmis. Sirenos turi būti matomos iš pagrindinės privažiavimo prie pastato ar jo dalies gatvės pusės.
12. Atlikus gaisro aptikimo ir signalizavimo sistemos projektavimo ir įrengimo darbus, turi būti parengta išpildomoji projektinė dokumentacija su skeletinėmis schemomis, brėžiniais, sistemos vartojo instrukcijos lietuvių kalba.
13. Techninio aptarnavimo ir priežiūros darbai turi būti vykdomi vadovaujantis sudarytu reglamentinės techninės priežiūros planu, atliktus darbus fiksuoti nustatytos formos ir turinio žurnale „Gaisrinės automatikos įrenginio techninės priežiūros ir remonto apskaitos žurnalas“, nurodant vietą, datą, laiką, atliekamų darbų aprašymą.

7.3. Įeigos kontrolės sistema.

Objekto įeigos kontrolės sistema turi užtikrinti, kad darbuotojai ir lankytojai į teritoriją, pastatą įeitų tik nustačius jų asmens tapatybę. Kiekvieno darbuotojo ir lankytojo patekimas į objektą įėjimas/išėjimas turi būti registruojamas. Patekimo kontrolė į šio fizinės apsaugos lygio objektus turi būti vykdoma įrengta elektronine įeigos kontrolės sistema, valdoma nuotolinėmis kortelėmis (identifikatoriais) ir skaitytuvais, įrengtais prie įėjimo į pastatus durų ir šalia vartų įrengtų vartelių, jei patekimas į teritoriją kontroliuojamas automatizuotais vartais. Lankytojų patekimo kontrolei vykdyti gali būti naudojamos ne tik elektroninės apsaugos priemonės, bet ir leidimų išdavimas, užtikrinant registravimą skaitmeninėse ir nustatytos formos leidimų išdavimą.

1. Projektuojant ir įrengiant elektroninę įeigos kontrolės sistemą numatyti jų pajungimą į atskirą kompiuterinį tinklą.
2. Objektuose įrengiama EĮKS su bekontakčiais „smart“ technologijos skaitytuvais, kurių darbinis dažnis 125 kHz ir jie palaiko standartų ISO/IEC 14443 ir ISO/IEC 15693 reikalavimus atitinkančias korteles.
3. Padidinto saugumo patalpose įrengiama EĮKS turi turėti (B) patekimo klasę, pagal standarto LST EN EN50131 reikalavimus, kurioje nustatytas laiko grafikas ir registracijos funkcija bei atliekama apsauginė funkcija, aptinkant ir nutraukiant nesankcionuotą patekimą.
4. Patekimo kontrolei užtikrinti įslaptintos informacijos saugojimo ar darbo su įslaptinta informacija patalpose įrengta EĮKS turi, užtikrinant (B) patekimo klasę pagal standarto LST EN EN50131 reikalavimus, papildomai prie durų įrengti kodinę spyną su 4-6 kodų ar didesniu skaičių deriniu arba biometrinę sistemą.
5. Įslaptintos informacijos saugojimo ar darbo su įslaptinta informacija patalpose įrengiama EĮKS su bekontakčiu 13,56 Mifare technologijos kortelių skaitytuvu, nuskaitančiu Mifare DESFire EV1/EV2 kortelių vidinių sektorių informaciją (saugus režimas).
6. Pasirenkant EĮKS jos naudojama programinė įranga būsenos grafiniam atvaizdavimui ir interaktyviam valdymui turi turėti nemokamą programinį aprūpinimą ją naudojant ar atnaujinant.
7. EĮKS naudojama bekontaktė „smart“ tipo atstūminė kortelė (identifikatorius) turi būti tinkama termospaudai.
8. Patekimo į pastatą fizinei kontrolei svarbi apsauginio užtvaro (vartelių) konstrukcija, turi užtikrinti patekimą tik galiojančio leidimo savininkui, neleidžiant kartu patekti antram asmeniui.
9. Vykdant patekimo į objektą darbuotojų kontrolę ir užlaikant galimą pažeidėją, bandant nesankcionuotai patekti į objektą, įrengti EĮKS mechaninį užtvarą 0,9 iki 1 metro aukščio sukamuosius vartelius su šoninėmis svirtimis ir sparnais, apsunkinant galimybę juos įveikti perlipant ar pralendant.
10. Patekimo kontrolės registracijos įrašai su asmens duomenimis skaitmeninėje ar popierinėje laikmenose turi būti saugomi ne trumpiau kaip 6 mėnesius ir ne daugiau kaip 1 metus.
11. Vykdant atvykusių lankytojų registraciją, įrašyti atvykusių vardą, pavardę, atvykimo ir išvykimo laiką ir priimančio asmens vardą, pavardę. Lankytojams negalima suteikti prieigos prie lankytojų registracijos įrašų, t.y. lankytojai negali peržiūrėti ankstesnių lankytojų įrašų.
12. Prie įėjimo į objektą durų įrengti pasikalbėjimo įrenginį vaizdo telefonspynę, svarbią kontroliuojant interesantų patekimą po darbo valandų arba prieš darbo pradžią.
13. Turi būti numatyta galimybė įeigos kontrolės sistemą valdyti per programinę įrangą su vizualizacijos funkcionalumu (grafiniam sistemos būsenos atvaizdavimui su žemėlapių ir prietaisų piktogramų įkėlimu bei interaktyviu valdymu). Sistema turi palaikyti konfigūruojamą darbo režimą pagal laiko

grafiką (durų atblokavimas/užblokavimas nustatytomis valandomis). Šios programinės įrangos licencijos bei jos atnaujinimai turi būti nemokami.

