

Otázka A1

Vyjmenujte poplachové systémy, které mohou odesílat signály a zprávy do dohledového poplachového a přijímacího centra (ARC)-dříve PCO. Popište poplachový zabezpečovací a tísňový systém (I&HAS), z jakých prvků se skládá, co může detekovat a k čemu se využívá. Z vybraných pomůcek vyberte prvky I&HAS. Jaký rozdíl je mezi sběrníkovým a bezdrátovým systémem? Předvedte reakci operátora/operátorky na přijatou zprávu: slabá baterie (nízké napájecí napětí) v bezdrátovém prostorovém pohybovém detektoru v jednom ze střežených objektů

Odpověď :

Do dohledového a poplachového centra (ARC – Alarm Receiving Centre, DPPC/ dříve PCO) mohou odesílat signály a zprávy zejména tyto systémy:

- 1. PZTS (Poplachový zabezpečovací a tísňový systém) – dříve EZS**
 - vloupání, narušení objektu, tísňové volání, sabotáž systému.
- 2. EPS (Elektrická požární signalizace)**
 - požární poplach, porucha systému, výpadek napájení.
- 3. CCTV/VSS (kamerové a videosystémy)**
 - obrazové alamy, detekce pohybu, videoverifikace poplachu.
- 4. ACS/EKV (přístupové a docházkové systémy)**
 - informace o vstupech, neoprávněných průchodech, otevření dveří
- 5. SAS (systémy přivolání pomoci)**
 - tísňová tlačítka, ochrana osob, nouzová volání.
- 6. GPS a monitorovací systémy vozidel**
 - poloha vozidla, přepadení, krádež vozidla.
- 7. Technologické a provozní systémy budov**
 - výpadek elektrické energie, poruchy chlazení, vytápění, vzduchotechniky a dalších technologií.
- 8. Detekční systémy ochrany prostředí**
 - detektory úniku plynu,
 - detektory zaplavení vodou,

- detektory kouře,
- teplotní čidla.

9. Perimetrické detekční systémy

- ochrana oplocení, areálů a vnějšího pláště objektu.

Stručně

Nejčastěji jsou na ARC napojeny PZTS (EZS), EPS, kamerové systémy CCTV/VSS, přístupové systémy ACS, tísňové systémy SAS a různé technologické monitorovací systémy budov.

Tísňový systém I&HAS

I&HAS - EZS (Intruder and Hold-up Alarm System) je anglické označení pro poplachový zabezpečovací a tísňový systém (PZTS). Dříve EZS .Slouží k ochraně osob, majetku a objektů před neoprávněným vniknutím, přepadením nebo jiným bezpečnostním incidentem. Při vyhodnocení poplachové situace odesílá informaci uživateli, bezpečnostní službě nebo na dohledové a poplachové centrum (ARC).

Základní prvky systému I&HAS

1. Ústředna

- řídicí a vyhodnocovací jednotka systému,
- zpracovává informace z detektorů,
- vyhledává poplach a předává zprávy na ARC.

2. Detektory

- pohybové detektory (PIR),
- magnetické kontakty dveří a oken,
- detektory rozbití skla,
- venkovní a perimetrické detektory,
- případně detektory kouře, plynu nebo zaplavení

3. Ovládací zařízení

- klávesnice,
- čtečky karet nebo čipů,
- bezdrátové ovladače,
- mobilní aplikace.

4. Tísňová tlačítka

- slouží k vyhlášení tísňového poplachu při přeapadení nebo ohrožení osoby,
- mohou být pevná nebo přenosná.

5. Signalizační zařízení

- vnitřní a venkovní sirény,
- světelné majáky,
- akustická a optická signalizace poplachu

6. Komunikační zařízení

- GSM/GPRS komunikátor,
- LAN/IP komunikátor,
- případně telefonní linka nebo rádiový přenos,
- zajišťuje přenos zpráv na ARC.

7. Napájecí zdroje

- síťový zdroj,
 - záložní akumulátor pro provoz při výpadku elektrické energie
- Schéma funkce

Detektor → Ústředna → Komunikátor → ARC (DPPC/PCO) → Operátor / Zásahová jednotka

Při narušení objektu detektor vyšle signál do ústředny, ta jej vyhodnotí a prostřednictvím komunikátoru odešle poplachovou zprávu do ARC, kde operátor zahájí příslušná opatření.

Rozdíl mezi sběrniovým a bezdrátovým poplachovým systémem

Kritérium	Sběrniový systém	Bezdrátový systém
Přenos informací	Po kabelové sběrnici mezi ústřednou a prvky systému.	Pomocí rádiového signálu.

Instalace	Nutná kabeláž, vhodné zejména pro novostavby.	Rychlá montáž bez sekání zdí a vedení kabelů.
Spolehlivost	Velmi vysoká, méně náchylná k rušení.	Může být ovlivněna rádiovým rušením nebo překážkami.
Napájení detektorů	Zajištěno po sběrnici z ústředny.	Každý prvek má vlastní baterii.
Údržba	Minimální, není třeba měnit baterie.	Nutná pravidelná kontrola a výměna baterií.
Rozšiřování systému	Složitější, často vyžaduje nové kabely.	Jednoduché přidávání dalších prvků.
Pořizovací náklady	Vyšší náklady na instalaci kabeláže.	Nižší instalační náklady, ale vyšší náklady na baterie.
Vhodné použití	Velké objekty, firmy, průmyslové areály.	Byty, rodinné domy a hotové objekty.

Sběrníkový poplachový systém

- Všechny detektory, klávesnice a další prvky jsou propojeny datovou sběrnici (kabelem) s ústřednou.
- Ústředna komunikuje s jednotlivými zařízeními a současně je napájí.
- Výhodou je vysoká spolehlivost, rychlá komunikace a nízké nároky na údržbu.

Bezdrátový poplachový systém

- Zařízení komunikují s ústřednou rádiově.
- Detektory a ovladače jsou napájeny bateriemi.
- Výhodou je snadná a rychlá instalace bez stavebních úprav.
- Nevýhodou je nutnost pravidelně kontrolovat stav baterií a možnost rádiového rušení.

Shrnutí

Sběrníkový systém je vhodnější tam, kde lze instalovat kabeláž a je požadována maximální spolehlivost.

Bezdrátový systém je ideální pro dodatečné zabezpečení již hotových budov, kde by vedení kabelů bylo náročné nebo drahé.

Pokud je u bezdrátového prostorového pohybového detektoru signalizováno nízké napětí baterie, je nutné:

1. Identifikovat detektor, který hlásí slabou baterii (na klávesnici, v aplikaci nebo na ústředně systému).
2. Vyměnit baterii za nový typ doporučený výrobcem.
3. Po výměně zkontrolovat správnou funkci detektoru – provést test pohybu a ověřit komunikaci s ústřednou.
4. Ujistit se, že na ústředně zmizela poruchová hláška „nízké napětí“ nebo „slabá baterie“.
5. Použité baterie ekologicky zlikvidovat ve sběrném místě.

Pokud se baterie nevymění včas:

- detektor může přestat komunikovat s ústřednou,
- vznikne porucha zabezpečovacího systému,
- chráněný prostor nemusí být plně zabezpečen.

Stručná odpověď do školení:

Při signalizaci nízkého napětí je nutné co nejdříve vyměnit baterii v detektoru za nový předepsaný typ a následně otestovat správnou funkci detektoru i komunikaci s ústřednou.

Otázka A2

Vyjmenujte poplachové systémy, které mohou odesílat signály a zprávy do dohledového poplachového a přijímacího centra (ARC). Popište elektrickou požární signalizaci (FADS), k čemu slouží, z jakých prvků se skládá, co může detekovat. Z vybraných pomůcek vyberte prvky FADS. Vyjmenujte následná zařízení, která lze aktivací tísňového prostředku FADS

spustit, jsou-li v objektu instalována. Předved'te řešení zaznamenaného signálu předpožár hlásiče plamene

Odpověď :

Do dohledového a poplachového centra (ARC – Alarm Receiving Centre, DPPC/PCO) mohou odesílat signály a zprávy zejména tyto systémy:

10. PZTS (Poplachový zabezpečovací a tísňový systém) – dříve EZS

- vloupání, narušení objektu, tísňové volání, sabotáž systému.

11. EPS (Elektrická požární signalizace)

- požární poplach, porucha systému, výpadek napájení.

12. CCTV/VSS (kamerové a videosystémy)

- obrazové alarmy, detekce pohybu, videoverifikace poplachu.

13. ACS/EKV (přístupové a docházkové systémy)

- informace o vstupech, neoprávněných průchodech, otevření dveří

14. SAS (systémy přivolání pomoci)

- tísňová tlačítka, ochrana osob, nouzová volání.

15. GPS a monitorovací systémy vozidel

- poloha vozidla, přepadení, krádež vozidla.

16. Technologické a provozní systémy budov

- výpadek elektrické energie, poruchy chlazení, vytápění, vzduchotechniky a dalších technologií.

17. Detekční systémy ochrany prostředí

- detektory úniku plynu,
- detektory zaplavení vodou,
- detektory kouře,
- teplotní čidla.

18. Perimetrické detekční systémy

- ochrana oplocení, areálů a vnějšího pláště objektu.

Stručně

Nejčastěji jsou na ARC napojeny PZTS (EZS), EPS, kamerové systémy CCTV/VSS, přístupové systémy ACS, tísňové systémy SAS a různé technologické monitorovací systémy budov.

Elektrická požární signalizace (EPS, FADS/FDS)

Elektrická požární signalizace (EPS), někdy označovaná jako FADS (Fire Alarm Detection System), slouží k včasné detekci požáru, jeho lokalizaci a vyhlášení poplachu. Jejím hlavním úkolem je chránit osoby, majetek a umožnit rychlý zásah hasičů.

Požární systém automaticky sleduje chráněné prostory a při zjištění požáru vyšle poplach, případně předá informaci na hasičský záchranný sbor nebo dohledové centrum.

Základní prvky EPS (FADS)

1. Požární ústředna

- řídicí a vyhodnocovací jednotka systému,
- přijímá informace od detektorů,
- vyhlašuje poplach a ovládá navazující zařízení.

2. Automatické hlásiče požáru

- kouřové (optické, ionizační),
- tepelné,
- plamenné,
- kombinované hlásiče.

3. Tlačítkové hlásiče požáru

- umožňují osobě ručně vyhlásit požární poplach,
- umísťují se na únikových cestách a u východů.

4. Akustická a optická signalizace

- sirény,
- majáky,
- informují osoby v objektu o požáru.

