MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

MINIMÁLNY ŠTANDARD PRE AUDIT BEZPEČNOSTI A OCHRANY VYSOKEJ ŠKOLY

prof. Ing. Zdeněk Dvořák, PhD.
pplk. prof. JUDr. et Mgr. Jana Šimonová, PhD.
prof. Ing. Andrej Veľas, PhD.

AKADÉMIA POLICAJNÉHO ZBORU

ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta bezpečnostného inžinierstva

2024

OBSAH

TERMINOLÓGIA OCHRANY MÄKKÝCH CIEĽOV

Audit je súhrn nezávislých, objektívnych, overovacích, hodnotiacich, uisťovacích a konzultačných činností zameraných na zdokonaľovanie riadiacich a kontrolných procesov so zohľadnením medzinárodne uznávaných audítorských štandardov.

Bezpečnostný audit je špecifický systematický proces získavania údajov a ich objektívneho vyhodnocovania navrhnutý na posúdenie bezpečnostných rizík, ktorým čelia v danom prípade školy. Výsledkom sú kontrolné opatrenia alebo protiopatrenia školy na zmiernenie týchto rizík.

Audit bezpečnosti a ochrany školy je komplexný prehľad politík, postupov a fyzického prostredia inštitúcie s cieľom identifikovať a posúdiť potenciálne riziká a zraniteľné miesta. Cieľom auditu je zlepšiť celkovú bezpečnosť a ochranu školskej komunity, vrátane žiakov, študentov, pedagógov, zamestnancov a návštevníkov.

Audit bezpečnosti a ochrany na školách pozostáva z týchto kľúčových oblastí:

- Fyzická bezpečnosť: zahŕňa hodnotenie budov a pozemkov, systémov kontroly prístupu, núdzového osvetlenia a značenia, protipožiarnych systémov a iných opatrení fyzickej bezpečnosti.
- Informačná bezpečnosť: zahŕňa hodnotenie IT infraštruktúry škôl, politík a postupov informačnej bezpečnosti a kybernetickej bezpečnosti.
- Pripravenosť na núdzové situácie a adekvátna reakcia: zahŕňa hodnotenie núdzových plánov, postupov a výcviku školy pre rôzne potenciálne núdzové situácie, ako sú požiare, incidenty so strelnou zbraňou a prírodné katastrofy.
- Prevencia a riešenie incidentov: zahŕňa hodnotenie programov prevencie kriminality na škole, postupov hlásenia a riešenie incidentov, postupy služieb podpory obetí.
- Environmentálna bezpečnosť: zahŕňa hodnotenie politík a postupov škôl pri nakladaní s nebezpečnými látkami, likvidáciou odpadu a inými environmentálnymi rizikami.

Proces auditu bezpečnosti a ochrany na školách pozostáva z nasledujúcich krokov:

1. Plánovanie a určenie rozsahu: audítorský tím definuje rozsah auditu, identifikuje oblasti, ktoré sa majú hodnotiť, a vypracuje harmonogram auditu.
2. Zber údajov: audítorský tím zhromažďuje údaje rôznymi metódami, ako sú dotazník, kontroly dokumentov.
3. Bezpečnostná prehliadka: fyzické preverenie nadobudnutých údajov, rozhovory a obhliadky miest.
4. Analýza a hodnotenie: audítorský tím analyzuje zhromaždené údaje a identifikuje potenciálne riziká a zraniteľné miesta.
5. Spracovanie a implementácia: audítorský tím vypracuje správu, ktorá zhrňuje zistenia auditu a odporúča zlepšenia, nastaví plán implementácie odporúčaní z auditu.
6. Bezpečnostné posúdenie: objektívne zhodnotenie stavu a funkčnosti aplikovaných opatrení fyzickej ochrany školy vyplývajúcich z auditu, je základným prostriedkom pre nastavenie účinného bezpečnostného systému.

Dotazník je vedeckou metódou empirického výskumu, ktorá sa používa v spoločenských vedách na hromadné a rýchle zisťovanie faktov, názorov, postojov, preferencií, hodnôt, motívov, potrieb, záujmov a i. údajov od veľkého počtu respondentov.

Dotazník bezpečnosti a ochrany školy je dotazník primárne zameraných na ochranu osôb na školách distribuovaný na úrovni základných a stredných škôl, ktorý bude spoločne vypĺňaný riaditeľom školy a kontaktným policajtom určeným pre príslušnú školu. Slúži pre rýchle získanie údajov o bezpečnostných incidentoch, preventívnych opatreniach a úrovni zabezpečenia jednotlivých škôl.

Prieskum bezpečnosti je zhromažďovanie terénnych údajov o verejnej mienke na tému bezpečnosť, pričom môžu byť užitočné najmä pri odhaľovaní novovzniknutých hrozieb.

Mäkké ciele sú miesta s vysokou koncentráciou osôb a minimálnym stupňom zabezpečenia proti násilným útokom, alebo prostredie, ktoré je ľahko dostupné, priťahuje množstvo ľudí a je ľahkým cieľom útoku pomocou dostupných zbraní a pomerne jednoduchou taktikou. Sú to napr. školy, cirkevné objekty, nemocnice, kultúrne centrá/podujatia, športové centrá/podujatia, nočné kluby, divadlá, opery, kiná, kaviarne a reštaurácie, objekty verejnej dopravy, ale aj hromadné dopravné prostriedky.

Tvrdé ciele sú chránené resp. strážené objekty, ktoré majú zavedené opatrenia znižujúce riziká útoku, majú realizované technické, organizačné a režimové opatrenia, prípadne fyzickú ochranu. Niektoré nie sú verejnosti prístupné, resp. majú nastavený režim vstupu (vojenské zariadenia, vládne budovy, objekty diplomatických misií, jadrové elektrárne a pod.).

Ozbrojený útočník je ozbrojený páchateľ, ktorý koná s úmyslom usmrtiť alebo zraniť čo najväčší počet osôb; páchateľ orientovaný na hromadné ciele zložené z osôb bez rozdielu rasy, povolania, veku a prípadne iných špecifík; páchateľ útoku so zbraňou, pričom zbraňou rozumieme akýkoľvek predmet, ktorý môže urobiť útok voči telu dôraznejším (napr. strelná zbraň, bodná zbraň, sečná zbraň, alebo dopravný prostriedok).

Prevencia útoku na mäkké ciele predstavuje dlhodobú a cieľavedomú činnosť vedúcu ku zníženiu rizika útoku na mäkký cieľ. Zahŕňa predvídanie rizikových faktorov a spôsoby znižovania rizík útokov prostredníctvom pripravenosti dotknutých osôb, vlády a spoločnosti.

Vysoké školy

Predstavujú vrcholné vzdelávacie, vedecké a umelecké ustanovizne. Poslaním vysokých škôl, ktoré sú súčasťou európskeho priestoru vysokoškolského vzdelávania a spoločného európskeho výskumného priestoru, je prispievať k rozvoju vzdelanosti, poznania, vedy a kultúry v súlade s potrebami spoločnosti, rozvíjať vedomosti, zručnosti, múdrosť, tvorivosť a dobro človeka a tým prispievať k rozvoju vedomostnej spoločnosti. Napĺňanie tohto poslania so zameraním na študenta je predmetom hlavnej činnosti vysokých škôl. Hlavnou úlohou vysokých škôl pri napĺňaní ich poslania je poskytovanie vysokoškolského vzdelávania v súlade s potrebami spoločnosti a tvorivé vedecké bádanie alebo tvorivá umelecká činnosť. Pojem vysoká škola v texte používať jednotne pre označenie univerzít, vysokých škôl a pobočiek zahraničných vysokých škôl.