14. Gaisro aliarmo atveju, evakuacinės durys su įrengta praėjimo kontrolės sistema turi atsiblokuoti ir leisti netrukdomai evakuotis be kortelės/pažymėjimo panaudojimo. Išėjimas iš padidinto saugumo patalpų (serverinės, ryšių patalpos, archyvai) vykdomas vidiniu durų atidarymo mygtuko paspaudimu.
15. Praėjimo kontrolės sistemos išplėtimo (tarpiniai) kontroleriai montuojami virš pakabinamų lubų arba kitose lengvai nepasiekiamose vietose, tačiau turi būti užtikrinamas priėjimas 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.
16. Praėjimo kontrolės sistema turi būti jungiama Į "TB tinklą" įrengiant reikiamus ryšio perdavimo sprendimus ir turėti galimybę įrengtais ryšiais perduoti informacija apie įrangos veikimo statusą (gedimus, prisijungimus ir t.t), suteikti prieigą prie duomenų bazės ir ją koreguoti (įvesti vartotojus, korteles ir t.t.).

7.4. Uždara vaizdo stebėjimo sistema.

Vaizdo stebėjimo sistema yra viena iš apsaugos sistemų dalių, skirta objekto vidinės ir išorinės dalies, svarbių patalpų bei prieigų prie jų vizualiam stebėjimui ir apsaugai, jei vaizdo kamerose suprogramuota judesio detekcija. Objektuose įrengiamos valdomos vidinės ir išorinės vaizdo kameros bus efektyvios ir veiksmingos, jei reaguos į elektroninių sistemų pažeidimų vietas, įsijungs garsiniai ar šviesiniai indikatoriai. Uždaros vaizdo stebėjimo sistemos pagrindinis tikslas, gavus informacinį pranešimą apie pažeidimą ar nesankcionuotą patekimą, judėjimą teritorijoje ar pastatuose, persijungti į pažeidimo vietą įvertinant pažeidimo pobūdį arba stebėti situaciją pasirinktoje vietoje realiu laiku. Vaizdo kamerų vaizdai stebimose zonose turi užtikrinti tokią kokybę, kuri suteiktų aiškų veiksmų atpažinimą. Įslaptintų dokumentų saugojimo ir darbo su įslaptinta informacija patalpose turi būti pakankama vaizdo kokybė, identifikuojant darbuotojus ir jų judėjimą, nustatant jų asmens tapatybę.

Vaizdo stebėjimo sistema projektuojama ir įrengiama pastato perimetrui 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 lenteles 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.

1. Projektuojant ir įrengiant uždarą vaizdo stebėjimo sistemą, naudoti valdomas ir stacionarias skaitmenines spalvotas vaizdo kameras, VSS pajungti į atskirą kompiuterinį tinklą.

2. Projektuojant VSS ir pasirenkant sistemos gamintoją patikrinti, ar jis yra išleidęs sistemos programinės įrangos atnaujinimus, įvertinimą, kokią naudą ir/ar žalą sistemos naujinių įdiegimas turėtų įtakos sistemai.
3. Pastato, vidinių patalpų apžvalgai montuojamų vaizdo stebėjimo kamerų vieta ir aukštis parenkamas toks, kad registruoti visus įeinančius į pastatą ir praeinančius per kontroliuojamas duris, artėjančius prie svarbių patalpų durų (LST EN 50132-7 - objekto klasifikavimas ir/arba objekto identifikacija), matyti svarbių patalpų prieigas iš išorės (LST EN50132-7 - įsibrovėlio detekcija ir/arba objekto klasifikavimas).
4. Projektuojant ir įrengiant VSS pirmiausia būtina parengti techninę užduotį, kurioje turi būti numatytos ir vizualizuotos teritorijos plane stebėjimo zonos, vaizdo kamerų įrengimo vietos, nubrėžtos stebėjimo zonos, nurodyti kameros tikslai (ką ji turi stebėti, ar identifikuoti darbuotojus, aptikti judantį objektą, kt.).
5. Vaizdo stebėjimo sistemai suprogramavus judesio detekciją, ji turi veikti 24/7 režimu pagal judesio fiksavimą ir vykdyti objekto apsaugos funkcijas, integruojant ją kartu su apsauginės signalizacijos ir įeigos kontrolės sistemomis, užtikrinti pakankamą kadrų per sekundę įrašo spartą.
6. Suprojektavus VSS nustatyti vaizdo kamerų zonose jautrumą, parinkti kintamo židinio nuotolio objektyvus su automatiniu diafragmos nustatymu.
7. Įrengiant vaizdo kameras įslaptintos informacijos saugojimo ar darbo su įslaptinta informacija patalpose arba jų prieigose, užfiksuotam vaizdui numatyti 3-ią kokybės lygį ir vaizdo zonos tipą pagal galiojantį standartą LST EN 62676 – patenkantis asmuo atpažįstamas ir identifikuojamas.
8. Vaizdo kamerų įrašai turi būti saugomi 14 parų ir prireikus peržiūrimi, vėliau ištrinant jį iš kietojo disko ir užrašant iš naujo.
9. Įrengus vaizdo stebėjimo kameras privalomas jų patikrinimas dienos ir nakties metu, įvertinus objekte įrengtą bendrą ir apsauginį apšvietimą.
10. Esant nepakankamam teritorijos apšvietimui, pagrindinį apšvietimą papildyti apsauginiu apšvietimu, naudojant atrankinį apšvietimą su judesio detektoriais integruojant apšvietimo prietaisus.
11. Uždaros vaizdo stebėjimo sistemos skaitmeninio įrašymo sistema turi turėti kontrolės funkciją, kuri atpažintų ar skaitmeniniame vaizdo įraše buvo daromi pakeitimai, pagal galiojantį standartą LST EN 62676, turi būti sudaryta galimybė apsaugos poste atlikti realaus vaizdo peržiūrą.
12. Vykdant vaizdo stebėjimą objekte vadovautis Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo ir Europos Sąjungos Bendrojo duomenų apsaugos reglamento (ES) 2016/679 reikalavimais.
13. Jei už duomenų tvarkymą yra atsakingas Turto bankas – prie įėjimų į vaizdo stebėjimo sistemos fiksuojamą teritoriją, pastatą turi būti informacinės lenteles ar lipdukai: „Asmenų ir turto apsaugos tikslu vykdomas vaizdo stebėjimas. Teritorija ir patalpos stebimos vaizdo kameromis“. Valstybinė įmonė Turto bankas, įm. kodas 112021042, Kęstučio g. 45 , 08124 Vilnius, tel. +3705 2780900. Išsamesnė informacija el.paštu: info@turtas.lt