5. Přenosové zařízení

- odesílá zprávy na HZS nebo ARC,

- zajišťuje vzdálené hlášení požáru.

6. Napájecí zdroj a záložní baterie

- zajišťují funkci systému i při výpadku elektrické energie.

7. Ovládaná požárně bezpečnostní zařízení

- evakuační rozhlas,
- odvod kouře a tepla,
- požární dveře a klapky,
- vypnutí vzduchotechniky nebo technologických zařízení.

Stručná školní odpověď

Elektrická požární signalizace (EPS, FADS) slouží k včasnému zjištění požáru, vyhlášení poplachu a předání informace odpovědným osobám nebo hasičům. Skládá se z požární ústředny, automatických a tlačítkových hlásičů požáru, sirén a majáků, přenosového zařízení a napájecího zdroje se záložní baterií.

Pokud je z hlásiče plamene přijata informace „předpožár“,

znamená to, že detektor zaznamenal příznaky možného vzniku požáru, ale ještě nebyl vyhlášen plný požární poplach.

Postup obsluhy

- 1. Potvrdit přijetí zprávy na ústředně EPS.**
- 2. Zjistit místo hlášení** podle údajů na požární ústředně.
- 3. Provéřit daný prostor** pověřenou osobou nebo ostrahou.
- 4. Zkontrolovat, zda se nejedná o skutečný vznik požáru** (plamen, kouř, vysoká teplota).
- 5. Pokud je požár potvrzen:**
 - **vyhlásit požární poplach,**

- zahájit evakuaci osob,
 - přivolat Hasičský záchranný sbor.
6. Pokud se jedná o planý nebo poruchový stav:
- odstranit příčinu,
 - uvést systém do normálního provozu,
 - provést záznam do provozní knihy EPS.

Krátká odpověď do školení

Po přijetí informace „předpožár“ z hlásiče plamene je nutné ověřit místo hlášení, zkontrolovat, zda skutečně nevzniká požár, a podle výsledku buď vyhlásit požární poplach a přivolat hasiče, nebo odstranit příčinu a obnovit normální provoz systému.

Otázka A3

Vyjmenujte poplachové systémy, které mohou odesílat signály a zprávy do dohledového poplachového a přijímacího centra (ARC). Z jakých prvků se skládá dohledový videosystém (VSS), co může detekovat a k čemu se využívá. Popište rozdíl mezi IP kamerovým systémem a CCTV. Jedna z kamer z jednoho monitorovaného systému má poruchu, ztratili jste obraz, předvedte řešení situace

Odpověď :

Do dohledového a poplachového centra (ARC – Alarm Receiving Centre, DPPC/PCO) mohou odesílat signály a zprávy zejména tyto systémy:

19. PZTS (Poplachový zabezpečovací a tísňový systém) – dříve EZS

- vloupání, narušení objektu, tísňové volání, sabotáž systému.

20. EPS (Elektrická požární signalizace)

- požární poplach, porucha systému, výpadek napájení.

21. CCTV/VSS (kamerové a videosystémy)

- obrazové alarmy, detekce pohybu, videoverifikace poplachu.

22. ACS/EKV (přístupové a docházkové systémy)

- informace o vstupech, neoprávněných průchodech, otevření dveří

23. SAS (systémy přivolání pomoci)

- tísňová tlačítka, ochrana osob, nouzová volání.

24. GPS a monitorovací systémy vozidel

- poloha vozidla, přepadení, krádež vozidla.

25. Technologické a provozní systémy budov

- výpadek elektrické energie, poruchy chlazení, vytápění, vzduchotechniky a dalších technologií.

26. Detekční systémy ochrany prostředí

- detektory úniku plynu,
- detektory zaplavení vodou,
- detektory kouře,
- teplotní čidla.

27. Perimetrické detekční systémy

- ochrana oplocení, areálů a vnějšího pláště objektu.

Stručně

Nejčastěji jsou na ARC napojeny PZTS (EZS), EPS, kamerové systémy CCTV/VSS, přístupové systémy ACS, tísňové systémy SAS a různé technologické monitorovací systémy budov.

Dohledový videosystém (VSS)

VSS (Video Surveillance System) je kamerový systém určený k nepřetržitému sledování, záznamu a vyhodnocování dění v chráněném prostoru. Používá se k ochraně osob, majetku a objektů a může být napojen na dohledové a poplachové centrum (ARC).

Základní prvky VSS

1. Kamery

- pevné,
- otočné (PTZ),

- vnitřní a venkovní,
- denní/noční kamery

2. Záznamové zařízení (DVR/NVR)

- ukládá obrazový záznam,
- umožňuje zpětné přehrávání.

3. Monitor

- zobrazuje obraz z kamer v reálném čase

4. Přenosová síť

- kabelová nebo bezdrátová komunikace,
- přenos obrazu mezi kamerami a záznamovým zařízením.

5. Napájecí zdroje

- napájení kamer a ostatních zařízení.

6. Software pro správu videa

- umožňuje sledování, vyhledávání a vyhodnocování záznamů. **Co může VSS detekovat**

- pohyb osob nebo vozidel,
- vstup do zakázaného prostoru,
- překročení virtuální čáry,
- opuštěný nebo odcizený předmět,
- podezřelé chování osob,
- registrační značky vozidel (LPR),
- rozpoznání obličeje (u vybraných systémů)

K čemu se využívá

- ochrana objektů proti vloupání,
- dohled nad vstupy a parkovišti,
- kontrola výrobních a skladových prostor,
- monitoring veřejných prostranství,
- ověření poplachů z PZTS nebo EPS,

- identifikace pachatelů a dokumentace událostí.

Stručná školní odpověď do školení

Dohledový videosystém (VSS) slouží ke sledování a záznamu dění v chráněném prostoru. Skládá se z kamer, záznamového zařízení, monitoru, přenosové sítě, napájecích zdrojů a řídicího softwaru. Dokáže detekovat pohyb osob a vozidel, narušení střeženého prostoru a další bezpečnostní události. Využívá se k ochraně osob, majetku a k ověřování poplachů.

Rozdíl mezi IP kamerovým systémem a CCTV

Vlastnost	CCTV	IP kamerový systém
Přenos obrazu	Analogový signál po koaxiálním kabelu.	Digitální data po počítačové síti (LAN/Internet).
Kamery	Analogové kamery.	IP kamery s vlastní síťovou adresou.
Záznam	DVR (Digital Video Recorder).	NVR (Network Video Recorder) nebo server.
Kvalita obrazu	Obvykle nižší rozlišení.	Vysoké rozlišení (HD, Full HD, 4K i více).
Přístup na dálku	Omezený.	Jednoduchý vzdálený přístup přes síť nebo internet.
Inteligentní analýza obrazu	Omezené možnosti.	Pokročilé funkce – detekce pohybu, rozpoznání obličeje, čtení SPZ apod.
Instalace	Jednodušší u menších systémů.	Vhodná pro rozsáhlé moderní systémy.

CCTV (Closed-Circuit Television)

- Tradiční kamerový systém.

- Obraz z kamer je přenášén analogově po koaxiálním kabelu do záznamového zařízení DVR.
- Používá se především pro základní dohled a záznam obrazu **IP kamerový systém**
- Moderní digitální kamerový systém.
- Každá kamera je samostatné síťové zařízení s vlastní IP adresou.
- Obraz je přenášén po datové síti do NVR nebo na server.
- Umožňuje vzdálené sledování přes počítač nebo mobilní telefon a pokročilou analýzu obrazu.

Stručná odpověď do školení

CCTV je klasický analogový kamerový systém, který přenáší obraz po koaxiálním kabelu do DVR. IP kamerový systém je digitální, využívá počítačovou síť, nabízí vyšší kvalitu obrazu, vzdálený přístup a pokročilé funkce analýzy videa.

Otázka A4

Vyjmenujte poplachové systémy, které mohou odesílat signály a zprávy do dohledového poplachového a přijímacího centra (ARC). Popište systém kontroly vstupu (ACS). Z jakých prvků se skládá, co může detekovat a k čemu se využívá. Co je největší slabina ACS? Předvedte reakci operátora/operátorky při násilně otevřeném elektromagnetickém zámku střeženého objektu

Odpověď:

Do dohledového a poplachového centra (ARC – Alarm Receiving Centre, DPPC/PCO) mohou odesílat signály a zprávy zejména tyto systémy:

- 28. PZTS (Poplachový zabezpečovací a tísňový systém) – dříve EZS**
 - vloupání, narušení objektu, tísňové volání, sabotáž systému.
- 29. EPS (Elektrická požární signalizace)**
 - požární poplach, porucha systému, výpadek napájení.

30. CCTV/VSS (kamerové a videosystémy)

- obrazové alarmy, detekce pohybu, videoverifikace poplachu.

31. ACS/EKV (přístupové a docházkové systémy)

- informace o vstupech, neoprávněných průchodech, otevření dveří

32. SAS (systémy přivolání pomoci)

- tísňová tlačítka, ochrana osob, nouzová volání.

33. GPS a monitorovací systémy vozidel

- poloha vozidla, přepadení, krádež vozidla.

34. Technologické a provozní systémy budov

- výpadek elektrické energie, poruchy chlazení, vytápění, vzduchotechniky a dalších technologií.

35. Detekční systémy ochrany prostředí

- detektory úniku plynu,
- detektory zaplavení vodou,
- detektory kouře,
- teplotní čidla.

36. Perimetrické detekční systémy

- ochrana oplocení, areálů a vnějšího pláště objektu.

Stručně

Nejčastěji jsou na ARC napojeny PZTS (EZS), EPS, kamerové systémy CCTV/VSS, přístupové systémy ACS, tísňové systémy SAS a různé technologické monitorovací systémy budov.

System kontrolы vstupu ACS

ACS (Access Control System) je elektronický systém kontroly vstupu, který slouží k řízení a evidenci vstupu osob do budov, místností nebo chráněných prostor. Umožňuje vstup pouze oprávněným osobám a zaznamenává údaje o jejich pohybu.

Základní prvky systému ACS

1. Identifikační médium

- přístupová karta,
- čip (RFID),
- přívěsek,
- mobilní telefon,
- biometrický údaj (otisk prstu, obličej).

2. Čtečka

- snímá kartu, čip nebo biometrické údaje,
- předává informace řídicí jednotce.