Povinnosti vysokej školy z pohľadu zákonných ustanovení k bezpečnosti:

Zákon č. 131/2002 Z.z. o vysokých školách v znení neskorších predpisov

§108

Na účely ochrany bezpečnosti osôb a majetku je vysoká škola oprávnená pri riadení prístupu do svojich objektov a miestností spracúvať meno a priezvisko študenta, údaj o tom, či ide o študenta príslušnej vysokej školy a fakulty, číslo preukazu študenta, čas príchodu a čas odchodu; tieto údaje možno na účel podľa prvej vety spracúvať najviac po dobu šiestich mesiacov.

§ 80a

Ak vysoká škola využíva na evidenciu dochádzky, kontrolu prístupu do objektov, zvýšenie bezpečnosti a ochrany zdravia pri práci a na ďalšie účely súvisiace s jej činnosťou elektronický informačný systém, má právo na tento účel uchovávať a spracúvať osobné údaje zamestnancov a využívať ich na uvedené účely aj v elektronických preukazoch zamestnancov. Na uchovávanie a spracúvanie osobných údajov zamestnancov sa vzťahuje zákon (Zákon č. *428/2002 Z. z.* v znení neskorších predpisov)

Poznámka - údaje a informácie zistené v rámci auditu bezpečnosti a ochrany majú citlivý charakter

DEFINOVANIE ROZSAHU AUDITU BEZPEČNOSTI A OCHRANY NA ŠKOLÁCH

- Základné údaje o vysokej škole
- Definovanie aktív a hodnôt, ktoré chceme chrániť - život a zdravie študentov, zamestnancov, návštevníkov (predpokladaný počet osôb v budove/kapacita, počet zamestnancov, počet študentov)
- Aký objekt vysokej školy chcete chrániť? (napr. rektorát, učebný blok, laboratória, ubytovacie internáty, menzu, športoviská, hospodársku budovu ...) Rozdelenie na vonkajšie a vnútorné priestory, dispozícia, plány areálu, budov
- Aké sú Vaše prioritné antropogénne hrozby a riziká? (napr. hrozby – študent, návšteva, zamestnanec, náhodná osoba, riziká - útok so strelnou zbraňou, útok chladnou zbraňou, útok motorovým vozidlom, útok nástražným výbušným systémom, útok otravnou látkou ...)
- Aké sú Vaše rozpočtové a personálne možnosti (objem pripravených finančných prostriedkov a odhad počtu človeko-dní práce počas kalendárneho roka)?

Definovanie rozsahu v kontexte systému ochrany:

1. **Objektová bezpečnosť**- popis a charakteristiku objektu/priestoru, jeho osobitosti, režim vstupu (autorizovaný, bez autorizácie, s kontrolou vstupu bez nežiaducich predmetov, bez kontroly vstupu a pod.), mapa objektu (vonkajší perimeter, vnútorný perimeter), susedné budovy/objekty s ich nuansami,...
2. **Incidenty na škole** – minulá skúsenosť s incidentom, existencia riešeného incidentu na škole,

    - Evidencia incidentu (postup evidovania incidentu, spísanie zápisu, komu je sprístupnený zápis, kto vyhodnotí incident, kto sú najčastejšími partnermi pri riešení incidentov – PZ, vedenie VŠ, iné inštitúcie, ...)
    - postup riešenia incidentu (máme na mysli konkrétneho, ak bol na škole)
    - osobitosti incidentu v pozíciách

        študent - pedagóg,

        pedagóg - pedagóg,

        zamestnanec (administratíva, údržba, služby) - študent

        zamestnanec - pedagóg

        študent - zamestnanec

        pedagóg - zamestnanec

        nadriadený pedagóg – podriadený pedagóg,

        študent – študent

návšteva/bývalý absolvent - študent, alebo pedagóg

3. **Reakcie školy na vonkajšie hrozby a informovanosť na škole-** Preventívne opatrenia

   - Vizualizácia zákazu vstupu s nebezpečnými vecami, výstražné tabule, upozornenia,
   - vizualizácia smerov evakuácie, požiarne plány,
   - vzdelávacie aktivity prípravy školy na prípadne vonkajšie hrozby - školenia, preventívne programy, programy psychologickej pomoci, poradenské centrá

4. **Fyzická ochrana** – prítomnosť bezpečnostného personálu profesionálneho, preškoleného, z externého prostredia, nepreškoleného, prípadne žiadna

   Reakčné prvky (poskytujúce adekvátnu reakciu na mimoriadnu situáciu):

   - Zamestnanci a študenti: Mali by byť informovaní o bezpečnostných postupoch a o tom, ako reagovať v prípade incidentu.
   - Bezpečnostný manažér: Zodpovedá za koordináciu bezpečnostných aktivít a za implementáciu bezpečnostného plánu.
   - Referent krízového riadenia: Zodpovedá za riadenie krízových situácií.
   - Bezpečnostná služba / vlastná ochrana: Poskytuje fyzickú ochranu chráneného objektu a jeho okolia.
   - Vrátnici / informátori – monitorujú situáciu v objekte, dokážu upovedomiť oprávnené osoby.

5. **Technické zabezpečenie** - akými technickými systémami na ochranu osôb a majetku v jednotlivých objektoch a na miestach, ktoré sa javia ako potenciálne mäkké ciele, disponujete?

Poplachové systémy (detekcia): Dôležitá je detekcia rôznych typov hrozieb, ako napr. vniknutie, požiar, únik plynu a pod. Systém by mal byť navrhnutý tak, aby minimalizoval falošné poplachy a aby rýchlo a spoľahlivo detegoval reálne hrozby.

- Monitorovacie a dohľadové systémy (CCTV, VSS): Poskytujú vizuálne monitorovanie chráneného objektu a jeho okolia. Umožňujú identifikáciu páchateľov a zhromažďovanie dôkazov v prípade incidentu. Kamerový systém.
- Systémy na kontrolu a riadenie vstupov: Regulujú prístup do chráneného objektu a umožňujú identifikáciu a autorizáciu osôb (RFID prístupové systémy). Môžu obsahovať detektory nebezpečných predmetov.
- Elektrické zabezpečovacie systémy a tiesňové poplachové systémy: Slúžia na ochranu pred neoprávneným vniknutím a na signalizáciu núdzových situácií. Tiesňové poplachové systémy slúžia na manuálne vyvolanie poplachu
- Poplachové prenosové systémy – MPPC/PCO: Umožňujú prenos poplachových signálov, správ a informácií na monitorovacie a poplachové prijímacie centrum alebo na bezpečnostnú službu.
- Elektrická požiarna signalizácia: Umožňujú identifikáciu miesta požiaru (úmyselne aj neúmyselne založeného), je možné ich využiť ako tiesňový systém.
- Záložné zdroje a zálohovanie systémov ochrany objektov.

Mechanické zábranné prostriedky (spomalenie, zastavenie):

- Perimetrické (ploty, múry, steny, retardéry, zátarasy, výsuvné stĺpy ...): Zabraňujú neoprávnenému vstupu do chráneného objektu a spomaľujú páchateľov.
- Plášťové (okná, dvere, mreže, bezpečnostný systém dvojitých dverí,...): Chránia chránený objekt pred vniknutím a poškodením.
- Predmetové (trezory, pokladnice...): Chránia finančné hotovosti a cenné predmety pred krádežou a poškodením.