7.5. Elektroninės saugos sistemos informacinių pranešimų perdavimas.

Apsaugos tarnybos stebėjimo poste įrengta centralė ir nuotolinis CSP turi priimti trijų tipų siunčiamus signalus:

1. Kontrolės, t.y. ryšio ir sistemos būklės planinė patikra (test), patikrinant kaip veikia ryšio linija tarp objekto saugos sistemos ir CSP, informuojant apie objekto įjungimą/išjungimą, apie sabotažinio (liesties) kontakto suveikimą.
2. Pavojaus, kai pavojaus signalais informuojama apie įsilaužimą, užpuolimą, priverstinį signalizacijos atjungimą ir gaisro pavojų, suveikus detektoriui, pažeidus detektorių, nuspaudus užpuolimo (pavojaus) mygtuką.
3. Sistemos darbingumo (būsena ir technologijos), perduoda-priima į/iš stebėjimo CSP signalus apie sistemos periodinių testų rezultatus, gedimus sistemoje, zonų, daviklių, išplėtimo modulių poveikį, akumuliatoriaus išsikrovimą, elektros tinklo įtampos dingimą.
4. Elektroninės saugos sistemos, apsauginė signalizacija, gaisrinė signalizacija turi atitikti valdymo ir rodymo įrangai keliamus reikalavimus.
5. Elektroninės saugos, gaisro aptikimo ir signalizavimo sistemos pranešimai turi būti perduoti GSM ryšiu ir internetu į KM-1 kategorijos CSP įrengtus apsaugos tarnybų apsaugos ir stebėjimo postus.
6. Įrengus komunikatorių apsaugos valdymo centralė turi turėti galimybę perduoti elektroninės saugos, gaisro aptikimo ir signalizavimo sistemos pranešimus į du pultus, tame tarpe ir mobiliąją aplikaciją, debesis.

7.6. Mechaninės apsaugos priemonės, perimetrinės inžinerinės kliūtys

Perimetrinei tvorai ir vartams, kurie pažymi visą objekto išorinę teritorijos dalį, įveikti būtinos minimalios pastangos. Priklausomai nuo objekto vietos, tvoros ir vartų vertikaliosios dalies aukštis, medžiagos parenkamas pagal perimetrinei tvorai keliamus uždavinius. Objektuose įrengtos išorinės tvoros pagal konstrukciją, aukštį 1,5 m - 1,8 m priskiriamos teritoriją ribojančioms tvoroms. Su minimaliu pasiruošimu ir turint rankinius instrumentus, perimetrinę tvorą iš skirtingų medžiagų galima perpjauti/perkirpti, perlipti per 10-15 sekundžių, ją galima pralaužti transporto priemone, todėl, įrengiant tvorą ir įvažiavimo vartus, būtina apsvarstyti visus privalumus ir trūkumus, galimas išlaidas, jų eksploatavimą ir priežiūrą žiemos ar kitu metų laiku.

1. Priėmus sprendimą įrengti perimetrinės ribos inžinerinį užtvarą (tvorą) su įvažiavimo vartais, jų tinkamumą įvertinti pagal sudarytą vertinimo rangų lentelę, pasirenkant vieną iš medžiagų tvorai (metalinio tinklo cinkuota, segmentinė virinta panelinė, plieninių virbų, metalinė juostinė) ir vartų skydui:
   - atsparumas ir laiko trukmė perpjovimui;
   - vartai įvažiavimo vietose ir jų konstrukcija, valdymas ir priežiūra;
   - galimybė perlipti arba pralįsti nepastebėtam;
   - pralaužimas automobiliu;
   - atsparumas korozijai;
   - vidutinė tarnavimo trukmė ir eksploatavimo, priežiūros kaina;
   - estetinė išvaizda;
   - įrengimo kaina 100 m arba 1 m2 ir jo trukmė.
2. Objektuose įrengiama perimetrinė tvora pagal jos aukštį (1,5 m-1,8 m), konstrukciją turi atitikti teritoriją ribojančios tvoros apibūdinimą.
3. Tvora turi turėti viršutinės dalies apsaugą iš spygliuotos arba pjaunančios vielos, užaštrintais metaliniais strypais, priklausomai nuo tvoros konstrukcijos ir objekto vietos (miesto centras, rajonas).
4. Tvoros apsaugos lygį turi užtikrinti įrengti vartai, viršutinėje dalyje pritvirtinti užaštrinti metaliniai strypai ar kitos apsaugos priemonėmis nuo perlipimo, vartų aukštis su turi būti vienodas su tvoros aukščiu.
5. Pasirenkant vartų tipą, stumdomi vartai, slankiojantys slankiojamuoju bėgiu, atidaromi mechaniniai vartai, automatizuoti vartai, pagaminti iš skirtingų medžiagų skydų, būtina įvertinti įrengimo galimybes, transporto priemonių skaičių ir judėjimo intensyvumą, valdymo būdą (nuotolinis, identifikavimo kortele, kodas).
6. Įvertinus įvažiuojančių į teritoriją transporto priemonių skaičių, riziką nesankcionuotai patekti į vidinę teritoriją ir galimą poveikį, pasirenkamas transporto priemonių įvažiavimo į objektą ir judėjimo jame kontrolės būdas.
7. Įrengiama įvažiavimo kontrolės priemonė mechaniniai arba automatizuoti vartai:
   7.1. Įrengiant mechaninius vartus užrakinimui tinka spynos su kablio formos skląsčiu. Jei vartai neturi būti uždaromi iš išorės, siūloma naudoti pakabinamas spynas arba slankiojantį skląstį iš vidaus. Vartus rakinantis užraktas gali būti seifinis/plokštelinis arba cilindrinės šerdies ir sertifikuota spyna turi atitikti ES LST 12209 ir EN LST 1303 standartų antros ar trečios saugumo klasės reikalavimus.
   7.2. Vartų rakinimui naudojant pakabinamas spynas, jos turi atitikti 2-3 saugumo klases, rakinant iš vidinės pusės. Sertifikuota kabinamų spynų furnitūra turi atitikti saugumo reikalavimus pakabinamų spynų aktualiai klasei ir turi būti pritvirtinta prie vartų konstrukcijos taip, kad jos negalima būtų nusukti iš išorės.
   7.3. Įrengiant automatizuotus vartus, numatyti jų nuotolinį valdymą, blokavimą/ atblokavimą iš vidaus ekstremaliųjų situacijų atvejais.
8. Įvertinus objekto teritorijos užstatymą, pastato vidiniame kieme įrengtų transporto priemonių parkavimosi vietų skaičių, apsvarstyti būtinumą įdiegti transporto priemonių valstybinių numerių atpažinimo ir programinę įrašymo įrangą.
9. Objektų vidinių nedidelių parkavimo vietų įvažiavimo kontrolei vykdyti įrengti kelio užtvarus (šlagbaumus) su įrengtais EIKS identifikatoriais arba įvažiavimo kodais.