3. Řídicí jednotka

- vyhodnocuje oprávnění ke vstupu,
- rozhoduje o otevření nebo zamítnutí vstupu

4. Elektrický zámek nebo turniket

- fyzicky umožňuje nebo blokuje průchod osob

5. Software a databáze

- správa uživatelů a oprávnění,
- evidence všech vstupů a výstupů.

6. Napájecí zdroj a záložní baterie

- zajišťují provoz systému i při výpadku napájení.

Co systém ACS detekuje

- přiložení platné nebo neplatné karty,
- pokus o neoprávněný vstup,
- otevření nebo násilné otevření dveří,
- ponechání dveří otevřených,
- průchod osoby do chráněného prostoru,
- čas a místo vstupu uživatele.

K čemu se používá

- ochrana budov a objektů,

- řízení přístupu zaměstnanců,
- zabezpečení serveroven, skladů a technologických místností,
- evidence docházky,
- zvýšení bezpečnosti osob a majetku,
- spolupráce s kamerovými systémy a PZTS
-

Stručná školní odpověď

ACS (Access Control System) je systém kontroly vstupu, který umožňuje vstup pouze oprávněným osobám. Skládá se z identifikačního média (karta, čip), čtečky, řídicí jednotky, elektrického zámku, softwaru a napájení. Detekuje vstupy a pokusy o neoprávněný vstup a používá se k ochraně budov, osob a majetku.

Při zjištění násilného otevření elektromagnetického zámku systému ACS musí operátor postupovat podle bezpečnostních směrnic objektu.

Doporučený postup operátora

- 1. Přijmout a vyhodnotit poplachovou zprávu**
 - ověřit, o které dveře nebo vstup se jedná,
 - zjistit čas a typ události.
- 2. Provéřit situaci**
 - zkontrolovat kamerový systém (VSS/CCTV), pokud je k dispozici,
 - ověřit, zda se nejedná o oprávněný zásah nebo poruchu zařízení.
- 3. Kontaktovat odpovědnou osobu**
 - správce objektu,
 - bezpečnostní službu nebo ostrahu.
- 4. Vyslat zásahovou jednotku**
 - pokud nelze poplach vyhodnotit jako planý,

- provést fyzickou kontrolu objektu

5. Při potvrzeném narušení

- informovat Policii ČR,
- zabezpečit důkazy (záznamy kamer, údaje systému ACS).

6. Zapsat událost

- vytvořit záznam o průběhu události,
- uvést přijatá opatření a výsledky kontroly.

Stručná školní odpověď

Operátor musí vyhodnotit poplach, ověřit situaci pomocí kamerového systému, kontaktovat odpovědné osoby a podle potřeby vyslat zásahovou jednotku. Je-li potvrzeno násilné vniknutí, informuje Policii ČR a provede záznam o události.

Otázka A5

Vyjmenujte a popište úrovně ochrany střeženého objektu. K jednotlivým úrovním přiřadte poplachové systémy, které jsou pro příslušnou ochranu určeny. Popište, které prvky I&HAS se používají pro jednotlivé úrovně ochrany. Vybrané pomůcky přiřadte k jednotlivým typům ochran. Do které úrovně ochrany patří parkovací systém s automatickým rozpoznáním registračních značek vozidel (ANPR).

Odpověď:

Úrovně ochrany střeženého objektu

Ochrana objektu se obvykle rozděluje do několika vrstev (úrovní), které na sebe navazují. Cílem je odhalit narušitele co nejdříve a zabránit škodám.

1. Perimetrická ochrana (ochrana vnější hranice objektu)

Účel: Zachytit narušitele ještě před vstupem do objektu.

Používané systémy:

- Perimetrické detektory
- Infrazávory
- Mikrovlnné bariéry
- Ochrana oplocení
- Venkovní kamery VSS/CCTV

Příklad: Ochrana plotu průmyslového areálu.

2. Plášťová ochrana (ochrana obvodového pláště budovy)

Účel: Zjistit pokus o vniknutí přes dveře, okna nebo jiné otvory.

Používané systémy:

- PZTS / I&HAS
- Magnetické kontakty dveří a oken
- Detektory rozbití skla
- Otřesové a vibrační detektory
- Kamerový systém VSS

Příklad: Ochrana vstupních dveří a oken administrativní budovy.

3. Prostorová ochrana (dohledová ochrana)

Účel: Odhalit pohyb narušitele uvnitř objektu.

Používané systémy:

- Pohybové detektory PIR
- Duální detektory PIR/MW
- Stropní detektory
- Vnitřní VSS/CCTV
- PZTS / I&HAS

Příklad: Ochrana kanceláří, skladů a chodeb.

4. Předmětová ochrana

Účel: Chránit konkrétní cenné předměty.

Používané systémy:

- Trezorové kontakty
- Vibrační a otřesové detektory
- Detektory sejmutí předmětu
- Kamerové systémy VSS

Příklad: Ochrana trezoru, bankomatu nebo uměleckého díla.

5. Režimová ochrana (kontrola pohybu osob)

Účel: Zajistit vstup pouze oprávněným osobám.

Používané systémy:

- ACS (Access Control System)
- Čtečky karet a čipů
- Biometrické systémy
- Turnikety
- Docházkové systémy

Příklad: Vstup zaměstnanců do serverovny nebo výrobní haly.

6. Požární ochrana

Účel: Včasná detekce požáru a ochrana osob.

Používané systémy:

- EPS (Elektrická požární signalizace)
- Kouřové hlásiče
- Tepelné hlásiče
- Hlásiče plamene
- Tlačítkové hlásiče požáru

Příklad: Ochrana obchodních center, škol a výrobních provozů.

Přehled

Úroveň ochrany	Hlavní určení	Používané systémy
Perimetrická	Ochrana hranice pozemku	Perimetrické systémy, CCTV
Plášťová	Ochrana dveří a oken	PZTS, magnetické kontakty, detektory tříštění skla
Prostorová	Ochrana vnitřních prostor	PIR detektory, PZTS, CCTV
Předmětová	Ochrana cenností	Vibrační detektory, trezorové kontakty
Režimová	Kontrola vstupu osob	ACS, biometrie, turnikety
Požární	Detekce požáru	EPS, hlásiče kouře, tepla a plamene

Krátká odpověď do školy

Ochrana střeženého objektu se dělí na perimetrickou, plášťovou, prostorovou, předmětovou, režimovou a požární ochranu. K jejich realizaci se používají zejména systémy PZTS EZS(I&HAS), EPS (FADS), VSS/CCTV, ACS a perimetrické detekční systémy.

Parkovací systém s automatickým rozpoznáváním registračních značek (LPR/ANPR) patří především do:

1. Režimové ochrany

Protože slouží ke **kontrolě a řízení vjezdu vozidel** do střeženého prostoru. Systém ověřuje, zda má vozidlo oprávnění ke vjezdu, a podle výsledku otevře nebo neotevře závoru. Funkčně je podobný systému ACS pro osoby.

2. Prostorové (dohledová) ochrany VSS/CCTV

Současně je součástí **kamerového systému**, protože využívá kamery a software pro analýzu obrazu. Dokáže rozpoznávat registrační značky, evidovat průjezdy vozidel a ukládat obrazový záznam.

Odpověď do školy

Parkovací systém s automatickým rozpoznáváním registračních značek patří především do režimové ochrany a prostorové (dohledové) ochrany, protože kontroluje a řídí vstup (vjezd) oprávněných vozidel do objektu. Zároveň využívá prvky dohledového videosystému (VSS/CCTV), který zajišťuje snímání a identifikaci registračních značek.

Co je systém VSS?

VSS (Video Surveillance System)

je **dohledový videosystém**, tedy soustava kamer a dalších zařízení určených ke sledování, záznamu a vyhodnocování dění ve střeženém prostoru. Používá se k ochraně osob, majetku a objektů. Může pracovat samostatně nebo být propojen s dalšími bezpečnostními systémy, například PZTS (I&HAS), ACS nebo ARC.

Z čeho se skládá VSS

- kamery (pevné, otočné PTZ, vnitřní i venkovní),
- záznamové zařízení (DVR nebo NVR),
- monitory pro sledování obrazu,
- přenosová síť (kabelová nebo bezdrátová),
- software pro správu a vyhodnocování videa,
- napájecí zdroje.

Co dokáže VSS detekovat

- pohyb osob a vozidel,
- vstup do zakázaného prostoru,
- překročení virtuální čáry,
- opuštěné předměty,

- registrační značky vozidel (LPR/ANPR),
- podezřelé události a narušení objektu

K čemu se používá

- ochrana budov a areálů,
- dohled nad vstupy a parkovišti,
- ověřování poplachů z PZTS,
- identifikace pachatelů,
- evidence a zpětné vyhodnocení událostí,
- řízení vjezdu vozidel pomocí rozpoznávání registračních značek. **Krátká školní odpověď**

VSS (Video Surveillance System) je dohledový kamerový systém určený ke sledování a záznamu dění ve střeženém prostoru. Skládá se z kamer, **záznamového zařízení, monitorů, přenosové sítě a řídicího softwaru. Používá se k ochraně osob a majetku a k detekci bezpečnostních událostí.**

Otázka A6

Vysvětlete stupně zabezpečení objektu, třídy prostředí a homologaci poplachových systémů. Pro které stupně zabezpečení musí být použity dvě nezávislé přenosové trasy pro přenos informací do ARC. Ze kterého poplachového systému musí být signály přenášeny do ARC vždy dvěma nezávislými přenosovými trasami?

Odpověď :

1. Stupně zabezpečení objektu (bezpečnostní třídy)

Podle norem pro PZTS/I&HAS se rozlišují 4 stupně zabezpečení (Grade 1–4) podle úrovně rizika.

Stupeň 1 – Nízké riziko

- Předpokládá se náhodný pachatel s minimálními znalostmi.
- Ochrana bytů, malých skladů, zahradních objektů.

Stupeň 2 – Nízké až střední riziko

- Pachatel může mít základní znalosti zabezpečovací techniky.

- Rodinné domy, kanceláře, menší provozovny.

Stupeň 3 – Střední až vysoké riziko

- Pachatel disponuje znalostmi zabezpečovacích systémů a speciálním nářadím.
- Banky, zlatnictví, významné komerční objekty

Stupeň 4 – Vysoké riziko

- Pachatel je velmi zkušený a vybavený profesionální technikou.
 - Vojenské objekty, strategické provozy, trezory, státní instituce.
-

2. Třídy prostředí

Třída prostředí určuje, v jakých klimatických podmínkách může bezpečnostní zařízení pracovat.

Třída I – Vnitřní prostředí

- Vytápěné místnosti.
- Stabilní teplota a vlhkost.