Organizačné a režimové opatrenia

- Smernica pre používanie systémov kontroly vstupov, smernica pre kamerové dohľadové systémy, smernica pre EZS/TPS, smernica pre fyzickú ochranu, plán služieb na vrátnici, plán obchôdzok, revízie existujúcich systémov, núdzové plány
- Evidencia návštev, Evidencia vjazdu výjazdu MV, Evidencia vydaných kľúčov, atď.
- Vnútorný rozhlas – riadenie evakuácie, informovanie o bezpečnostnom incidente.
- Označenie zamestnancov, študentov/návštev
- Kompetencie na úseku bezpečnosti

6. **Realizácia manažérstva rizika v objektoch univerzity**:

- Identifikácia aktív – čo je predmetom ochrany, kde sa predmet ochrany nachádza (kde sú zvýšené koncentrácie osôb)
- Identifikujte všetky potenciálne hrozby pre váš mäkký cieľ (vždy pre každú budovu osobitne, ...) Vytvorte katalóg hrozieb. Identifikujte všetky zraniteľnosti, ktoré súvisia s vybraným subjektom. Pod zraniteľnosťou sa vníma slabé miesto zabezpečenia ale aj nedostatočné procesy. Vytvorte katalóg zraniteľnosti.
- Katalóg zraniteľností je potrebné prepojiť s databázou vhodných opatrení, ktoré sú relevantné pre konkrétnu zraniteľnosť
- Zhodnoťte pravdepodobnosť a dopad relevantných rizík (pre každú budovu osobitne...). Pod rizikom sa v tomto prípade myslí, kombinácia potenciálnej úrovne hrozby, zraniteľnosti a ich možného dopadu na aktíva (expertné posúdenie relevantnosti hrozieb, zraniteľností a dopadov) .
- Vhodným nástrojom môže byť kontrolný zoznam, kde budú jednotlivé číselné hodnoty nadobúdať hodnoty podľa škály: nie je = 0, malá hrozba = 1, stredná hrozba = 2, veľká hrozba = 3,....)
- Prioritizujte riziká na základe ich úrovne (expertné posúdenie relevantnosti hrozieb...)

7. **Výber a implementácia vhodných bezpečnostných a ochranných opatrení**:

- Na základe vykonaného posúdenia rizík vyberte vhodné bezpečnostné a ochranné opatrenia z rôznych kategórií (detekcia, prevencia, reakcia, zotavenie).
- Implementujte vybrané opatrenia s ohľadom na vaše špecifické potreby a možnosti.

8. **Testovanie, tréning a aktualizácia**:

- Pravidelne testujte a aktualizujte váš systém ochrany mäkkého cieľa, aby ste sa ubezpečili, že je stále efektívny (Spätná väzba).
- Súčasťou zavedeného systému musí byť plán pravidelného vzdelávania a tréningov zamestnancov univerzity (pre študentov vydať iba informatívne pokyny).

POSTUP VYPRACOVANIA AUDITU BEZPEČNOSTI A OCHRANY

1. Plánovanie a určenie rozsahu auditu: audítorský tím definuje rozsah auditu, identifikuje oblasti a objekty, ktoré sa majú hodnotiť, vypracuje harmonogram auditu.
2. Vstupné rozhovory so zástupcami konkrétnej vysokej školy v kontexte špecifikácie objektu (rektor, dekan, kvestor a pod)
3. Zber údajov: audítorský tím zhromažďuje údaje rôznymi metódami, ako sú dotazník bezpečnosti a ochrany, kontroly dokumentov, komunikáciou a ohliadkou na mieste.
4. Bezpečnostná prehliadka: fyzické preverenie nadobudnutých údajov, rozhovory a obhliadky miest.
5. Vyhodnotenie hrozieb - analýza a hodnotenie- audítorský tím analyzuje zhromaždené údaje a identifikuje potenciálne riziká a zraniteľné miesta. Katalóg významných hrozieb.
6. Spracovanie a implementácia: audítorský tím vypracuje správu z auditu, ktorá zahŕňa zistenia auditu, navrhuje opatrenia na zlepšenia stavu v kontexte relevantných hrozieb, nastaví plán implementácie odporúčaní z auditu.
7. Bezpečnostné posúdenie: objektívne zhodnotenie stavu a funkčnosti aplikovaných opatrení fyzickej ochrany školy vyplývajúcich z auditu, je základným prostriedkom pre nastavenie účinného bezpečnostného systému.

ŠTRUKTÚRA SPRÁVY Z AUDITU BEZPEČNOSTI A OCHRANY VYSOKEJ ŠKOLY

---

1. Úvod auditu bezpečnosti a ochrany VŠ, vymedzenie špecifík VŠ, štúdium bezpečnostnej dokumentácie
2. Bezpečnostná prehliadka objektov VŠ so zameraním na oblasti (zber údajov, môže byť aj formou dotazníka)
3. **Analýza bezpečnostných požiadaviek** - Minimálna úroveň ochrany môže vyplývať z tzv. bezpečnostných požiadaviek, ktoré môžu byť dané:
    a) štátom - prostredníctvom všeobecne záväzných právnych predpisov (bezpečnostné požiadavky podľa zákona o ochrane osobných údajov, podľa zákona o kybernetickej bezpečnosti, podľa zákona o informačných technológiách vo verejnej správe, podľa zákona o súkromnej bezpečnosti),
    b) normalizačným úradom - prostredníctvom technického predpisu (štandardy MZP, EZS/TPS, VSS, EPS, SKV, PPS)
    c) poisťovacou spoločnosťou - prostredníctvom zmluvných podmienok,
    d) materskou spoločnosťou - formou vnútorných organizačných nariadení,
    e) inou treťou stranou - prostredníctvom predpisu, zmluvy, nariadenia, normy, štandardy atď.
4. **Analýza vonkajšieho bezpečnostného prostredia** (dislokácia objektu, plán objektu, okolitá zástavba, okolité porasty, mapy, dislokácia najbližšieho útvaru PZ, alebo zazmluvnenej SBS, potenciálne hrozby)
5. **Analýza vnútorného bezpečnostného prostredia** (pôdorysy budov, kto riadi bezpečnosť, zodpovednosť za jednotlivé úseky bezpečnosti, spôsob riešenia jednotlivých bezpečnostných incidentov, smernice pre výkon FO, prostriedky MZP, EZS/TPS, VSS, EPS, SKV, PPS a ich presná dislokácia).

Poplachové systémy (detekcia): Dôležitá je detekcia rôznych typov hrozieb, ako napr. vniknutie, požiar, únik plynu a pod. Systém by mal byť navrhnutý tak, aby minimalizoval falošné poplachy a aby rýchlo a spoľahlivo detegoval reálne hrozby.

- Monitorovacie a dohľadové systémy (CCTV, VSS): Poskytujú vizuálne monitorovanie chráneného objektu a jeho okolia. Umožňujú identifikáciu páchateľov a zhromažďovanie dôkazov v prípade incidentu. Analýza pokrytia objektov, spôsobu ukladania a vyhodnocovania záznamov, čas ukladania, (rozpoznanie/identifikácia/monitorovanie), nočné videnie.
- Systémy na kontrolu a riadenie vstupov (SKV): Regulujú prístup do chráneného objektu a umožňujú identifikáciu a autorizáciu osôb. Pokrytie (vchody, učebne, vjazdy, garáže, atď.), oprávnenia, prideľovanie oprávnení, kľúčový režim, evidencia...
- Elektrické zabezpečovacie systémy a tiesňové poplachové systémy (EZS/TPS): Slúžia na ochranu pred neoprávneným vniknutím a na signalizáciu núdzových situácií. Detegujú narušenie chránených priestorov v nočných hodinách, pokus o neoprávnený vstup do vybraných priestorov

(strechy, sklady nebezpečných látok a pod.) Tiesňové poplachové systémy slúžia na manuálne vyvolanie poplachu. Pokrytie (budovy, vybrané priestory a pod.), vyhodnocovanie poplachových signálov a správ, pravidelné revízie...

- Poplachové prenosové systémy (PPS): Umožňujú prenos poplachových signálov, správ a informácií na monitorovacie a poplachové prijímacie centrum alebo na bezpečnostnú službu. Minimálne dve nezávislé poplachové prenosové cesty.
- Elektrická požiarna signalizácia (EPS): Umožňujú identifikáciu miesta požiaru (úmyselne aj neúmyselne založeného), je možné ich využiť ako tiesňový systém. Pokrytie objektu/budov.
- Integrácia hore uvedených poplachových systémov. Integrované poplachové systémy.
- Záložné napájacie zdroje, zálohovanie správ.