7.7. Padidinto saugumo patalpų mechaninės apsaugos priemonės.

1. Įrengiant serverines, kitas padidinto saugumo, įslaptintos informacijos saugojimo ar darbo su įslaptinta informacija patalpas, vadovautis bendraisiais reikalavimais apsaugos priemonių projektavimui ir įrengimui pateiktais šiame standarte.
2. Durys iš plastiko ar kitų medžiagų su durų skydu iš stiklo nepriskiriamos jokioms apsaugos klasėms, todėl įrengtos svarbiose patalpose (serverinėse, dokumentų saugyklose, techninėse patalpose) turi būti pakeistos naujomis, sumažinant galimus saugumo pažeidžiamumus.
3. Įslaptintos informacijos saugojimo ir darbo su įslaptinta informacija patalpos, kurios yra žemesniame negu 4 m aukštyje nuo žemės paviršiaus turi būti apsaugotas langais su rėmais, pagamintais iš tvirtos medžiagos, stiklas padengtas 400 mkm apsaugine plėvele įtvirtinta rėme, lango stakta turi būti sutvirtinama dviem mūrvinėmis į mūro sieną iš šono, varstomoji lango dalis fiksuojama užsklendimo mechaniniu įtaisu neleidžiant langui atsidaryti.
4. Įrengiant padidinto saugumo patalpų duris būtina pateikti UAB Statybos produkcijos sertifikavimo centro (SPSC) išduotus durų atitikties pažymėjimus ar kitų šalių notifikuotų laboratorijų ir jas kontroliuojančių institucijų pateiktus atitikties sertifikatus.

7.8. Fizinė apsauga (apsaugos darbuotojai).

LR asmens ir turto apsaugos įstatyme suteikta teisė vykdyti apsaugos funkcijas tik apsaugos darbuotojams, kurie yra baigę apsaugos darbuotojų mokymo programą (kodas 260086116), išlaikę egzaminus ir nustatyta tvarka gavus teisę dirbti apsaugos darbuotoju, apsaugininku. Apsaugos darbuotojų, dirbančių objekte, skaičius nustatomas, aprašant jų vykdomas funkcijas, įvertinant objekto sudėtingumą, žmonių ir transporto priemonių srautus, esamų įrengtų elektroninių saugos sistemų apimtį ir keliamas užduotis (vaizdo kamerų stebėjimas, patekimo kontrolės vykdymas, reagavimas į pažeidimo vietas, numatyti padidintos rizikos vietų apėjimai, kt.). Nustatant apsaugos tarnybos greito reagavimo ekipažo į pažeidimus reagavimo trukmę, turi būti įvertinta, ar apsaugos tarnyba turi reagavimo ekipažus ir turi galimybę reaguoti į pažeidimus. Pagal turimą greito reagavimo ekipažų ir saugomų objektų skaičių, numatyti reagavimo laiką dienos metu, nakties, didžiausių transporto srautų valandomis, mieste ar kaimiškoje vietovėje. Maksimalus reagavimo laikas į įvykio vietą, nustatytas pasaulyje - yra apie 15 minučių. Apsaugos tarnybai, vykdančiai objektų apsaugą, keliami šie reikalavimai.

1. Objektus turi saugoti apsaugos darbuotojai, baigę apsaugos darbuotojo mokymo programą (kodas 260086116), išlaikę egzaminus ir nustatyta tvarka įgavę teisę dirbti apsaugos darbuotoju.
2. Privaloma parengti vidaus tvarkomąjį dokumentą „objekto apsaugos instrukcija“ ar „įėjimo į administracinį pastatą, įslaptintos informacijos saugojimo patalpas, buvimo jose ir išėjimo taisykles“ su privalomu skirsniu „leidimų režimas“, kuris LR asmens ir turto apsaugos įstatyme nustatyta tvarka suteikia teisę atlikti asmens ar transporto priemonių patikrinimus, apžiūras, suteikia kitas įstatyme apsaugos darbuotojams nustatytas teises ir pareigas.
3. Įrengus elektronines saugos sistemas būtina apmokyti apsaugos darbuotojus naudotis šiomis sistemomis, parengti šių sistemų naudojimo instrukcijas.
4. Numatyti galimybę budintiems apsaugos darbuotojams (moterims ar vyrams) vykdyti asmens apžiūras ir patikrinimus, tik tos pačios lyties asmenims, sudarant jų budėjimo grafikus arba numatant apsaugos darbuotojų pakeitimus iškilus būtinybei atlikti asmens apžiūras.
5. Vaizdo kameros ir jų priklausiniai gali būti įrengiami tik turto nuomininkui reikalaujant ir pagrindžiant būtinumą dėl jų naudojimo bei pateikus techninę užduotį įrengimui.
6. Apsaugos darbuotojams, vykdant 24/7 valandų trukmės budėjimus objekte, sudarant budėjimo grafikus, suteikti jiems teisę į nustatytos trukmės poilsio pertraukėles, numatytas LR SM 2004 m. vasario 12 d. įsakymu Nr. V-65 patvirtintose Lietuvos higienos normose HN 32:2004 „darbas su videoterminalais, saugos ir sveikatos reikalavimai“. Suvestinė redakcija 2011-03-30.
7. Vertinant apsaugos tarnybų greito reagavimo ekipažo galimybę per numatytą laiką atvykti į saugomą objektą, privalome žinoti jų dislokacijos vietas ir reagavimo ekipažų skaičių miestuose ir rajonuose.
8. Nustatant maksimalų reagavimo į įvykio vietą laiką ir reaguojant daugiau kaip 15 minučių, numatyti kitas pažeidėjų užlaikymo ir sulaikymo priemones.