Třída II – Všeobecné vnitřní prostředí

- Nevytápěné objekty.
- Mírné kolísání teplot.

Třída III – Venkovní chráněné prostředí

- Přístřešky, kryté venkovní prostory.
- Větší změny teplot a vlhkosti.

Třída IV – Venkovní prostředí

- Přímé působení povětrnostních vlivů.
 - Déšť, sníh, vítr, mráz, sluneční záření.
-

3. Homologace poplachových systémů

Homologace znamená, že zařízení bylo:

- odzkoušeno akreditovanou zkušebnou,
- splňuje požadavky příslušných norem,

- získalo certifikát o shodě,
- může být použito v bezpečnostních systémech daného stupně zabezpečení.

Homologace zaručuje, že detektory, ústředny, komunikátory a další prvky splňují požadavky na spolehlivost, odolnost a bezpečnost.

4. Dvě nezávislé přenosové trasy do ARC

Pro vyšší stupně zabezpečení je požadován zálohovaný přenos informací do ARC.

Povinné dvě nezávislé přenosové cesty:

- Stupeň 3
- Stupeň 4

Tedy střední až vysoké riziko napadení objektu

Typicky:

- hlavní trasa: LAN/IP,
- záložní trasa: GSM/GPRS nebo rádiová síť.

Při výpadku jedné přenosové cesty musí být poplachová zpráva automaticky přenesena druhou nezávislou trasou.

Stručná odpověď do školení

Stupně zabezpečení objektu jsou **1 až 4 podle míry rizika**. Třídy prostředí I–IV **určují podmínky, ve kterých může zařízení pracovat**. Homologace je certifikace potvrzující splnění požadavků příslušných norem. Dvě nezávislé přenosové trasy do ARC musí být použity u systémů stupně zabezpečení **3 a 4**

Signály musí být vždy přenášeny dvěma nezávislými přenosovými trasami zejména u poplachových zabezpečovacích a tísňových systémů (PZTS **EPS/ I&HAS-EZS**) ve stupni zabezpečení 3 a 4 (**střední až vysoké riziko napadení objektu**), které jsou připojeny na ARC (Alarm Receiving Centre).

Proč dvě přenosové trasy?

Důvodem je zajištění spolehlivého přenosu poplachové informace i při poruše nebo sabotáži jedné cesty.

ARC (Alarm Receiving Centre) **PCO**

ARC – Alarm Receiving Centre je dohledové a poplachové přijímací centrum (DPPC, **dříve PCO – pult centralizované ochrany**). Je to pracoviště s nepřetržitou obsluhou, které přijímá, vyhodnocuje a zpracovává poplachové, poruchové a informační zprávy z bezpečnostních systémů objektů.

Jaké signály ARC přijímá?

- z PZTS (poplachové zabezpečovací a tísňové systémy),
- z EPS (elektrická požární signalizace)
- z VSS/CCTV (kamerové systémy)
- z ACS (systémy kontroly vstupu)
- z technologických a monitorovacích systémů budov.

Co dělá operátor ARC?

1. Přijme poplachovou zprávu.
2. Vyhodnotí situaci (často pomocí kamer).
3. Kontaktuje odpovědné osoby.
4. V případě potřeby vyšle zásahovou jednotku nebo informuje Policii ČR či HZS.

Krátká odpověď do školy

ARC (Alarm Receiving Centre) je dohledové a poplachové přijímací centrum, které nepřetržitě přijímá a vyhodnocuje zprávy z bezpečnostních systémů (PZTS, EPS, VSS, ACS) a zajišťuje odpovídající reakci na poplachové události.

Otázka A7

Jaké poplachové přenosové trasy se používají pro přenos signálů a informací z poplachového systému, resp. poplachového přenosového zařízení do dohledového poplachového a přijímacího centra. Vyjmenujte a popište poplachová přenosová zařízení

pro I&HAS a FADS. Jaký rozdíl je mezi ztrátou komunikace dohledového centra s poplachovým přenosovým zařízením a ztrátou komunikace s ústřednou poplachového systému? Předved'te úkony při zaznamenané 24hodinové ztrátě komunikace ARC s monitorovaným I&HAS, poplachovým přenosovým zařízením je GSM komunikátor

Odpověď :

Při přenosu poplachových signálů z elektrického zabezpečovacího systému (EZS), elektrické požární signalizace (EPS) nebo jiného poplachového systému do dohledového centra (PCO – pult centrální ochrany, poplachové přijímací centrum) se používají různé poplachové přenosové trasy. Norma ČSN EN 50136 se vztahuje na přenos poplachových, poruchových i stavových zpráv mezi střeženým objektem a přijímacím centrem

Nejčastější přenosové trasy

1. Pevná telefonní síť (PSTN)
 - klasická telefonní linka,
 - dnes se používá již méně často.
2. Mobilní síť GSM/GPRS/3G/4G/5G
 - přenos dat prostřednictvím mobilního operátora,
 - velmi rozšířené řešení,
 - umožňuje přenos poplachu, poruch i technických informací.
3. Internetové připojení (IP přenos)
 - přenos po datové síti LAN nebo internetu,
 - rychlý a levný způsob komunikace.
4. Rádiové sítě
 - vlastní rádiové sítě provozovatele PCO,
 - využívají se zejména tam, kde není spolehlivé internetové nebo telefonní spojení.
5. Optické sítě
 - přenos po optických kabelech,

- vysoká rychlost a odolnost proti rušení.

6. Kombinované (duální) přenosové trasy

- např. IP + GSM/GPRS,
- jedna cesta je hlavní a druhá záložní,
- při výpadku jedné trasy systém automaticky přepne na druhou.
- používá se u objektů s vyššími bezpečnostními požadavky.

Požadavky na přenosové trasy

Přenosová trasa musí zajistit:

- spolehlivý přenos poplachové zprávy,
- dostatečnou dostupnost spojení,
- ochranu proti sabotáži,
- dohled nad funkčností komunikace,
- přenos poruchových a stavových hlášení.

Stručně pro školení:

V současné praxi se nejčastěji používá IP přenos po internetu doplněný o záložní GSM/GPRS/LTE trasu, případně samostatný GSM přenos nebo rádiová síť PCO.

U systémů I&HAS (Intruder and Hold-up Alarm Systems – **EZS** poplachové zabezpečovací a tísňové systémy) a FADS (Fire Alarm Detection Systems – **EPS** systémy požární detekce a signalizace) se používají tato poplachová přenosová zařízení (ATD – Alarm Transmission Device):

1. Telefonní přenosové zařízení

- Přenáší poplachové zprávy prostřednictvím veřejné telefonní sítě (PSTN).
- Dříve nejrozšířenější způsob přenosu.
- Dnes se používá spíše jako doplňková nebo záložní cesta. 2. GSM/GPRS/LTE komunikátor
- Přenos signálů prostřednictvím mobilní sítě.
- Umožňuje přenos poplachových, poruchových i stavových zpráv.

- Často slouží jako hlavní nebo záložní komunikace3. IP komunikátor
- Přenos po počítačové síti LAN nebo internetu.
- Vyznačuje se vysokou rychlostí a nízkými provozními náklady.
- Patří k nejpoužívanějším moderním řešením.

4. Rádiové přenosové zařízení

- Přenáší informace prostřednictvím rádiové sítě provozované bezpečnostní službou nebo PCO.
- Nezávisí na veřejných telekomunikačních sítích.
- Vhodné pro objekty s vysokými požadavky na bezpečnost.

5. Optické přenosové zařízení

- Využívá optické kabely.
- Poskytuje vysokou rychlost přenosu a odolnost proti rušení.
- Používá se zejména u rozsáhlých nebo kritických objektů.

6. Duální (kombinované) přenosové zařízení

- Kombinuje dvě nezávislé přenosové cesty, například:
 - IP + GSM,
 - optika + GSM,
 - rádiová síť + GSM.
- Zajišťuje vysokou spolehlivost při výpadku jedné přenosové trasy.

Funkce poplachových přenosových zařízení

Poplachová přenosová zařízení zajišťují:

- přenos poplachových zpráv,
- přenos poruchových hlášení,
- přenos stavových informací,
- dohled nad funkčností spojení,
- signalizaci sabotáže nebo přerušení komunikace.

Shrnutí pro školení :

Nejčastěji používanými zařízeními pro I&HAS (EZS) a FADS (EPS) jsou dnes IP komunikátory, GSM/LTE komunikátory a jejich duální kombinace, které přenášejí informace do poplachového přijímacího centra (ARC/PCO).

Rozdíl spočívá v místě, kde došlo k přerušení komunikace:

1. Ztráta komunikace dohledového centra (PCO) s poplachovým přenosovým zařízením (ATD)

- Dohledové centrum (PCO/ARC) již nekomunikuje s přenosovým zařízením umístěným v objektu.
- **Příčinou může být výpadek internetu, GSM sítě, telefonní linky, rádiové sítě nebo porucha samotného komunikátoru.**
- Dohledové centrum neví, zda je poplachový systém stále funkční, protože ztratilo spojení s jeho komunikačním rozhraním.
- Obvykle je vyhlášena porucha přenosové cesty. **Příklad: Ústředna EZS pracuje správně, ale nefunguje GSM komunikátor. Poplach by vznikl, ale nedostal by se do PCO.**

2. Ztráta komunikace mezi poplachovým přenosovým zařízením a ústřednou poplachového systému

- Komunikátor je stále připojen k dohledovému centru a „hlásí se“, ale nedokáže komunikovat s ústřednou EZS/EPS.
- **Příčinou může být poškozený datový kabel, porucha sběrnice, odpojení komunikátoru nebo porucha ústředny.**
- Dohledové centrum vidí, že komunikátor je aktivní, ale dostává informaci o poruše spojení s ústřednou.
- **Poplachové události vzniklé v ústředně nemohou být předány komunikátoru.**

Příklad: IP komunikátor je připojen k internetu a komunikuje s PCO, ale je přerušen kabel mezi komunikátorem a ústřednou. PCO vidí komunikátor online, ale neobdrží informace o poplachu.

Stručné shrnutí

Stav	Co je mimo provoz?	Vidí dohledové centrum zařízení?
Ztráta komunikace PCO ↔ ATD	Přenosová cesta nebo komunikátor	Ne
Ztráta komunikace ATD ↔ ústředna	Spojení komunikátoru s ústřednou	Ano, ale hlásí poruchu

Jednoduše řečeno: v prvním případě dohledové centrum „nevidí“ komunikátor, ve druhém komunikátor „nevidí“ ústřednu.