Mechanické zábranné prostriedky (MZP) (spomalenie, zastavenie):

- Perimetrické (ploty, múry, retardéry, ...): Zabraňujú neoprávnenému vstupu do chráneného objektu a spomaľujú páchateľov.
- Plášťové (okná, dvere, mreže,...): Chránia chránený objekt pred vniknutím a poškodením.
- Predmetové (trezory, ...): Chránia cenné predmety pred krádežou a poškodením.
- Prostriedky k zabráneniu vstupu na strechy budov

Reakčné prvky (poskytujúce adekvátnu reakciu na mimoriadnu situáciu):

- Zamestnanci a študenti: Mali by byť informovaní o bezpečnostných postupoch a o tom, ako reagovať v prípade incidentu.
- Bezpečnostný manažér: Zodpovedá za koordináciu bezpečnostných aktivít a za implementáciu bezpečnostného plánu.
- Referent krízového riadenia: Zodpovedá za riadenie krízových situácií.
- Bezpečnostná služba / vlastná ochrana: Poskytuje fyzickú ochranu chráneného objektu a jeho okolia.
- Vrátnici / informátori – monitorujú situáciu v objekte, dokážu upovedomiť oprávnené osoby.
- Vyrozumenie osôb v rámci objektu - Evakuačný rozhlasový systém, SMS, iné spôsoby.

Organizačné a režimové opatrenia

- Smernica pre používanie systémov kontroly vstupov, smernica pre kamerové dohľadové systém, smernica pre EZS/TPS, smernica pre fyzickú ochranu, plán služieb na vrátnici, plán obchôdzok, revízie existujúcich systémov, núdzové plány
- Vediete Evidenciu návštev, Evidenciu vjazdu výjazdu MV, Evidencia vydaných kľúčov, atď.
- Označenie zamestnancov, študentov/návštev
- Kompetencie na úseku bezpečnosti

Preventívne opatrenia
    - Výstražné tabule, upozornenia, smery evakuácie, požiarne plány, školenia, preventívne programy, programy psychologickej pomoci, poradenské centrá
6. **Manažment rizík** (Klasifikácia úrovne hrozby, úrovne zraniteľnosti, dopadu na aktíva, kritéria hodnotenia rizík, klasifikácia rizika podľa celkového bodového hodnotenia, možné scénare útokov, register a ohodnotenie hrozieb, register a ohodnotenie zraniteľných miest, register a ohodnotenie aktív, určenie subjektívnej pravdepodobnosti, hodnotenie rizík, bezpečnostný protokol

7. **Návrh opatrení** (stratégia zaobchádzania s rizikami, návrh zmien v systéme ochrany objektu, návrhy a odporúčania, náklady a prínosy). Na základe identifikovaných hrozieb a slabých miest, vytvorenie konkrétneho plánu na adresovanie a zlepšenie bezpečnostných opatrení, vrátane časového rámca a odhadovaných nákladov.

8. **Záver** rozpracovaný detailne pre rektora vysokej školy a informatívne pre správnu radu vysokej školy. Na základe identifikovaných hrozieb a slabých miest vytvorenie konkrétneho plánu na adresovanie a zlepšenie bezpečnostných opatrení vrátane časového rámca a odhadovaných nákladov. Mechanizmy pre získavanie spätnej väzby od študentov a zamestnancov o ich pohľade na bezpečnosť a návrhy na jej zlepšenie.

MINIMÁLNE ODPORÚČANIA PRE ŠKOLY

Minimálny (odporúčaný) štandard pre školy by mal vychádzať z minimálnych požiadaviek na zabezpečenie objektov a zo súčasne platných právnych predpisov.

Vonkajšie prostredie

Keďže školy na Slovensku boli historicky zakladané v rôznych obdobiach a v rôzne situovaných objektoch, je potrebné venovať pozornosť zabezpečeniu perimetra (okolia) objektu. Perimetrom je myslené okolie objektu. Ochranné prvky sú predovšetkým plotové systémy a bariéry. Tie by mali byť situované tak, aby nebol umožnený vjazd motorovým vozidlom (okrem vozidiel záchranných zložiek) do areálu školy neoprávneným osobám. V prípade vjazdu výjazdu zamestnancov a zásobovania, by mal byť vstup riadený vhodným prostriedkom. Odporúča sa vytvorenie vhodných parkovacích miest pre verejnosť, umožňujúce bezpečné nastupovanie a vystupovanie žiakov/študentov.

Oplotenie objektu by malo byť udržiavané a neporušené. Z pohľadu štandardov poisťovní a technických noriem by malo mať výšku viac ako 100 cm. Je vhodné, ak sa dá oplotenie objektu uzamknúť ako prevencia proti vonkajšiemu narušiteľovi, v prípade, že študenti sa pohybujú na nádvorí objektu, prípadne prináležiacich športoviskách. Plochy v okolí perimetra by mali byť udržiavané a bez kríkov, či lesných porastov. Popri budovách by mali byť jasne odčlenené (bariérou, betónovými stĺpikmi) a vedené chodníky, ktoré majú byť dostatočne široké pre bezpečný pohyb osôb. Vstup do objektu školy by mal byť riadne označený, že sa jedná o priestor vysokej školy. Verejné používanie športovísk v areáli školy prináša riziká, ktoré je potrebné zvážiť. Jedná sa o príležitosť pre potenciálnych páchateľov na obhliadku objektov a úroveň ich zabezpečenia. Perimeter objektu je možné monitorovať kamerovým systém s využitím inteligentných algoritmov na identifikáciu ŠPZ, prekonania oplotenia a pohybu v vo vyhradenom priestore. Monitorovanie kamerovým dohľadovým systémom je fakultatívne a závisí od finančných možností školy.

V nočných hodinách sa odporúča vonkajšie osvetlenie perimetra, ktoré umožňuje detekciu bezpečnostných incidentov.

Plášť budovy

Plášť budovy by mal byť navrhnutý a situovaný tak, aby minimalizoval možnosť ukrytia sa a krytý prístup k oknám, alebo dverám objektu. Všetky dvere na plášti budovy musia mať možnosť uzamknutia a počas prevádzky by mali byť uzamknuté. Pre vylúčenie neoprávneného vstupu do budovy by mal byť jasne označený vstup do budovy s elektronickým zvončekom. Osoba otvárajúca dvere pre návštevy musí mať prehľad o tom, kto do objektu vstupuje. Pre tento účel je možné využiť je možné kamerový systém, alebo videovrátnik. Výhodou je možnosť obojsmernej komunikácie. Návštevný režim by mal byť jasne stanovený. Taktiež musí byť jasný spôsob príchodu odchodu zamestnancov a ich evidencia. Zároveň musí byť jasný spôsob opustenia školy zamestnancami a študentmi v osobitných prípadoch (náhly odchod k lekárovi). V prípade, že objekt má vrátnicu, mala by obsahovať tiesňové tlačidlo.

Všetky prístupy na rebríky vedúce na strechy musia byť zabezpečené. Taktiež vstupy do technických priestorov, kotolní, alebo suterénu. Zvody, prípadne hromozvody by mali obsahovať zábranu proti šplhaniu, prípadne lezeniu na strechy. Okná budov na prízemí v rizikových lokalitách by nemali umožňovať úplné otvorenie. V prípade, že áno, mali by byť doplnené o vhodne kotvené mreže. Odporúča sa inštalovať na okná obmedzovače otvorenia. Vonkajšie dvere by mali obsahovať uzatvárací mechanizmus a detekciu otvorenia dverí magnetickým kontaktom. Zámky dverí by mali mať pasívnu odolnosť podľa STN EN 1627 RC.3

a vyššiu. Zároveň by mali obsahovať upozornenie, že ich otvorenie spôsobí poplach. Vonkajšie i vnútorné dvere by mali umožňovať uzamknutie. Vhodný je systém generálneho kľúča alebo uzamykania zvnútra priamo v dverách. Dvere by mali byť otvárané tak, aby umožňovali bezproblémovú evakuáciu. Za otváranie/uzatváranie dverí je vhodné určiť zodpovednú osobu.