8. PRIVALOMOS APSAUGOS PRIEMONĖS KETVIRTO APSAUGOS LYGIO OBJEKTUOSE.

Ketvirto apsaugos lygio objektams priskiriami pastatai, statiniai, patalpos su skirtinga paskirtimi, vykdomos veiklos intensyvumu ar nenaudojami pagal paskirtį. Įrengiamų elektroninių saugos sistemų ir naudojamų mechaninių apsaugos priemonių tikslas, sugebėti aptikti įsibrovėlį, užlaikyti jį iki atvyks apsaugos tarnybos greito reagavimo ekipažas. Šiuose pastatuose esančios padidinto saugumo patalpos, serverinės, komutacinės patalpos, dokumentų saugyklos (archyvai), kt. įvertinus jų svarbą, galimas rizikas turi būti įvardintos. Įvertinus naudojamų apsaugos priemonių veiksmingumą, efektyvumą ir šiame standarte numatytus bendruosius reikalavimus projektavimui ir įrengimui įrengti papildomas apsaugos priemones. Priklausomai nuo galimų saugumo pažeidžiamumų, rizikų vykdomai veiklai ar išvengiant valdomo turto sunaikinimo, šio apsaugos lygio objektuose turi būti įrengiamos arba naudojamos šios apsaugos priemonės:

- Apsauginė (įsibrovimo) pavojaus signalizavimo sistema;
- Gaisro aptikimo ir signalizavimo sistema;
- Įeigos kontrolės sistema;
- Uždara vaizdo stebėjimo sistema;
- Elektroninės saugos sistemos informacinių pranešimų perdavimas.
- Padidinto saugumo patalpų mechaninės apsaugos priemonės.

Ketvirtam apsaugos lygiui priskiriamas:

- valdomas turtas, kuris yra apskričių centrų miestų teritorijose ir naudojamas pilnu intensyvumu. Kuriame nuolatos būna naudotojai/lankytojai (jei objekte yra keli nuomininkai ar klientų aptarnavimo skyriai, padidinto saugumo patalpos (serverinės, archyvai, kt.), turi būti numatytos papildomos apsaugos priemonės;
- valdomas turtas, kuris yra laikinai nenaudojamas pagal paskirtį, nedaro įtakos kitų turtų eksploatacijai;
- valdomas turtas, kuris yra laikinai nenaudojamas pagal paskirtį, daro įtaką kitų turtų eksploatacijai, numatomos papildomos apsaugos priemonės patekimo apribojimui.

8.1. Valdomas turtas, kuris yra apskričių centrų miestų teritorijose ir naudojamas pilnu intensyvumu.

Tai pilnu intensyvumu naudojami objektai, kuriuose nuolatos būna darbuotojai, vykdomas pilnas veiklos funkcionavimo užtikrinimas su apsilankančiais interesantais/lankytojais. Administraciniame pastate turi būti nustatyti ir įvertinti svarbiausi funkciniai vienetai, padidinto saugumo patalpos, pasitarimų kambariai ir vadovų kabinetai, dokumentų saugyklos (archyvai), techninės patalpos. Įrengiamos arba naudojamos apsaugos priemonėmis turi aptikti, įvertinti, prilaikyti pašalinius, trečiuosius asmenis, iki atvyks atsakomosios pajėgos, apsaugos tarnybos greito reagavimo ekipažas.

8.1.1. Apsauginė (įsibrovimo) pavojaus signalizavimo sistema.

1. Techninė užduotis projektavimui parengiama įvertinus objekto dydį, išplanavimą, apskaičiavus kontroliuojamų įėjimų (zonų) skaičių, numatant galimo išplėtimo zonų skaičių su privalomu zonų rezervu sistemoje, įvertinti įvykių atminties skaičių.
2. Įėjimo į pastatą duryse, pirmo aukšto languose įrengti magnetokontaktinius, stiklo dūžio detektorius, pastato viduje, koridoriuose ir bendro naudojimo patalpose įrengti pasyvinius infraraudonųjų spindulių PIR detektorius.
3. Įrengtų elektroninių saugos sistemų kontrolei ir valdymui, pastate įrengiama vieninga apsaugos sistema. Poreikiui esant, skaidoma į atskiras, nepriklausomas sritis.
4. Apsaugos signalizacija turi turėtu ne mažiau 10 nepriklausomų sričių, vienoje sistemoje.
5. Įsibrovimo pavojaus signalizavimo pultas (centralė) turi būti įrengtas objekto apsaugos poste arba serverinėje, ryšių patalpoje ar rakinamoje spintoje šalia visą dieną dirbančio darbuotojo darbo vietos, priskirto atsakingu už šio objekto apsaugą ir kontrolę.
6. Padidinto saugumo patalpose, išskirtose kaip svarbiausi funkciniai vienetai, atskira apsaugos sritimi ir valdymo kodu, įrengti infraraudonųjų spindulių judesio PIR, durų magnetokontaktinius ir stiklo dūžio detektorius.
7. Nesankcionuotas patekimas į šias patalpas centralėje turi būti atvaizduojamas garsiniais ir šviesiniais indikatoriais, veikiančiais bandant nesankcionuotai patekti į šias patalpas arba neįjungus centralės valdymo kodo.