Pokud dojde ke 24hodinové ztrátě komunikace mezi PCO (poplachovým přijímacím centrem) a ústřednou poplachového systému, jedná se o závažnou poruchu přenosu, kterou je nutné neprodleně řešit.

Doporučený postup

1. Ověřit příčinu poruchy

- zkontrolovat napájení ústředny,
- ověřit funkčnost komunikátoru (IP, GSM, rádiového),
- prověřit stav internetového, telefonního nebo GSM připojení.

2. Kontaktovat servisní organizaci

- nahlásit poruchu odpovědné servisní firmě,
- zajistit co nejrychlejší diagnostiku a opravu.

3. Provést místní kontrolu systému

- ověřit, zda je ústředna funkční,
- zkontrolovat, zda nejsou hlášeny další poruchy nebo sabotážní stavy.

4. Zajistit náhradní opatření

- zvýšit fyzickou ostrahu objektu,
- provádět častější kontroly objektu,
- případně využít záložní přenosovou trasu (např. GSM místo IP).

5. Po obnovení spojení

- provést zkoušku přenosu poplachových signálů,
- ověřit správný příjem zpráv na PCO,
- zaznamenat poruchu a její odstranění do provozní dokumentace.

Zkoušková odpověď

Při 24hodinové ztrátě komunikace s PCO je nutné zjistit příčinu poruchy, zkontrolovat ústřednu, komunikátor a přenosovou trasu, informovat servisní organizaci a zajistit náhradní bezpečnostní opatření. Po odstranění závady se provede test přenosu a ověří se správná komunikace s dohledovým centrem.

Otázka A8

Z čeho se skládá dohledové poplachové a přijímací centrum (ARC), k čemu slouží, v jakém režimu pracuje. Jaký je rozdíl mezi ARC a velínem s grafickými nadstavbami jednotlivých poplachových systémů? Jaký je rozdíl mezi ARC a monitorovacími a vizuálními systémy pro správu budov?

Odpověď

Dohledové poplachové a přijímací centrum ARC (PCO)

ARC (Alarm Receiving Centre) neboli PCO (Pult centralizované ochrany) je pracoviště, které přijímá, vyhodnocuje a zpracovává poplachové, poruchové a stavové informace ze střežených objektů. Je určeno pro nepřetržitý dohled nad zabezpečovacími a požárními systémy.

Z čeho se skládá ARC (PCO)

1. Poplachové přijímací zařízení

- přijímá zprávy z komunikátorů a ústředn,

- dekóduje a zpracovává přijaté signály.
2. Počítačový systém s monitorovacím softwarem
- zobrazuje události operátorům,
 - vede databázi objektů,
 - archivuje všechny události.
3. Pracoviště operátora
- monitory, ovládací prvky, komunikační prostředky,
 - umožňuje vyhodnocení a řešení poplachových stavů.
4. Komunikační prostředky
- telefonní linky,
 - internetové připojení,
 - GSM/LTE sítě,
 - rádiové sítě.
5. Záložní napájení
- UPS a záložní zdroje,
 - zajišťují provoz při výpadku elektrické energie.
6. Záznamová a archivační zařízení
- ukládají historii poplachů, poruch a zásahů.
-

K čemu slouží

ARC (PCO) slouží k:

- přijímání poplachových signálů z EZS/I&HAS, EPS/FADS a dalších systémů,
 - sledování poruch a ztráty komunikace,
 - vyhodnocování přijatých informací,
 - informování zásahových jednotek, hasičů, policie nebo obsluhy objektu,
 - evidenci a archivaci všech událostí.
-

V jakém režimu pracuje

ARC (PCO) pracuje v nepřetržitém režimu 24 hodin denně, 7 dní v týdnu (24/7). Operátoři neustále sledují stav připojených objektů a reagují na:

- poplach,
- tísňové volání,
- požární poplach,
- sabotáž,
- poruchu systému,
- ztrátu komunikace.

Krátká zkušková odpověď

ARC (PCO) je dohledové a přijímací centrum, které nepřetržitě přijímá a vyhodnocuje poplachové, poruchové a stavové zprávy ze střežených objektů. Skládá se z přijímacích zařízení, počítačového systému, pracovišť operátorů, komunikačních prostředků, archivačních zařízení a záložního napájení. Pracuje v režimu 24 hodin denně, 7 dní v týdnu a zajišťuje vyrozumění a koordinaci zásahu při mimořádných událostech.

Rozdíl mezi ARC (PCO) a monitorovacím systémem pro správu budov (BMS)

ARC (PCO)	Monitorovací systém správy budov (BMS)
-----------	--

Slouží především k ochraně osob a majetku.	Slouží k řízení a správě technologií budovy.
Přijímá poplachové, tísňové, požární a poruchové signály. [technickenormy.cz], [technicke-...rmy-csn.cz]	Sleduje a ovládá technická zařízení budovy (vytápění, klimatizaci, vzduchotechniku, osvětlení, výtahy apod.).
Na poplach reaguje operátor a podle stanovených postupů vysílá zásahovou jednotku, informuje policii nebo hasiče.	Obsluha řeší provozní stavy a poruchy technologií budovy.
Pracuje v režimu bezpečnostního a požárního dohledu 24/7. [technickenormy.cz], [nahledy.normy.biz]	Pracuje v režimu technického managementu budovy.
Zpracovává informace ze systémů I&HAS, FADS/EPS, CCTV, ACS apod.	Zpracovává informace z měřidel, čidel teploty, kotelen, vzduchotechniky, rozvodů energií atd.

ARC (PCO)

- **Hlavním úkolem je ochrana osob, majetku a včasná reakce na mimořádné události.**
- **Řeší:**
 - vloupání,
 - přepadení,
 - požár,
 - sabotáž,
 - ztrátu komunikace,
 - technické poruchy bezpečnostních systémů. [technickenormy.cz], [technicke-...rmy-csn.cz]

BMS (Building Management System)

- **Hlavním úkolem je efektivní provoz budovy.**
- **Řídí například:**
 - vytápění,

- chlazení,
- klimatizaci,
- osvětlení,
- spotřebu energií,
- záložní zdroje,
- technologie budovy.
-

Stručná odpověď ke zkoušce

ARC (PCO) je bezpečnostní dohledové centrum určené pro příjem a vyhodnocení poplachových, tísňových a požárních hlášení.

Monitorovací systém pro správu budov (BMS) slouží k řízení a sledování technologií budovy, jako jsou vytápění, klimatizace nebo osvětlení. ARC řeší bezpečnostní události, zatímco BMS řeší provoz a správu budovy.

Otázka A9

Co to je komunikační protokol? Jaké typy komunikačních protokolů se používají pro přenos signálů z I&HAS do ARC? Krátce popište nejpoužívanější typy komunikačních protokolů a rozdíly mezi nimi.

Odpověď :

Co je komunikační protokol?

Komunikační protokol je soubor pravidel, podle kterých si mezi sebou vyměňují informace ústředna EZS (I&HAS), poplachové přenosové zařízení a dohledové centrum ARC (PCO). Protokol určuje formát zprávy, způsob kódování událostí, potvrzování přijetí zpráv a kontrolu správnosti přenosu.

Bez komunikačního protokolu by PCO nedokázalo správně rozpoznat, zda přijatá zpráva znamená například:

- vloupání,
- požární poplach,
- tísňové volání,
- sabotáž,
- technickou poruchu,
- zapnutí nebo vypnutí střežení.

Nejčastější protokoly používané mezi EZS a PCO

1. Contact ID (CID)

- Nejrozšířenější protokol na světě.
- Vyvinut společností Ademco.
- Přenáší čtyřmístné kódy událostí.
- Umožňuje přenos velkého množství různých stavů a poplachů.

Výhody:

- vysoká kompatibilita,
- jednoduchost,
- podpora většiny ústředen a PCO.

2. SIA (Security Industry Association)

- Standardizovaný protokol organizace SIA.
- Používá se pro telefonní i IP komunikaci.
- Přenáší podrobnější informace než některé starší protokoly.

Výhody:

- standardizace,
- vysoká spolehlivost,
- široké použití v moderních systémech.

3. DC-09 (SIA DC-09)

- Moderní IP protokol vycházející ze standardu SIA.
- Určen pro přenos po internetu.
- Používá šifrování a potvrzování zpráv.

Výhody:

- vysoké zabezpečení,
- vhodný pro IP komunikaci,
- splňuje současné požadavky na bezpečnost.

4. Proprietární (výrobní) protokoly

- Vytvářejí je jednotliví výrobci zabezpečovacích systémů.
- Používají se mezi konkrétní ústřednou a přijímacím zařízením PCO.

Příklady:

- **Jablotron,**
- Paradox,
- Galaxy,
- DSC,
- Honeywell.

Přenosová média

Protokoly mohou být přenášeny:

- po telefonní síti PSTN,
- po GSM/GPRS/LTE sítích,
- po internetu (IP),
- po rádiových sítích,
- po optických sítích.

Krátká zkušková odpověď

Komunikační protokol je soubor pravidel pro výměnu informací mezi ústřednou EZS popř.EPS, přenosovým zařízením a dohledovým centrem ARC (PCO). Určuje formát zpráv a způsob jejich přenosu. Nejčastěji používané protokoly jsou Contact ID (CID), SIA, SIA DC-09

a proprietární protokoly jednotlivých výrobců. Přenos probíhá po telefonní síti, GSM, internetu nebo rádiové síti.

Otázka A10

Předved'te a vysvětlete příslušnou odezvu operátora/operátorky na základní typy přijímaných signálů a zpráv z I&HAS. Uved'te priority při jejich zpracování.

Odpověď:

Odezva operátora ARC (PCO) na základní typy signálů z I&HAS a priority jejich zpracování

Operátor ARC (PCO) musí po přijetí každého signálu postupovat podle stanovených provozních předpisů. Základním pravidlem je, že čím vyšší je riziko ohrožení života a zdraví, tím vyšší je prioritizace zpracování.

Priority zpracování signálů

- 1. Tísňový (Hold-up, Panic) poplach – nejvyšší prioritizace**
- 2. Požární poplach**
- 3. Poplach z narušení objektu (vloupání)**
- 4. Sabotážní poplach**
- 5. Technické poplachy**
- 6. Poruchová hlášení**
- 7. Stavové a informační zprávy**

1. Tísňový poplach (Panic, Hold-up Alarm)

Význam

Signalizuje bezprostřední ohrožení osoby (přepadení, loupež, násilí).