Vnútorné prostredie

Vstup do objektu by mal byť v rámci možností evidovaný. Vhodné sú prístupové systémy na báze rádiofrekvenčných technológií (RFID.

Vnútorné priestory objektov škôl je možné rozčleniť na verejnú a neverejnú časť, prípadne na jednotlivé zóny a monitorovať pohyb medzi nimi. Zóny môžu mať rôzne stupne odolnosti.

Kľúče od dverí učební by mali mať učitelia počas výučby pri sebe. Umožní to v prípade bezpečnostného incidentu uzavrieť triedu.

Dôležité je označenie priestorov pre zjednodušenie orientácie a označenie únikový trás.

V školách je možné využívať aktivity, umožňujúce kontrolu a evidenciu vstupu. Napr. Vstup do IT miestností, vstup do špecializovaných učební, knižnice, a pod.

Serverovne by mali byť zabezpečené, servery uzamknuté v bezpečnostných skriniach typu RACK. Rozvodné skrine elektriny a plynu by mali byť riadne označené a zabezpečené pred neoprávneným prístupom.

Kamerový systém v objekte školy je možné využiť na dohľadávanie bezpečnostných incidentov z minulosti, alebo online monitorovanie oprávnenou osobou. Výhodou je použitie umelej inteligencie na vyhľadávanie bezpečnostných incidentov v reálnom čase s adekvátnym zásahom. Kamerovým systémom môžu byť monitorované miesta s potenciálnou možnosťou vzniku bezpečnostného incidentu (vchody, šatne, chodby, triedy, perimeter objektu a ďalšie).

Vnútorné priestory v nočných hodinách, prípadne mimo prevádzkových hodín cez víkendy a v čase voľna musia byť uzamknuté. Môžu byť chránené elektrickým zabezpečovacím a tiesňovým poplachovým systémom (EZS/TPS) s prenosom poplachu na monitorovacie poplachové prijímacie centrum/Pult centralizovanej ochrany Policajného zboru/Mestskej polície, prípadne osoby, ktoré dokážu zabezpečiť adekvátny zásah. Zároveň môžu byť monitorované kamerovým dohľadovým systémom, pre overenie poplachovej informácie. Elektrický zabezpečovací systém je možné využiť aj pre detekciu neoprávneného prístupu do skladov, laboratórií a dielní v čase mimo výučby, takže môžu slúžiť aj ako systém na kontrolu vstupov (doplnenie o klávesnice, resp. čítačky vo vybraných priestoroch)

Elektrický zabezpečovací a tiesňový poplachový systém je možné využiť aj na manuálne vyvolanie poplachu v prípade tiesne (bezpečnostný incident, zdravotné problémy a pod.). Tiesňové tlačidlá môžu byť umiestnené v triedach a chodbách pod skleneným rozbitným krytom, alebo môžu byť nositeľné učiteľmi vo forme príveskov.

Režimové opatrenia

Tieto opatrenia sa týkajú pokynov, príkazov, obmedzení, smerníc a slúžia k nastaveniu režimu objektu. Režimové opatrenia sa týkajú zamestnancov, návštev, študentov a informácií v rámci objektu. Školy by mali mať vypracovaný (okrem školského poriadku a ďalších dokumentov stanovených nadriadenými orgánmi školy):

- Režim vjazdu/výjazdu motorových vozidiel,
- Režim vstupu/výstupu osôb,
- Režim prideľovania identifikačných predmetov (čipy, tokeny),
- Režim obsluhy systémov technickej ochrany objektov,
- Postupy pre mimoriadne situácie/Evakuačný plán, atď.

Fyzická ochrana

Osoby poverené výkonom fyzickej ochrany musia spĺňať náležitosti stanovené zákonom NR SR č. 473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Podľa tohoto zákona je možné strážnu službu realizovať komerčne na základe zmluvy s vybranou Súkromnou bezpečnostnou službou (SBS), alebo formou Vlastnej ochrany (VO) vlastnými zamestnancami v pracovno-právnom pomere.

Doba, rozsah, podmienky výkonu a ďalšie detaily sú zvyčajne stanovené v smernici pre výkon strážnej služby.

POZOR! Vrátnici nie sú oprávnení vykonávať zásah v oblasti ochrany osôb a majetku. Zásah v objekte sú oprávnení vykonávať príslušníci Policajného zboru, prípadne Mestskej polície.

Vrátnici sú informátormi, ktorí môžu viesť evidenciu návštev tak, že sa osoba sama zapíše do zoznamu návštev.

V prípade, že je fyzická ochrana realizovaná zmluvne SBS, alebo vlastnými zamestnancami VO môžu tieto osoby:

- Monitorovať vnútorné i vonkajšie priestory prostredníctvom kamerových dohľadových systémov.
- Môžu použiť vecné donucovacie prostriedky a ďalej podľa zákona 473/2005:
    - Presvedčiť sa zrakom, hmatom alebo technickými prostriedkami, či ten, kto vstupuje do chráneného objektu alebo na chránené miesto alebo z neho vystupuje, nemá pri sebe alebo na sebe predmety pochádzajúce z protiprávnej činnosti súvisiacej s chráneným objektom, chráneným miestom alebo chránenou osobou alebo nemá pri sebe alebo na sebe predmety, ktorými by mohol spáchať protiprávnu činnosť, a tieto mu odobrať.
    - Zakázať vstup do chráneného objektu alebo na chránené miesto nepovolaným osobám.
    - Zakázať vstup do chráneného objektu alebo na chránené miesto osobám, ktoré majú pri sebe zbraň, ak je do chráneného objektu alebo na chránené miesto vstup so zbraňou zakázaný.
    - Viesť evidenciu o vstupe alebo výstupe osôb a dopravných prostriedkov do chráneného objektu alebo z chráneného objektu alebo na chránené miesto alebo z chráneného miesta; na tento účel je oprávnený vyžadovať preukázanie totožnosti alebo preukázanie príslušnosti k ozbrojenému zboru, ozbrojenému bezpečnostnému zboru alebo ozbrojeným silám Slovenskej republiky.
    - Zaznamenávať technickými prostriedkami vstup alebo výstup osôb a dopravných prostriedkov do chráneného objektu alebo na chránené miesto alebo z chráneného objektu alebo z chráneného miesta.
    - Vyžadovať preukázanie totožnosti u osoby, ktorá je pristihnutá pri páchaní priestupku alebo trestného činu, ktorý súvisí s výkonom fyzickej ochrany, alebo bezprostredne po spáchaní takéhoto priestupku alebo trestného činu.
    - V súvislosti s výkonom fyzickej ochrany vyžadovať preukázanie totožnosti osoby, ktorá bola pristihnutá pri neoprávnenom vstupe do chráneného objektu alebo na chránené miesto, alebo osoby, ktorá bola pristihnutá pri neoprávnenom výstupe z chráneného objektu alebo z chráneného miesta.

- Presvedčiť sa, či ten, kto vstupuje do chráneného objektu alebo na chránené miesto s dopravným prostriedkom alebo z neho vystupuje s dopravným prostriedkom, nemá v dopravnom prostriedku alebo na dopravnom prostriedku predmety alebo zvieratá pochádzajúce z protiprávnej činnosti súvisiacej s chránenou osobou alebo s chráneným objektom.
- Vyviesť nepovolanú osobu z chráneného objektu alebo z chráneného miesta.