8. Apsauginės signalizacijos valdymui naudojamas liečiamu ekranu valdymo pultelis turi būti įrengtas prie įėjimo į pastatą durų.
9. Apsaugos sistemos centralės ir jos išplėtimo modulių komutacinės dėžutės turi būti papildomai apsaugotos antisabotažiniais davikliais.
10. Apsaugos sistemos pilnas funkcionalumas turi būti prieinamas be papildomų licencijų įsigijimo.
11. Įvertinus poreikį, įrengti bevielius (stacionarius, nešiojamus) užpuolimo pavojaus signalizavimo sistemos (pavojaus mygtukus).
12. Prie įsibrovimo pavojaus signalizavimo pulto (centralė) su integruotu įeigos kontrolės sistemų valdikliu, prijungti GSM komunikatorių, skirtą pranešimų perdavimui GSM tinklais. Apsaugos sistemos centralė turi sąveikauti su trečių gamintojų GSM modeliais.
13. Apsaugos signalizacijos sistema turi turėti automatinio signalizacijos pridavimo ir atjungimo funkciją pagal pasirenkamą laiko grafiką (auto-arm ir disarm).
14. Apsaugos signalizacija turi turėti galimybę pajungti įeigos/praėjimo kontrolės sistemą.
15. Turi būti galimybė valdyti, stebėti apsaugos sistemos įvykius per mobilią aplikaciją (apps).

8.1.2. Gaisro aptikimo ir signalizavimo sistema.

1. Gaisrinė signalizacija įrengiama vadovaujantis galiojančiais teisės aktais ir privalomais normatyviniais reikalavimais.
2. Gaisrinės signalizacijos centralę projektuoti ir įrengti objekto apsaugos poste arba bendrosiose patalpose, koridoriuose, šalia visą dieną dirbančio darbuotojo darbo vietos, priskirto atsakingu už šio objekto apsaugą ir kontrolę.
3. Gaisro aptikimo ir signalizavimo sistemos gaisro ir gedimo signalai, aliarmo signalai iš patalpų perduodami į vidaus ir lauko 95 dB galingumo sirenas, dubliuojami į apsaugos tarnybos CSP.
4. Jei pastate daugiau nei vienas nuomininkas – įrengiama gaisrinės signalizacijos centralė su kartotuvu.
5. Pastate turi būti vieninga priešgaisrinė sistema. Jei įrengtos kelios priešgaisrinės signalizacijos centralės, jos turi būti apjungtos, kad, nustačius vienoje sistemoje gaisro aliarmą, jis būtu perduotas kitoms.
6. Rankinius gaisro signalizatorius įrengti laiptinėse, prie išėjimų, evakuacijos keliuose, koridoriuose, normatyviniuose dokumentuose nustatyta tvarka.
7. Objekte įrengtų dokumentų saugyklų (archyvai), bibliotekos, kabinetai apsaugai nuo gaisro, projektuoti ir įrengti optinius dūmų, garažų, dirbtuvių, virtuvės patalpose temperatūrinius detektorius.
8. Įvertinus turimų gaisrinės signalizacijos kabelių išdėstymą, įrengti adresinę gaisro židinio (vietos) nustatymo sistemą.

8.1.3. Įeigos kontrolės sistema.

1. Vykdant lankytojų patekimo kontrolę, pagal išankstinę registraciją, prie įėjimo į objektą durų arba viešoje zonoje, įrengtoje pastate, įrengiamas pasikalbėjimo įrenginys su vaizdo kamera atvykusiems lankytojams (telefonspynė).
2. Patekimo kontrolė gali būti vykdoma įrengta elektronine įeigos kontrolės sistema pastate valdoma nuotolinėmis kortelėmis (identifikatoriais) ir skaitytuvais, esančiais šalia įėjimo durų arba registruojant nustatyto pavyzdžio popierinėse laikmenose ir dokumentų valdymo sistemoje.
3. Objektuose įrengti EĮKS su bekontakčiais „smart“ technologijos skaitytuvais, kurių darbinis dažnis 125 kHz ir jie palaiko standartų ISO/IEC 14443 ir ISO/IEC 15693 reikalavimus atitinkančias korteles.
4. Įvertinus interesantų, apsilankančių objekte, skaičių ir naudojamą fizinę apsaugą (apsaugos ar administracijos darbuotojai), asmenų nesankcionuoto patekimo užlaikymui, įrengti EĮKS mechaninius barjerus sukamuosius vartelius, kurių aukštis nuo 0,9 iki 1 metro, taip apsunkinant galimybę praļįsti pro užtvarą arba jį perlipti ir patekti į pastatą.
5. Padidinto saugumo patalpose įrengta EĮKS turi užtikrinti (B) patekimo klasę pagal standarto LST EN EN50131 reikalavimus, papildomai prie durų įrengti kodinę spyną su 4-6 kodų ar didesniu skaičių deriniu arba biometrinę piršto atspaudo sistemą.
6. Vykdant atvykusių lankytojų registraciją, įrašyti atvykusių vardą, pavardę, atvykimo ir išvykimo laiką ir priimančio asmens vardą, pavardę. Lankytojams negalima suteikti prieigos prie lankytojų registracijos įrašų, t.y. lankytojai negali peržiūrėti ankstesnių lankytojų įrašų.

7. Turi būti galimybė įeigos kontrolės sistemą valdyti per programinę įrangą su vizualizacijos funkcionalumu (grafiniam sistemos būsenos atvaizdavimui su žemėlapių ir prietaisų piktogramų įkėlimu bei interaktyviu valdymu). Sistema turi palaikyti konfigūruojamą darbo režimą pagal laiko grafiką (durų atblokavimas/užblokavimas nustatytomis valandomis). Šios programinės įrangos licencijos bei jos atnaujinimai turi būti nemokami.
8. Gaisro aliarmo atveju, evakuacinės durys su įrengta praėjimo kontrolės sistema turi atsiblokuoti ir leisti netrukdomai evakuotis be kortelės/pažymėjimo panaudojimo. Išėjimas iš padidinto saugumo patalpų (serverinės, ryšių patalpos, archyvai) vykdomas vidinio durų atidarymo mygtuko paspaudimu.
9. Praėjimo kontrolės sistemos išplėtimo (tarpiniai) kontroleriai montuojami virš pakabinamų lubų arba kitose lengvai nepasiekiamose vietose, tačiau turi būti užtikrinamas priėjimas 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.
10. Praėjimo kontrolės sistema turi būti jungiama Į "TB tinklą" įrengiant reikiamus ryšio perdavimo sprendimus ir turėti galimybę įrengtais ryšiais perduoti informacija apie įrangos veikimo statusą (gedimus, prisijungimus ir t.t), suteikti prieigą prie duomenų bazės ir ją koreguoti (įvesti vartotojus, korteles ir t.t.).