Odezva operátora

- okamžitě vyhodnotí událost,
- neprovádí zdržující ověřování u chráněné osoby,
- vysílá zásahovou jednotku,
- podle pokynů informuje Policii ČR,
- sleduje další příchozí zprávy z objektu.

Priorita

Nejvyšší

2. Požární poplach

Význam

Signalizace vzniku požáru nebo kouře.

Odezva operátora

- ověří objekt a typ hlásiče,
- informuje hasičský záchranný sbor nebo odpovědnou osobu podle provozních postupů,
- zaznamená průběh události,
- sleduje další zprávy z požárního systému.

Priorita

Velmi vysoká

3. Poplach z narušení objektu (vloupání)

Význam

Detektor zaznamenal neoprávněný vstup do střeženého prostoru.

Odezva operátora

- ověří identifikaci objektu a zóny,
- kontaktuje odpovědnou osobu dle instrukcí,

- vysílá výjezdovou skupinu,
- při potvrzení narušení informuje Policii ČR.

Priorita

Vysoká

4. Sabotážní (Tamper) poplach

Význam

Pokus o manipulaci se systémem:

- otevření krytu,
- poškození vedení,
- odpojení zařízení,
- zásah do ústředny.

Odezva operátora

- prověří charakter sabotáže,
- kontaktuje oprávněnou osobu,
- podle závažnosti vyšle zásahovou jednotku,
- provede záznam události.

Priorita

Vysoká

5. Technický poplach

Význam

Může jít například o:

- únik plynu,
- zaplavení,
- překročení teplotních limitů,
- výpadek technologie.

Odezva operátora

- informuje určenou kontaktní osobu,
- zajistí technický zásah,
- sleduje další vývoj události.

Priorita

Střední až vysoká

6. Poruchová hlášení

Význam

Například:

- výpadek napájení,
- slabý akumulátor,
- porucha komunikátoru,
- ztráta spojení.

Odezva operátora

- ověří rozsah poruchy,
- informuje servisní organizaci nebo správce,
- eviduje poruchu,
- kontroluje její odstranění.

Priorita

Střední

7. Stavové (informační) zprávy

Význam

Běžné provozní informace:

- zapnutí střežení,
- vypnutí střežení,
- testovací hlášení,
- periodická kontrola spojení.

Odezva operátora

- zprávu zaznamená systém,
- obvykle není nutný žádný zásah.

Priorita

Nízká

Stručná odpověď ke zkoušce

Operátor ARC (PCO) přijímá tísňové, požární, vloupací, sabotážní, technické, poruchové a stavové zprávy z I&HAS. Na tísňové a požární poplachy reaguje okamžitě, na vloupání a sabotáž vysílá zásah nebo informuje policii. U poruch zajišťuje servisní zásah a stavové zprávy pouze eviduje. Priority zpracování jsou: tísňový poplach, požární poplach, vloupání, sabotáž, technické poplachy, poruchy a nakonec stavové zprávy.

Uchazeč obdrží u zkoušky konkrétní příklad, např. požár v objektu.

Otázka A11

Jak a proč se provádí vyloučení náhodně vyvolaných poplachových signálů?

Odpověď:

Jak a proč se provádí vyloučení náhodně vyvolaných poplachových signálů?

Vyloučení náhodně (falešně) vyvolaných poplachů se provádí proto, aby nedocházelo ke zbytečným výjezdům zásahových jednotek, policie nebo hasičů a aby se snížily provozní náklady a zvýšila důvěryhodnost systému.

Nejčastější příčiny falešných poplachů

- chyba obsluhy při zapínání nebo vypínání systému,
- neuzavřená okna nebo dveře,
- pohyb zvířat ve střeženém prostoru,
- průvan, vibrace nebo jiné rušivé vlivy,
- porucha detektoru nebo ústředny,
- nesprávně nastavený systém.

Jak operátor postupuje

1. **Ověří identifikaci objektu a zóny**
 - zjistí, který detektor nebo část systému poplach vyvolala.
2. **Prověří historii událostí**
 - zkontroluje předchozí poplachu, poruchy a stav systému.
3. **Kontakuje odpovědnou osobu**
 - telefonicky ověří, zda se v objektu nachází oprávněná osoba,
 - ověří identitu pomocí hesla nebo bezpečnostních údajů.
4. **Využije dostupné ověřovací prostředky**
 - kamerový systém (CCTV),
 - audioverifikaci,
 - další detektory v objektu.
5. **Vyhodnotí poplach**
 - je-li potvrzeno narušení, zajistí zásah,
 - je-li prokázán omyl nebo chyba obsluhy, událost eviduje jako falešný poplach.

Metody snižování falešných poplachů

- dvoustupňové potvrzení poplachu (aktivace více detektorů),
- verifikace kamerovým systémem,
- pravidelná údržba zařízení,

- školení uživatelů systému,
- správné nastavení citlivosti detektorů.

Stručná odpověď ke zkoušce

Vyloučení náhodně vyvolaných poplachových signálů se provádí ověřením poplachu před vysláním zásahu. Operátor kontroluje zónu poplachu, historii událostí, kontaktuje odpovědnou osobu a využívá kamerovou nebo jinou verifikaci. Cílem je odlišit skutečný poplach od falešného a zabránit zbytečným výjezdům zásahových složek.

Otázka B12

Podle snímků obrazovky předved'te vhodný postup činnosti při zaznamenání tísňového poplachu (použití tísňového tlačítka). Po příjezdu na místo vyhlášení tísně výjezdová skupina zjistila osobu, která napadá „barmanku“. Třetí osoba se na situaci dívá. Situace potvrzena obrazem z dohledového videosystému (VSS). Zajistěte příslušnou pomoc

Odpověď:

Postup operátora ARC (PCO) při přijetí tísňového poplachu z tísňového tlačítka

Situace:

- **Přijat tísňový poplach (Panic/Hold-up Alarm).**
- **Kamerový systém (VSS) potvrzuje napadení barmanky agresivní osobou.**
- **Na místě je další osoba, která situaci pouze sleduje.**

Tísňový poplach představuje bezprostřední ohrožení zdraví nebo života a má nejvyšší prioritu zpracování.

Správný postup operátora

1. Přijetí a vyhodnocení poplachu

- Operátor identifikuje objekt a typ poplachu.
- Ověří, že se jedná o tísňový poplach z tísňového tlačítka.
- Okamžitě zobrazí kamery VSS.

2. Ověření situace

- Na obrazu VSS je vidět fyzické napadení barmanky.
- Událost je potvrzena obrazovou verifikací.
- Není nutné další telefonické ověřování.

3. Vyrozumění složek IZS

- Neprodleně kontaktovat linku 158 (Policie ČR).
- Oznámit:
 - adresu objektu,
 - charakter události (fyzické napadení),
 - počet zúčastněných osob,
 - aktuální vývoj situace podle kamer.

4. Vyslání výjezdové skupiny

- Vyslat nejbližší zásahovou jednotku.
- Průběžně poskytovat výjezdové skupině informace z VSS.

5. Sledování události

- Nepřetržitě sledovat kamerový systém.
- Zaznamenávat změny situace:

- útěk pachatele,
- použití zbraně,
- příchod dalších osob,
- zranění napadené osoby.

6. Poskytnutí další pomoci

Pokud je zřejmé, že:

- barmanka utrpěla zranění,
- hrozí zdravotní komplikace,

operátor současně přivolá Zdravotnickou záchrannou službu (155).

7. Dokumentace

- Zaznamenat čas přijetí poplachu.
- Evidovat všechny provedené úkony.
- Archivovat videozáznam pro potřeby Policie ČR.

Co dělat s třetí osobou?

Operátor ani výjezdová skupina nesmí předpokládat, že třetí osoba je pachatel nebo pomocník. Je nutné:

- sledovat její chování,
- předat informaci policii,
- vyčkat na zjištění její role.

Může se jednat o:

- svědka,

- zákazníka,
 - kolegu,
 - případného spolupachatele.
-

Zkoušková odpověď

Po přijetí tísňového poplachu operátor ihned ověří událost pomocí VSS. Pokud je napadení osoby potvrzeno obrazem, bez prodlení informuje Policii ČR a vysílá výjezdovou skupinu. Současně monitoruje situaci pomocí kamer a v případě zranění přivolá zdravotnickou záchrannou službu. Všechny úkony zaznamenává do systému ARC a archivuje videozáznam jako důkazní materiál-
Důležité-operátor neopouští své stanoviště ,přičemž vykonává kamerový dohled, pozoruje a vyhodnocuje situaci na místě činu !!! Dává aktuální pokyny výjezdové skupině a složkám IZS.

Otázka B 13

Podle snímků obrazovky předvedte vhodný postup činnosti při zaznamenání tísňového poplachu AMBULANCE (použití tísňového tlačítka lékař) Po příjezdu na místo vyhlášení tísně výjezdová skupina zjistila zraněnou osobu, která upadá do bezvědomí. Přivolejte příslušnou pomoc

Odpověď:

Pokud byl zaznamenán tísňový poplach AMBULANCE vyvolaný tísňovým tlačítkem „lékař“ pomocí tísňového tlačítka a výjezdová skupina po příjezdu na místo nalezne zraněnou osobu upadající do bezvědomí, vhodný postup je následující:

Postup činnosti

1. Přijetí tísňového poplachu

- **Potvrdit přijetí poplachu.**
- **Zjistit místo vyhlášení tísně.**
- **Neprodleně vyslat výjezdovou skupinu na určené místo.**

2. Příjezd na místo události

- **Zajistit vlastní bezpečnost a bezpečnost okolí.**
- **Vyhledat osobu, která vyhlásila tísňový poplach.**
- **Provést rychlé zhodnocení situace.**

3. Zjištění zraněné osoby

- **Oslovit postiženého a ověřit vědomí.**
- **Zkontrolovat dýchání a základní životní funkce.**
- **Pokud osoba upadá do bezvědomí, zahájit odpovídající první pomoc.**

4. Přivolání příslušné pomoci

- **Okamžitě kontaktovat Zdravotnickou záchrannou službu – linka 155.**
- **Případně využít jednotné evropské číslo tísňového volání 112.**
- **Operátorovi sdělit:**
 - **přesné místo události,**
 - **počet zraněných osob,**
 - **stav postiženého (upadá do bezvědomí),**
 - **své jméno a telefonní kontakt.**

5. Poskytování první pomoci

- Pokud postižený dýchá, uložit jej do stabilizované polohy a sledovat jeho stav.
- Pokud nedýchá normálně, zahájit KPR (resuscitaci-nepřímou masáž srdce postiženého) a použít AED (automatizovaný externí defibrilátor), je-li k dispozici.
- Průběžně komunikovat s operátorem ZZS podle jeho pokynů.