Bezpečnostná dokumentácia

Bezpečnostná dokumentácia školy poukazuje na dôležitosť ochrany života a zdravia študentov, ale aj dôležitosť ochrany majetku. Bezpečnostná dokumentácia by mala obsahovať:

- Stratégiu bezpečnosti (dlhodobé ciele), resp. Bezpečnostnú politiku,
- Bezpečnostné smernice, Bezpečnostný protokol
- Plán areálu, resp. objektov v areáli školy,
- Dokumentácia k prvkom technickej ochrany objektov, revízne správy, záznamy o školenia, oprávnené osoby
- Zmluvy o poskytovaní fyzickej ochrany a k technickej ochrane objektov
- Evidencia bezpečnostných incidentov
- Postupy pre riešenie bezpečnostných incidentov

Ako to využiť v rámci interného auditu?

- Uvedený postup je potrebné dodržať. Pri posudzovaní jednotlivých oblastí je potrebné dodržať platné právne predpisy, technické normy, normalizačné informácie a pravidlá dobrej praxe.
- Audit je možné vykonať aj vlastnými zamestnancami (FBI UNIZA, APZ, AOS M. R. Štefánika)
- Výstup interného auditu je potrebné predložiť rektorovi na vykonanie opatrení, správnej rade iba záver pre informáciu (určite nie Akademickému senátu)

Ako využiť v rámci externého auditu?

- Pri verejnom obstarávaní auditu môžu vzniknúť problémy v porovnateľnosti výstupov, avšak napriek možným nedostatkom, vykonanie auditu podľa postupu hore umožní zvýšenie úrovne bezpečnosti, ochrany a povedomia o fyzickej a objektovej bezpečnosti na univerzitách.

Zoznam noriem a odporúčané informačné zdroje v ochrane mäkkých cieľov

NORMY A PRÁVNE PREDPISY SÚVISIACE S BEZPEČNOSŤOU ŠKÔL

Predchádzanie zločinnosti

Zákon NR SR č. 583/ 2008 Z. z. o prevencii kriminality a inej protispoločenskej činnosti a o zmene a doplnení niektorých zákonov.

STN P CEN/TS 14383-1 Predchádzanie zločinnosti. Územné plánovanie a navrhovanie. Časť 1: Definície špecifických termínov.

STN P CEN/TS 14383-2 Predchádzanie zločinnosti prostredníctvom navrhovania budov, územného plánovania a údržby mesta. Časť 2: Zásady a postup.

STN P CEN/TS 14383-3 Predchádzanie zločinnosti. Územné plánovanie a navrhovanie. Časť 3: Obytné priestory.

STN P CEN/TS 14383-4 Predchádzanie zločinnosti. Územné plánovanie a navrhovanie. Časť 4: Obchodné a administratívne priestory.

STN P CEN/TS 14383-5 Predchádzanie zločinnosti. Územné plánovanie a navrhovanie. Časť 5: Čerpacie stanice pohonných hmôt.

STN P CEN/TS 14383-6 Predchádzanie zločinnosti. Územné plánovanie a navrhovanie budov. Časť 6: Školy a vzdelávacie inštitúcie.

TNI CEN/TR 14383-7 Predchádzanie zločinnosti. Územné plánovanie a navrhovanie budov. Časť 7: Navrhovanie a manažérstvo zariadení a priestorov verejnej dopravy.

TNI CEN/TR 14383-8 Predchádzanie zločinnosti. Územné plánovanie a navrhovanie. Časť 8: Ochrana budov a priestorov proti kriminálnym útokom vozidlami.

EZS/TPS - Elektrické zabezpečovacie a tiesňové poplachové systémy

STN EN 50131-1 (33 4591) Poplachové systémy. Elektrické zabezpečovacie systémy. Časť 1: Všeobecné požiadavky.

STN EN 50131-1/Z1 (33 4591) Poplachové systémy. Elektrické zabezpečovacie a tiesňové poplachové systémy. Časť 1: Požiadavky na systém.

STN EN 50131-1/Zmena IS2. Poplachové systémy. Elektrické zabezpečovacie a tiesňové poplachové systémy. Časť 1: Požiadavky na systém.

STN EN 50131-1/Zmena A2 Poplachové systémy. Elektrické zabezpečovacie a tiesňové poplachové systémy. Časť 1: Požiadavky na systém.

STN EN 50131-1/Zmena A3 Poplachové systémy. Elektrické zabezpečovacie a tiesňové poplachové systémy. Časť 1: Požiadavky na systém.

STN P CLC/TS 50131-2-2 (33 4591) Poplachové systémy. Elektrické zabezpečovacie systémy. Časť 2-2: Požiadavky na pasívne infračervené detektory.

STN P CLC/TS 50131-2-3 (33 4591) Poplachové systémy. Elektrické zabezpečovacie systémy. Časť 2-3: Požiadavky na mikrovlnové detektory.

STN EN 50131-2-3/Zmena IS1 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-3: Požiadavky na mikrovlnné detektory.

STN EN 50131-2-4 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-4: Požiadavky na kombinované pasívne infračervené a mikrovlnné detektory.

STN P CLC/TS 50131-2-5 (33 4591) Poplachové systémy. Elektrické zabezpečovacie systémy. Časť 2-5: Požiadavky na kombinované pasívne infračervené a ultrazvukové detektory.

STN CLC/TS 50131-2-6 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-6: Kontakty otvorenia (magnetické).

STN EN 50131-2-6/Zmena IS1 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-6: Kontakty otvorenia (magnetické).

STN EN 50131-2-7-1 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-7-1: Detektory narušenia. Detektory rozbitia skla (akustické).

STN EN 50131-2-7-1/Zmena A1 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-7-1: Detektory narušenia. Detektory rozbitia skla (akustické).

STN EN 50131-2-7-1/Zmena IS1 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-7-1: Detektory narušenia. Detektory rozbitia skla (akustické).

STN EN 50131-2-7-1/Zmena A2 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-7-1: Detektory narušenia. Detektory rozbitia skla (akustické).

STN EN 50131-2-7-2 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-7-2: Detektory narušenia. Detektory rozbitia skla (pasívne).

STN EN 50131-2-7-2/Zmena IS1 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-7-2: Detektory narušenia. Detektory rozbitia skla (pasívne).

STN EN 50131-2-7-2/Zmena A1 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-7-2: Detektory narušenia. Detektory rozbitia skla (pasívne).

STN EN 50131-2-7-2/Zmena A2 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-7-2: Detektory narušenia. Detektory rozbitia skla (pasívne).

STN EN 50131-2-7-3 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-7-3: Detektory narušenia. Detektory rozbitia skla (aktívne).

STN EN 50131-2-7-3/Zmena A1 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-7-3: Detektory narušenia. Detektory rozbitia skla (aktívne).

STN EN 50131-2-7-3/Zmena A2 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-7-3: Detektory narušenia. Detektory rozbitia skla (aktívne).

STN EN 50131-2-7-3/Zmena IS1 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-7-3: Detektory narušenia. Detektory rozbitia skla (aktívne).

STN EN 50131-2-8 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-8: Detektory narušenia. Detektory otrasov.

STN P CLC/TS 50131-2-9 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-9: Detektory narušenia. Aktívne infračervené detektory.

STN EN 50131-2-10 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-10: Detektory narušenia. Kontakty stavu zopnutia (magnetické).

STN P CLC/TS 50131-2-11 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 2-11: Detektory narušenia. ALDDR.

STN P CLC/TS 50131-3 (33 4591) Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 3: Ústredne.

STN EN 50131-4 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 4: Výstražné zariadenia.

STN P CLC/TS 50131-5-1 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Prepojenia. Časť 5-1: Požiadavky na vodičové prepojenie I&HAS zariadení umiestnených v chránených priestoroch.

STN EN 50131-5-3 (33 4591) Poplachové systémy. Elektrické zabezpečovacie systémy. Časť 5-3: Požiadavky na prepojovacie zariadenia využívajúce techniku rádiového prenosu.

STN P CLC/TS 50131-5-4 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 5-4: Skúšanie kompatibility systému pre zariadenia EZS/TPS umiestnené v chránených priestoroch.