8.1.4. Uždara vaizdo stebėjimo sistema.

1. Uždara vaizdo stebėjimo sistema objekte įrengiama dėl asmenų ir turto saugumo nuomininkui pageidaujant, į tinklą nejungiama, atliekamas tik vaizdo įrašymas į įrašymo įrenginį.
2. Įrengti spalvotas skaitmenines vaizdo stebėjimo kameras, įrašus kaupti serveryje arba skaitmeniniame vaizdo įrašymo įrenginyje.
3. Ant objekto sienos, kuriame vykdomas vaizdo stebėjimas, pakabinti lenteles su užrašu „Asmenų ir turto apsaugos tikslu patalpose vykdomas vaizdo stebėjimas“, nurodant įmonę, įmonės kodą, telefoną, vaizdo įrašų saugojimo trukmę atsakingo už asmens duomenų apsaugą elektroninį paštą, kuriuo galima kreiptis norint gauti informacijos ir sužinoti savo teises šiais klausimais.

8.1.5. Elektroninės saugos sistemos informacinių pranešimų perdavimas.

1. Įsibrovimo pavojaus signalizavimo ir gaisrinės signalizacijos valdymo pultas (centralė), įrengus komunikatorių, turi perduoti aliarminį signalą GSM ryšiu į apsaugos tarnybos centralizuotą stebėjimo pultą (CSP).

8.1.6. Mechaninės apsaugos priemonės (tvoros ir vartai).

1. Objekte mechaninės apsaugos priemonės, tvoros, vartai įrengiami tik nuomininkui pageidaujant.
2. Objekte atliekamas tik susidėvėjusių tvorų, vartų remonto, rekonstrukcijos ar atnaujinimo darbai arba planinis jų valdymo mechanizmų pakeitimas.
3. Objektų vidinių nedidelių parkavimo vietų įvažiavimo kontrolei vykdyti įrengti kelio užtvarus (šlagbaumus) su įrengtais EIKS identifikatoriais arba įvažiavimo kodais.

8.1.7. Padidinto saugumo patalpų mechaninės apsaugos priemonės.

5. Įrengiant serverines, kitas padidinto saugumo, įslaptintos informacijos saugojimo ar darbo su įslaptinta informacija patalpas, vadovautis bendraisiais reikalavimais apsaugos priemonių projektavimui ir įrengimui pateiktais šiame standarte.
6. Durys iš plastiko ar kitų medžiagų su durų skydu iš stiklo nepriskiriamos jokioms apsaugos klasėms, todėl įrengtos svarbiose patalpose (serverinėse, dokumentų saugyklose, techninėse patalpose) turi būti pakeistos naujomis, sumažinant galimus saugumo pažeidžiamumus.
7. Įslaptintos informacijos saugojimo ir darbo su įslaptinta informacija patalpos, kurios yra žemesniame negu 4 m aukštyje nuo žemės paviršiaus, turi būti apsaugotos langais su rėmais, pagamintais iš tvirtos medžiagos, stiklas padengtas 400 mkm apsaugine plėvele, įtvirtinta rėme, lango stakta turi

būti sutvirtinama dviem mūrvinėmis į mūro sieną iš šono, varstomoji lango stakta turi būti sutvirtinama dviem mūrvinėmis į mūro sieną iš šono, varstomoji lango dalis fiksuojama užsklendimo mechaniniu įtaisu jam neleidžiant atsidaryti.

8. Įrengiant padidinto saugumo patalpų duris būtina pateikti UAB Statybos produkcijos sertifikavimo centro (SPSC) išduotus durų atitikties pažymėjimus ar kitų šalių notifikuotų laboratorijų ir jas kontroliuojančių institucijų pateiktus atitikties sertifikatus.

8.1.8. Fizinė apsauga (apsaugos darbuotojai).

1. Fizinė apsauga (apsaugos darbuotojai) arba apsaugininkas, įstatymo nustatyta tvarka įsigijęs licenciją šiai veiklai, vykdoma tik nuomininkui pageidaujant.
2. LR asmens ir turto apsaugos įstatyme suteikta teisė vykdyti apsaugos funkcijas tik apsaugos darbuotojams, apsaugininkai, kurie yra baigę apsaugos darbuotojų mokymo programą (kodas 260086116), išlaikę egzaminus ir nustatyta tvarka gavę teisę dirbti apsaugos darbuotoju, apsaugininku.