6. Předání postiženého

- Po příjezdu zdravotnické záchranné služby předat informace o události, zjištěném stavu a provedených úkonech.

Vzor hlášení na tísňovou linku 155

„Zde operátor dohledového centra bezpečnostní agentury B2p. Naše výjezdová skupina, která se t.č. nachází na adrese [místo události] hlásí, že zde byla nalezena zraněná osoba, která upadá do bezvědomí. Žádáme o okamžité vyslání zdravotnické záchranné služby. Na místě je jedna zraněná osoba. Kontaktní telefon na velitele výjezdové skupiny: [číslo].“

Operátor dohledového centra provede zápis o incidentu do knihy incidentů PCO.

Podle snímků obrazovky předved'te vhodný postup činnosti při zaznamenání signálu POŽÁR z hlásiče kouře. Po příjezdu na místo vyhlášení požáru výjezdová skupina zjistila zakouřenou budovu. Rozrušená žena informuje o zraněném muži na schodech do suterénu. Zajistěte příslušnou pomoc.

Odpověď:

Postup při signálu POŽÁR z hlásiče kouře(plamene,teploty)

1. Přijetí signálu POŽÁR

- **Přijmout a ověřit poplach z hlásiče kouře.**
- **Zjistit místo vzniku poplachu.**
- **Vyslat výjezdovou skupinu k prověření události.**
- **Informovat odpovědné osoby dle interních postupů.**

2. Příjezd výjezdové skupiny

- **Přiblížit se k objektu bezpečně a sledovat známky požáru.**
- **Zjistit, že budova je zakouřená.**
- **Nevstupovat do silně zakouřených prostor bez odpovídajících ochranných prostředků.**
- **Vyhodnotit situaci jako možné ohrožení života a zdraví osob.**

3. Přivolání příslušné pomoci

Okamžitě volat:

Hasičský záchranný sbor – 150 nebo Linku tísňového volání – 112

Oznámit:

- **přesnou adresu události,**
- **že je objekt zakouřený a hrozí požár,**
- **informaci o zraněné osobě v objektu,**
- **počet ohrožených osob,**

- své jméno a telefonní kontakt.

Současně podle potřeby přivolat:

Zdravotnickou záchrannou službu – 155, protože se v objektu nachází zraněný muž.

4. Informace od svědka

- Vyslechnout rozrušenou ženu.
- Získat informace o poloze zraněného muže (na schodech do suterénu).
- Zjistit, zda jsou v budově další osoby.

5. Záchrana osob

- Pokud je vstup bezpečný a nehrozí bezprostřední nebezpečí, pokusit se o vyvedení osob z objektu.
- Neohrozit vlastní život.
- Udržovat komunikaci se zraněným, pokud je při vědomí.

6. Poskytnutí první pomoci

Po dosažení zraněného:

- Zkontrolovat vědomí a dýchání.
- Zastavit případné krvácení.
- Při bezvědomí a normálním dýchání uložit do stabilizované polohy.
- Při zástavě dechu zahájit KPR (resuscitaci) a použít AED (defibrilátor), je-li k dispozici.
- Průběžně sledovat stav postiženého až do příjezdu ZZS.

7. Předání složkám IZS

Po příjezdu hasičů a zdravotníků předat:

- místo nalezení zraněného,
- jeho zdravotní stav,
- informace od svědků,
- provedené úkony první pomoci.

Vzor hlášení na linku 112 (155)

Zde operátor dohledového centra Jan Novák, „na adrese [adresa] byl zaznamenán signál POŽÁR z hlásiče kouře. Po příjezdu jsme zjistili zakouřenou budovu. Svědek uvádí, že na schodech do suterénu se nachází zraněný muž. Žádáme o okamžité vyslání hasičů a zdravotnické záchranné služby.“

Otázka B 15

Podle snímků obrazovky předved'te vhodný postup činnosti při zaznamenání signálů výpadek síťového napájení z více střežených objektů v jedné lokalitě najednou. Jakým způsobem jsou poplachové systémy zálohovány proti výpadku síťového napájení a na jak dlouho? Je ústředna bezdrátového I&HAS (EZS) ve střeženém objektu připojenému k rozvodné elektrické síti napájena síťovým napájením nebo pouze akumulátorem?

Odpověď:

Postup při zaznamenání signálů „Výpadek síťového napájení“ z více objektů v jedné lokalitě

1. Přijmout a vyhodnotit signály

- Ověřit, že se jedná o více objektů ve stejné lokalitě.
- Zkontrolovat čas vzniku událostí a porovnat je.

2. Vyhodnocení situace

- Pokud výpadek nastal současně na více objektech, je pravděpodobnou příčinou porucha distribuční elektrické sítě.
- Ověřit dostupné informace o výpadku elektrické energie v dané oblasti.

3. Informování odpovědných osob

- Informovat určené kontaktní osoby dle stanovených postupů.
- Zaznamenat událost do evidence.

4. Monitoring objektů

- Sledovat stav spojení s jednotlivými zabezpečovacími systémy.
- Reagovat na případné další poplachové nebo poruchové stavy.

5. Vyslání výjezdové skupiny

- Pouze pokud to vyžadují interní postupy nebo pokud jsou hlášeny další poruchy, ztráta komunikace či narušení objektu.

Jak jsou poplachové systémy zálohovány proti výpadku síťového napájení?

Poplachové systémy (I&HAS/EZS) jsou běžně zálohovány:

- Vestavěným akumulátorem v ústředně.
- Případně dalšími záložními zdroji (UPS) u významných objektů.

Při výpadku elektrické energie přebírá napájení automaticky akumulátor, aniž by došlo k přerušení činnosti systému.

Jak dlouho vydrží zálohování?

Doba zálohování závisí na typu systému, kapacitě akumulátoru a požadavcích norem.

Typicky:

- 12 až 24 hodin běžného provozu,
- u některých profesionálních systémů i déle,
- následně musí být systém schopen vyhlásit poplachový stav po stanovenou dobu.

Je ústředna bezdrátového I&HAS (EZS) napájena síťovým napájením nebo pouze akumulátorem?

Ve střeženém objektu připojeném k elektrické síti je ústředna:

- Primárně napájena ze síťového napájení 230 V.
- Současně obsahuje záložní akumulátor, který se automaticky používá při výpadku elektrické energie.
- Není za běžného provozu napájena pouze akumulátorem.

Akumulátor slouží jako záložní zdroj pro zajištění nepřetržité funkce systému při poruše nebo výpadku elektrické sítě.

Stručná odpověď ke zkoušce

Při současném výpadku síťového napájení ve více objektech ve stejné lokalitě vyhodnotím pravděpodobný výpadek distribuční sítě, informuji odpovědné osoby a sleduji další stavy systému.

Poplachové systémy jsou zálohovány akumulátorem v ústředně,

obvykle na dobu 12–24 hodin. Ústředna I&HAS (EZS) je za normálního stavu napájena ze sítě 230 V a akumulátor slouží jako automatická záloha při výpadku napájení.

Otázka č. B16

Předvedte a vysvětlete řízení činnosti bezpečnostního zásahu, který vede k omezení osobní svobody podezřelé osoby ze spáchání trestného činu. Osoba fyzicky napadla barmanku střeženého objektu.

Odpověď:

Postup operátora dohledového centra při řízení zásahu

Situace: Ve střeženém objektu došlo k fyzickému napadení barmanky. Podezřelá osoba je na místě a hrozí její útěk.

1. Přijetí informace

- **Přijmu oznámení o incidentu.**
- **Zjistím:**
 - **místo události,**
 - **počet zúčastněných osob,**
 - **zda je pachatel stále na místě,**
 - **zda jsou zranění,**
 - **zda nehrozí další útok.**

2. Vyslání výjezdové skupiny

- **Okamžitě vysílám nejbližší výjezdovou skupinu.**
- **Předávám všechny dostupné informace o podezřelé osobě a situaci.**

3. Přivolání Policie ČR

- Jelikož došlo k fyzickému napadení osoby a existuje podezření ze spáchání trestného činu, kontaktuji Policii ČR na lince 158.
- Sdělím místo události, popis pachatele a aktuální situaci.

4. Pokyny výjezdové skupině

- Provést bezpečný příjezd na místo.
- Oddělit pachatele od poškozené osoby.
- Zabránit dalšímu napadání osob.
- Vyhodnotit, zda existuje důvod k omezení osobní svobody.

5. Omezení osobní svobody

Pokud byla osoba přistižena při trestném činu nebo bezprostředně po něm a hrozí útěk, může být její osobní svoboda omezena do příjezdu Policie ČR. Takovou osobu je nutné bezodkladně předat policii.

- Použijí se pouze nezbytné a přiměřené prostředky.
- Nesmí dojít k nepřiměřenému násilí.
- Osoba je pod dohledem do příjezdu policie.

6. Poskytnutí pomoci poškozené

- Zjistit zdravotní stav barmanky.
- Je-li zraněna, přivolat Zdravotnickou záchrannou službu – 155.
- Poskytnout první pomoc v rozsahu svých schopností.

7. Předání Policii ČR

Po příjezdu policie:

- předat zajištěnou osobu orgánu činném v trestním řízení

- sdělit okolnosti události,
- předat identifikační údaje svědků,
- zajistit případné kamerové záznamy.

Stručná odpověď ke zkoušce

Po přijetí oznámení o fyzickém napadení barmanky vyšlu výjezdovou skupinu a přivolám Policii ČR. Výjezdová skupina zajistí bezpečnost osob, zabrání útěku podezřelého a v případě splnění zákonných podmínek omezí jeho osobní svobodu do příjezdu policie. Současně zajistí první pomoc poškozené osobě a v případě potřeby přivolá zdravotnickou záchrannou službu. Podezřelá osoba je následně předána Policii ČR.

Otázka B 17

Předvedte a vysvětlete řízení činnosti v místech, kde vzniklo podezření na spáchání trestného činu nebo přestupku. Co je v narušeném objektu do příjezdu policie nutné kontrolovat a zajistit?

Odpověď:

Řízení činnosti v místě podezření na spáchání trestného činu nebo přestupku

Postup operátora dohledového centra

- 1. Přijetí informace o události**
 - Zjistit místo události.
 - Ověřit charakter události (vloupání, krádež, poškození majetku, napadení apod.).
 - Vyhodnotit závažnost situace.
- 2. Vyslání výjezdové skupiny**

- Okamžitě vyslat výjezdovou skupinu k prověření.
- Předat jí všechny dostupné informace.