STN EN 50131-6 (33 4591) Poplachové systémy. Elektrické zabezpečovacie systémy. Časť 6: Napájacie zdroje.

STN EN 50131-6/Zmena A1 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 6: Napájacie zdroje.

STN P CLC/TS 50131-7 (33 4591) Poplachové systémy. Elektrické zabezpečovacie systémy. Časť 7: Pokyny na používanie.

STN EN 50131-8 (33 4591) Poplachové systémy. Elektrické zabezpečovacie systémy. Časť 8: Zabezpečovacie zahmlievacie zariadenia/systémy.

STN P CLC/TS 50131-9 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 9: Overenie poplachu. Metódy a zásady.

STN EN 50131-10 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 10: Špecifické požiadavky na použitie prijímača/vysielača chránených priestorov (SPT).

STN P CLC/TS 50131-11 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 11: Tiesňové hlásiče.

STN P CLC/TS 50131-11/Zmena IS1 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 11: Tiesňové hlásiče.

STN P CLC/TS 50131-12 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 12: Metódy a požiadavky na nastavenie a uvedenie do pôvodného stavu poplachových zabezpečovacích systémov (IAS).

STN EN 50131-13 Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 13: Bezpečnostné pyrotechnické ochranné zariadenia.

STN EN 50131-13/Oprava AC Poplachové systémy. Elektrické zabezpečovacie a tiesňové systémy. Časť 13: Bezpečnostné pyrotechnické ochranné zariadenia.

Technické normalizačné informácie k EZS/TPS

TNI 33 4591 Komentár k STN P CLC/TS 50131-7: 2004 Prehliadky a funkčné skúšky EZS Odborné prehliadky elektrickej inštalácie

TNI 334591-1 (334591) Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Návrh systému PZTS - Komentář k ČSN CLC/TS 50131-7: 2011.

TNI 334591-2 (334591) Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 2: Montáž PZTS - Komentář k ČSN CLC/TS 50131-7: 2011.

TNI CLC/TR 50515 Súbor vysvetlení k normám na poplachové systémy.

TNI CLC/TR 50531 Poplachové systémy. Termíny a definície.

CCTV – obrazové sledovacie systémy

STN EN 62676-1-1 Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 1-1: Požiadavky na obrazové systémy.

STN EN 62676-1-1/Oprava AC Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 1-1: Požiadavky na obrazové systémy.

STN EN 62676-1-2 (334592) Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 1-2: Obrazový prenos. Všeobecné požiadavky na obrazový prenos.

STN EN 62676-1-2/Oprava AC Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 1-2: Obrazový prenos. Všeobecné požiadavky na obrazový prenos.

STN EN 62676-2-1 Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 2-1: Obrazové prenosové protokoly. Všeobecné požiadavky.

STN EN 62676-2-2 Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 2-2: Obrazové prenosové protokoly. Implementácia IP interoperability založená na službách HTTP a REST.

STN EN IEC 62676-2-31 Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 2-31: Živý prenos a riadenie založené na webových službách.

STN EN IEC 62676-2-32 Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 2-32: Riadenie záznamu a reprodukcie založené na webových službách.

STN EN IEC 62676-2-33 Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 2-33: Obrazové prenosové protokoly. Vzostupné spojenie (uplink) na cloud a prístup k vzdialenému systému riadenia.

STN EN 62676-3 Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 3: Analógové a digitálne videorozhrania.

STN EN 62676-3/Oprava AC Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 3: Analógové a digitálne videorozhrania.

STN EN 62676-4 (334592) Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 4: Pokyny na používanie.

STN EN IEC 62676-5 Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 5: Špecifikácie údajov a charakteristiky kvality zobrazenia kamerových zariadení.

SKV – systémy kontroly vstupov

STN EN 60839-11-1 (334593) Poplachové a elektronické bezpečnostné systémy. Časť 11-1: Elektronické systémy kontroly vstupov. Požiadavky na systém a jeho súčasti.

STN EN 60839-11-1/Oprava AC2 Poplachové a elektronické bezpečnostné systémy. Časť 11-1: Elektronické systémy kontroly vstupov. Požiadavky na systém a jeho súčasti.

STN EN 60839-11-2 (334593) Poplachové a elektronické bezpečnostné systémy. Časť 11-2: Elektronické systémy kontroly vstupov. Pokyny na používanie.

STN EN 60839-11-2/Oprava AC Poplachové a elektronické bezpečnostné systémy. Časť 11-2: Elektronické systémy kontroly vstupov. Pokyny na používanie.

STN EN IEC 60839-11-5 Poplachové a elektronické bezpečnostné systémy. Časť 11-5: Elektronické systémy zabezpečenia prístupu. Protokol OSDP (Open Supervised Device Protocol).

STN EN 60839-11-31 Poplachové a elektronické bezpečnostné systémy. Časť 11-31: Elektronické systémy zabezpečenia prístupu. Základný protokol interoperability na báze webových služieb.

STN EN 60839-11-32 Poplachové a elektronické bezpečnostné systémy. Časť 11-32: Elektronické systémy zabezpečenia prístupu. Monitorovanie zabezpečenia prístupu na báze webových služieb.

STN EN IEC 60839-11-33 Poplachové a elektronické bezpečnostné systémy. Časť 11-33: Elektronické systémy zabezpečenia prístupu. Konfigurácia zabezpečenia prístupu na báze webových služieb.

TPS – Tiesňové poplachové systémy

STN EN 50134-1 (33 4594) Poplachové systémy. Systémy privolania pomoci. Časť 1: Požiadavky na systém.

STN EN 50134-2 Poplachové systémy. Systémy privolania pomoci. Časť 2: Aktivačné zariadenia.

STN EN 50134-3 Poplachové systémy. Systémy privolania pomoci. Časť 3: Miestna jednotka a ovládač.

STN EN 50134-3/Oprava AC Poplachové systémy. Systémy privolania pomoci. Časť 3: Miestna jednotka a ovládač.

STN EN 50134-5 Poplachové systémy. Systémy privolania pomoci. Časť 5: Prepojenia a prenos správ.

STN EN 50134-7 Poplachové systémy. Systémy privolania pomoci. Časť 7: Pokyny na používanie.

STN P CLC/TS 50134-9 Poplachové systémy. Systémy privolania pomoci. Časť 9: IP komunikačný protokol.

PPS – poplachové prenosové systémy

STN EN 50136-1 (33 4596) Poplachové systémy. Poplachové prenosové systémy a zariadenia. Časť 1-1: Všeobecné požiadavky na poplachové prenosové systémy.

STN EN 50136-1/Zmena A1 Poplachové systémy. Poplachové prenosové systémy a zariadenia. Časť 1: Všeobecné požiadavky na poplachové prenosové systémy.

STN EN 50136-2 Poplachové systémy. Poplachové prenosové systémy a zariadenia. Časť 2: Požiadavky na prijímač/vysielač chránených priestorov.

STN EN 50136-2/Zmena A1 Poplachové systémy. Poplachové prenosové systémy a zariadenia. Časť 2: Požiadavky na prijímač/vysielač chránených priestorov.

STN EN 50136-3 Poplachové systémy. Poplachové prenosové systémy a zariadenia. Časť 3: Požiadavky na prijímač/vysielač prijímacieho centra.

STN P CLC/TS 50136-4 Poplachové systémy. Poplachové prenosové systémy a zariadenia. Časť 4: Indikačné zariadenia využívané v poplachových dohľadových strediskách.

STN P CLC/TS 50136-7 Poplachové systémy. Poplachové prenosové systémy a zariadenia. Časť 7: Pokyny na používanie.

STN P CLC/TS 50136-9 Poplachové systémy. Poplachové prenosové systémy a zariadenia. Časť 9: Požiadavky na spoločný protokol na prenos poplachu používajúci Internet Protocol (IP).

STN P CLC/TS 50136-10 Poplachové systémy. Poplachové prenosové systémy a zariadenia. Časť 10: Požiadavky na vzdialený prístup.