Priedas Nr.1

PRIVALOMŲ IR NORMATYVINIŲ DOKUMENTŲ SĄVADAS

1. Lietuvos Respublikos Vyriausybės 2022 m. kovo 30 d. nutarimas Nr. 280. Suvestinė redakcija 2022-12-30.
2. Lietuvos Respublikos Statybos įstatymas. Suvestinė redakcija 2021-01-01.
3. Lietuvos Respublikos Viešųjų pirkimų įstatymas 1996 m. rugpjūčio 13 d. Nr.I-1491. Suvestinė redakcija nuo 2023-01-01 iki 2023-12-31.
4. Lietuvos Respublikos Priešgaisrinės saugos įstatymas 2002 m. gruodžio 5 d. Nr. IX-1225. Suvestinė redakcija 2019-01-01.
5. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 820 „Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo įgyvendinimas“. Suvestinė redakcija 2021-12-21.
6. Lietuvos Respublikos Asmens ir turto apsaugos įstatymas. Nauja redakcija nuo 2018 11 01. Suvestinė redakcija 2020-07-01.
7. Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas. Nauja redakcija nuo 2018 m. birželio 30 d. Nr. I-1374.
8. Europos Sąjungos Bendrasis duomenų apsaugos reglamentas (ES) 2016/679.
9. Lietuvos Respublikos sveikatos apsaugos ministro 2004 m. vasario 12 d. įsakymas Nr. V-65 Lietuvos higienos norma HN 32:2004 „Darbas su video terminalais. Saugos ir sveikatos reikalavimai“. Suvestinė redakcija 2011-03-30.
10. STR 1.04.04:2017. "Statinio projektavimas, projekto ekspertizė". Suvestinė redakcija 2020-09-22.
11. STR 2.02.02:2004. „Visuomeninės paskirties pastatai“. Suvestinė redakcija 2016-06-29.
12. Lietuvos Respublikos aplinkos ministro 2019 m. kovo 29 d. įsakymas Nr. D1-186 STR 2.04.01:2018 „Pastatų atitvaros. Sienos, stogai, langai ir išorinės įėjimo durys“. Suvestinė redakcija 2022-01-01.
13. Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2010 m. gruodžio 7 d. įsakymu Nr. 1-338 patvirtinti „Gaisrinės saugos pagrindiniai reikalavimai“. Suvestinė redakcija 2020-05-01.
14. Priešgaisrinės apsaugos ir gelbėjimo departamento prie VRM direktoriaus patvirtintos „Gaisro aptikimo ir signalizavimo sistemų projektavimo ir įrengimo taisyklės“. Nauja redakcija nuo 2009 m. gegužės 22 d. įsakymu Nr. 1-168.
15. Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2011 m. rugpjūčio 23 d. įsakymu Nr. 1-251 patvirtintos „Gaisrinės saugos inžinerinių sistemų priežiūros rekomendacijos“.
16. Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2007 m. vasario 22 d. įsakymu Nr.1-66 patvirtinti „Normatyviniai statinio saugos dokumentai“. Suvestinė redakcija 2016-05-01.
17. Priešgaisrinės apsaugos ir gelbėjimo departamento prie VRM direktoriaus įsakymu patvirtintos Bendrosios gaisrinės saugos taisyklės. Nauja redakcija nuo 2010 m. liepos 27 d. įsakymu Nr. 1-223. Suvestinė redakcija 2023-05-01.
18. Gaisrinės saugos pagrindiniai reikalavimai. STR 2.01.01:1999 „Esminiai statinio reikalavimai. Higiena, sveikata, aplinkos apsauga“. Suvestinė redakcija 2002-11-09.
19. Statybos taisyklės ST 134637738.12:2023 „Statinių inžinerinių sistemų (nuotolinio ryšio telekomunikacijų) apsaugos nuo įsibrovimo ir apiplėšimo pavojaus signalizavimo, vaizdo stebėjimo, patekimo kontrolės, stacionarių gaisrų gesinimo, gaisro aptikimo ir signalizavimo, elektros įrenginių ir linijų, elektros bei nuotolinio ryšio (telekomunikacijų) inžinerinių tinklų įrengimo darbai“.
20. Lietuvos Respublikos energetikos ministro 2012 m. vasario 3 d. įsakymu Nr. 1-22 patvirtintos „Elektros įrenginių įrengimo bendrosios taisyklės“. Suvestinė redakcija nuo 2023-07-29.
21. Lietuvos Respublikos energetikos ministro 2013 m. kovo 5 d. įsakymu Nr. 1-52 patvirtintos „specialiųjų patalpų ir technologinių procesų elektros įrenginių įrengimo taisyklės“.
22. Lietuvos vyriausiojo archyvaro 2011 m. gruodžio 28 d. įsakymu Nr. V-157 patvirtintoss „Dokumentų saugojimo taisyklės“. Suvestinė redakcija 2022-11-05.
23. Automatinės gaisro aptikimo ir gaisrinės signalizacijos sistemos. LST EN 50130 grupės standartai.
24. Gaisro aptikimo ir signalizavimo sistemos. LST EN 54 grupės standartai.
25. Pavojaus signalizavimo sistemos. Įsibrovimo pavojaus signalizavimo sistemos - LST EN50131 grupės standartai. Suvestinė redakcija 2017.

26. Pavojaus signalizavimo sistemos. Saugumo reikalams naudojamos uždaro kontūro televizinės (CCTV) stebėjimo sistemos“. LST EN 50132 grupės standartai. „Objekto klasifikavimas ir/arba objekto identifikacija“ LST EN 50132-7.
27. Saugumo reikalams naudojamos vaizdo stebėjimo sistemos. LST EN 62676. Taikymo gairės LST EN 62676-4. Suvestinė redakcija 2014.
28. Pavojaus signalizavimo sistemos. Patekimo kontrolės sistemos - LST EN 50133 grupės standartai. Suvestinė redakcija 2009.
29. “Pavojaus signalizavimo sistemos. Pavojaus signalų perdavimo sistemos ir įrenginiai” LST EN 50136.
30. „Pavojaus signalizavimo sistemos - Kombinuotos ar integruotos pavojaus signalizavimo sistemos“ LST EN 50137.
31. Apsauga nuo viršįtampių. IEC EN 61643 - grupės standartai.
32. Statybiniai apkaustai. Spynų šerdys. Reikalavimai ir bandymo metodai. LST EN 1303.
33. Patikimo saugojimo įrenginiai. Atsparumo ugniai klasifikacija ir bandymo metodai. LST EN 1047-1.
34. Patikimo saugojimo įrenginiai. Reikalavimai, klasifikacija atsparumo įsilaužimui bandymo metodai. LST EN 1143-1, LST EN 1143-2.
35. Statybiniai apkaustai. Mechaninės spynos ir jų užraktų plokštelės. Reikalavimai ir bandymo metodai. LST EN 12209:2003/AC:2005**.**
36. Statybiniai apkaustai. Spynų šerdys. Reikalavimai ir bandymų metodai. LST EN 1303:2005.
37. Statybos techninis reglamentas STR 1.02.01:2017 „Statybos dalyvių atestavimo ir teisės pripažinimo tvarkos aprašas“. Suvestinė redakcija 2023-05-01.
38. Evakuacinių spynų gamyba, bandymai, panaudojimas. LST EN 179.
39. Evakuacinė sistema LST EN 1125.
40. Durų užsidarymui ir atsidarymui valdyti durų varčioje sumontuoti durų pritraukėjai. LST EN 1154.