Systémy perimetrickej ochrany

STN P CLC/TS 50661-1 Poplachové systémy. Systémy vonkajšej perimetrickej ochrany. Časť 1: Požiadavky na systém.

Integrované bezpečnostné systémy

STN P CLC/TS 50398 Poplachové systémy. Kombinované a integrované poplachové systémy. Všeobecné požiadavky.

STN EN 50398-1 Poplachové systémy. Kombinované a integrované poplachové systémy. Časť 1: Všeobecné požiadavky.

Poplachové systémy všeobecne

STN EN 50130-4 Poplachové systémy. Časť 4: Elektromagnetická kompatibilita. Norma na skupinu výrobkov: Požiadavky na odolnosť súčastí požiarnych, zabezpečovacích a tiesňových systémov, systémov CCTV, systémov kontroly vstupu a systémov privolania pomoci.

STN EN 50130-4/Zmena A1 Poplachové systémy. Časť 4: Elektromagnetická kompatibilita. Norma na skupinu výrobkov: Požiadavky na odolnosť súčastí požiarnych, zabezpečovacích a tiesňových systémov, systémov CCTV, systémov kontroly vstupu a systémov privolania pomoci.

STN EN 50130-5 Poplachové systémy. Časť 5: Skúšobné metódy vplyvu prostredia.

EPS – elektrická požiarna signalizácia

STN 342710 (342710) Predpisy pre zariadenia elektrickej požiarnej signalizácie.

STN 730875 (730875) Požiarna bezpečnosť stavieb. Navrhovanie elektrickej požiarnej signalizácie.

STN EN 54-1 Elektrická požiarna signalizácia. Časť 1: Úvod.

STN EN 54-2+AC Elektrická požiarna signalizácia. Časť 2: Ústredňa elektrickej požiarnej signalizácie.

STN EN 54-3+A1 Elektrická požiarna signalizácia. Časť 3: Zariadenia akustickej poplachovej signalizácie požiaru.

STN EN 54-4+AC Elektrická požiarna signalizácia. Časť 4: Napájacie zariadenia.

STN EN 54-4+AC/Zmena A1 Elektrická požiarna signalizácia. Časť 4: Napájacie zariadenia.

STN EN 54-5+A1 Elektrická požiarna signalizácia. Časť 5: Tepelné hlásiče. Bodové tepelné hlásiče.

STN EN 54-7 Elektrická požiarna signalizácia. Časť 7: Dymové hlásiče. Bodové hlásiče využívajúce rozptyl svetla, prenikajúce svetlo alebo ionizáciu.

STN EN 54-10 Elektrická požiarna signalizácia. Časť 10: Plameňové hlásiče. Bodové hlásiče.

STN EN 54-10/Zmena A1 Elektrická požiarna signalizácia. Časť 10: Plameňové hlásiče. Bodové hlásiče.

STN EN 54-11 Elektrická požiarna signalizácia. Časť 11: Tlačidlové hlásiče požiaru.

STN EN 54-11/Zmena A1 Elektrická požiarna signalizácia. Časť 11: Tlačidlové hlásiče požiaru.

STN EN 54-12 Elektrická požiarna signalizácia. Časť 12: Dymové hlásiče. Lineárne hlásiče využívajúce optický svetelný lúč.

STN EN 54-13+A1 Elektrická požiarna signalizácia. Časť 13: Posúdenie kompatibility a pripojiteľnosti súčastí systému.

STN EN 54-16 Elektrická požiarna signalizácia. Časť 16: Ústredňa hlasovej signalizácie požiaru.

STN EN 54-17 Elektrická požiarna signalizácia. Časť 17: Oddeľovacie prvky proti skratu.

STN EN 54-18 Elektrická požiarna signalizácia. Časť 18: Zariadenia vstupu/výstupu.

STN EN 54-18/Oprava AC Elektrická požiarna signalizácia. Časť 18: Zariadenia vstupu/výstupu.

STN EN 54-20 Elektrická požiarna signalizácia. Časť 20: Nasávacie dymové hlásiče.

STN EN 54-20/Oprava AC Elektrická požiarna signalizácia. Časť 20: Nasávacie dymové hlásiče.

STN EN 54-21 Elektrická požiarna signalizácia. Časť 21: Zariadenia na prenos signalizácie požiaru a signalizácie porúch.

STN EN 54-22+A1 Elektrická požiarna signalizácia. Časť 22: Resetovateľné tepelné hlásiče líniového typu.

STN EN 54-23 Elektrická požiarna signalizácia. Časť 23: Zariadenia signalizácie požiaru. Vizuálne signalizačné zariadenia.

STN EN 54-24 Elektrická požiarna signalizácia. Časť 24: Súčasti systému hlasovej signalizácie požiaru – reproduktory.

STN EN 54-25 Elektrická požiarna signalizácia. Časť 25: Súčasti využívajúce rádiové spoje.

STN EN 54-26 Elektrická požiarna signalizácia. Časť 26: Hlásiče oxidu uhoľnatého. Bodové hlásiče.

STN EN 54-27 Elektrická požiarna signalizácia. Časť 27: Dymové hlásiče na kontrolu vzduchotechnických potrubí.

STN EN 54-28 Elektrická požiarna signalizácia. Časť 28: Neresetovateľné tepelné hlásiče líniového typu.

STN EN 54-29 Elektrická požiarna signalizácia. Časť 29: Viacsnímačové požiarne hlásiče. Bodové hlásiče s kombinovaným dymovým a tepelným snímačom.

STN EN 54-30 Elektrická požiarna signalizácia. Časť 30: Viacsnímačové požiarne hlásiče. Bodové hlásiče s kombinovaným snímačom oxidu uhoľnatého a tepelným snímačom.

STN EN 54-31+A1 Elektrická požiarna signalizácia. Časť 31: Viacsnímačové požiarne hlásiče. Bodové hlásiče s kombinovaným dymovým snímačom, snímačom oxidu uhoľnatého a voliteľným tepelným snímačom.

MPPC/PCO

STN EN 50518 Monitorovacie a poplachové prijímacie centrá.

STN EN 50518/Zmena A1 Monitorovacie a poplachové prijímacie centrá.

iné

STN EN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000: 2018).

STN EN ISO 14001 Systémy manažérstva environmentu. Požiadavky s pokynmi na použitie (ISO 14001: 2015).

Zákon č. 473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov.

Vyhláška 634/2005 Ministerstva vnútra Slovenskej republiky z 5. decembra 2005, ktorou sa vykonávajú niektoré ustanovenia zákona č. 473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti)

Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

ISO 18788 Management system for private security operations - Requirements with guidance for use.

STN EN 12519 (746100) Okná a dvere. Terminológia.

STN EN 15602 (950501) Poskytovatelia bezpečnostných služieb. Terminológia.

STN ISO 31000 Manažérstvo rizika. Zásady a návod.

STN ISO 31010 Manažérstvo rizika. Techniky posúdenia rizika.

STN ISO 31073 Manažérstvo rizika. Slovník.

Nezáväzné:

A Risk Assessment Methodology (RAM) for Physical Security. 2005. Sandia Corporation, White Paper.

PNJ 131 SK Poplachové systémy. Pravidlá zriaďovania elektrických zabezpečovacích systémov v objektoch (EZS) – podniková norma – obsahuje výňatok z STN EN 50131.

Ostatné informačné zdroje:

- Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky https://www.minedu.sk/
- Ministerstvo vnútra Slovenskej republiky: https://www.minv.sk/
- Policajný zbor SR https://www.minv.sk/?prehlad-zameranie-a-posobnost-sluzieb-policajneho-zboru
- Národný bezpečnostný úrad: https://www.nbu.gov.sk/index.html
- Slovenská komora súkromnej bezpečnosti: https://www.sksb.sk/)
- www.normoff.gov.sk
- www.bezpecnostvpraxi.sk