3. Přivolání Policie ČR

- Pokud vznikne podezření na trestný čin nebo přestupek, informovat Policii ČR na lince 158.
- Sdílet přesnou adresu a zjištěné skutečnosti.

Co je nutné v narušeném objektu kontrolovat a zajistit do příjezdu Policie ČR?

Zajištění místa události

- Zabránit vstupu nepovolaných osob.
- Vymezit prostor možného místa činu.
- Zajistit bezpečnost osob na místě.

Ochrana stop

- Nedotýkat se předmětů souvisejících s událostí.
- Nepřemisťovat věci, není-li to nezbytné z důvodu bezpečnosti.
- Nechodit zbytečně po místě činu.
- Chránit stopy před zničením nebo kontaminací.

Kontrola objektu

- Zjistit, zda se pachatel stále nenachází uvnitř.
- Zkontrolovat poškození vstupů, oken, dveří a zabezpečovacích prvků.
- Provéřit přítomnost zraněných osob.
- Zajistit případné svědky události.

Dokumentace zjištěného stavu

- **Poznamenat čas příjezdu a zjištěné skutečnosti.**
- **Zapamatovat si pohyb osob v okolí objektu.**
- **Zajistit kamerové záznamy, pokud jsou k dispozici.**

Předání Policii ČR

- Informovat policisty o všech zjištěných skutečnostech.
 - Označit místa možných stop.
 - Předat identifikační údaje svědků.
 - Předat případné kamerové záznamy nebo informace o nich.
-

Stručná odpověď ke zkoušce

Při podezření na spáchání trestného činu nebo přestupku vyšlu výjezdovou skupinu a informuji Policii ČR. Do jejího příjezdu zajistím místo události, zabráním vstupu nepovolaných osob, chráním stopy před zničením, kontroluji přítomnost pachatele a zraněných osob, zajišťuji svědky a dokumentuji zjištěný stav. Následně předám všechny informace Policii ČR.

Otázka B 18

Předvedte a vysvětlete pravidla postupu řízení činnosti při výhrůžkách bombovým útokem ve střeženém objektu

Odpověď:

Postup operátora dohledového centra při výhrůžce bombovým útokem ve střeženém objektu

1. Přijetí informace o hrozbě

Po přijetí informace o uložení výbušného systému nebo výhrůžce bombovým útokem:

- **zachovat klid!!!!**
- zjistit co nejvíce informací o hrozbě,
- zaznamenat čas přijetí oznámení,

- poznamenat si přesné znění výhrůžky,
- zjistit místo, kde má být bomba údajně umístěna,
- zjistit identitu oznamovatele, pokud je to možné.

2. Okamžité informování složek IZS

Neprodleně kontaktovat:

- Policii ČR – 158
- případně Integrovaný záchranný systém – 112

Operátor sdělí:

- adresu objektu,
- charakter hrozby,
- čas přijetí oznámení,
- všechny získané informace.

3. Řízení výjezdové skupiny

- Vyslat výjezdovou skupinu k objektu.
- Informovat ji, že se jedná o podezření na výbušné zařízení.
- **Zakázat jakoukoliv neodbornou manipulaci s podezřelými předměty.**

4. Evakuace osob

Pokud to vyžadují interní postupy nebo na pokyn Policie ČR:

- zahájit evakuaci osob z objektu,
- využít stanovené únikové cesty,
- zabránit vzniku paniky,
- přesunout osoby do bezpečné vzdálenosti.

5. Bezpečnostní opatření

- **Nevstupovat do rizikových prostor bez pokynu policie.**
- **Nedotýkat se podezřelých předmětů.**
- **Neotevírat nalezené balíčky nebo zavazadla.**
- **Nepoužívat v bezprostřední blízkosti podezřelého předmětu radiostanice ani mobilní telefony, pokud by mohly způsobit aktivaci zařízení podle pokynů zasahujících složek.**

6. Kontrola objektu

Pokud je kontrola prováděna, pak pouze v rozsahu interních pokynů a bez manipulace s nalezenými předměty:

- **vyhledávání neobvyklých balíčků,**
- **opuštěných zavazadel,**
- **předmětů nepatřících do daného prostředí,**
- **stop násilného vniknutí.**

7. Zajištění místa

- **Nepovolat nepovolané osoby do objektu.**
- **Uzavřít ohrožený prostor.**
- **Zajistit příjezdové komunikace pro složky IZS.**
- **Připravit informace pro Policii ČR.**

8. Předání Policii ČR

Po příjezdu policie předat:

- **čas oznámení,**
- **obsah výhrůžky,**
- **informace o volajícím,**

- výsledky kontroly objektu,
- seznam evakuovaných osob a svědků.

Stručná odpověď ke zkoušce

Při výhrůžce bombovým útokem jako operátor dohledového centra zjistím a zaznamenám všechny dostupné informace, okamžitě informuji Policii ČR, vyšlu výjezdovou skupinu a podle situace zajistím evakuaci osob. Zajistím uzavření prostoru, zakážu manipulaci s podezřelými předměty a připravím informace pro zasahující složky. Hlavním cílem je ochrana osob, zachování klidu a předání všech zjištěných skutečností Policii ČR.

Otázka B 19

Předvedte způsob řízení činnosti a vysvětlete rozdíl mezi evakuací osob z důvodu požáru, hrozbě bombovým útokem nebo při jiném hrozícím nebezpečí kdy je potřeba evakuovat větší počet osob.

Odpověď:

Pokud jde o zkoušku operátora DC (dohledového centra), měl by uchazeč prakticky předvést schopnost řídit evakuaci a koordinovat činnost zasahujících osob. Nejde pouze o znalost postupu, ale také o správnou komunikaci, předávání informací a rozhodování podle typu mimořádné události.

Praktické předvedení řízení činnosti

Operátor by měl prokázat, že umí:

1. Vyhodnotit vzniklou situaci

- **přijmout oznámení o mimořádné události,**
- **ověřit informace dostupnými prostředky (CCTV, EPS, EZS, ostražka apod.),**

- určit stupeň nebezpečí.

2. Vyhlásit odpovídající opatření

- aktivovat evakuační postup,
- informovat vedení objektu,
- přivolat složky IZS (HZS, Policii ČR, ZZS).

3. Řídit osoby zapojené do evakuace

- vydávat jasné a stručné pokyny,
- koordinovat členy ostrahy a odpovědné pracovníky,
- sledovat průběh evakuace.

4. Zajistit kontrolu a evidenci

- ověřit opuštění ohrožených prostor,
- určit shromaždiště,
- předat informace zasahujícím složkám.

Rozdíl mezi jednotlivými druhy evakuace

1. Evakuace při požáru

Cíl:

Co nejrychleji dostat osoby z bezprostředně ohroženého prostoru.

Postup:

- okamžité opuštění objektu po únikových cestách,
- zákaz používání výtahů,
- uzavírání dveří za sebou kvůli omezení šíření kouře,
- přesun na určené shromaždiště.

Charakteristika:

- rychlá a neodkladná evakuace,
 - hlavním nebezpečím je oheň, kouř a zplodiny hoření.
-

2. Evakuace při hrozbě bombovým útokem

Cíl:

Minimalizovat ohrožení osob případným výbuchem.

Postup:

- nepanikařit a nezveřejňovat detaily hrozby mezi lidmi,
- nevyhledávat podezřelý předmět vlastními silami,
- řídit se pokyny Policie ČR,
- osoby vyvést mimo předpokládaný dosah výbuchu.

Charakteristika:

- evakuace bývá organizovanější a řízenější než při požáru,
 - vyhýbá se místům, kde by mohl být nástražný systém,
 - často se stanovuje větší bezpečnostní vzdálenost od objektu.
-

3. Evakuace při jiném hrozícím nebezpečí

Například:

- únik nebezpečných látek,
- únik plynu,
- narušení statiky budovy,
- povodeň,

- aktivní útočník.

Postup:

Závisí na charakteru hrozby.

Může být:

- úplná evakuace objektu,
- částečná evakuace pouze některých prostor,
- nebo dokonce ukrytí osob uvnitř budovy (shelter-in-place), pokud je venkovní prostředí nebezpečnější.

Charakteristika:

- postup se přizpůsobuje konkrétní situaci,
- operátor musí vyhodnotit pokyny IZS a krizových plánů.

Stručná odpověď ke zkoušce

Při požáru se osoby rychle odvádějí z objektu po únikových cestách. Při bombové hrozbě se evakuace provádí řízeně a s ohledem na možné umístění výbušniny, zpravidla za součinnosti Policie ČR. Při jiném nebezpečí závisí způsob evakuace na druhu hrozby; může být úplná, částečná nebo může být naopak nařízeno ukrytí osob v objektu. Operátor DC musí umět celou činnost koordinovat, komunikovat s IZS a zajistit bezpečnost evakuovaných osob.

Otázka C 20

Zaznamenejte průběh revize I&HAS revizním technikem ve střeženém objektu.

Zaznamenejte průběh události slabá baterie (nízké napájecí napětí) v bezdrátovém prostorovém pohybovém detektoru v jednom ze střežených objektů. Zaznamenejte průběh

události porucha akumulátoru (nízké napájecí napětí záložního napájecího zdroje) v ústředně I&HAS v jednom ze střežených objektů.

Odpověď:

Záznam revize I&HAS (EZS) revizním technikem

Operátor dohledového centra musí zaznamenat do provozního deníku nebo informačního systému zejména:

- datum a čas zahájení revize,
- název a adresu objektu,
- jméno revizního technika,
- číslo služebního průkazu nebo firmy,
- rozsah prováděných prací,
- přechod objektu do servisního/revizního režimu,
- případné testování detektorů, sirén a přenosových cest,
- ukončení revize,
- potvrzení o uvedení systému do plného provozu.

Vzor záznamu

Plain Text

20.06.2026 09:00 hod.

Objekt: Hotel Alfa, Praha

Dostavil se revizní technik společnosti ABC Security,

p. Jan Novák.

Na žádost technika objekt převeden do servisního režimu.

Prováděna pravidelná revize I&HAS(EPS), funkční zkoušky detektorů, ústředny, sirén a přenosové cesty.

11:15 hod. Revize ukončena bez závad.

System uveden do střežení.

Zapsal: Operátor DC Antonín Zahálka

2. Záznam události – slabá baterie v bezdrátovém pohybovém detektoru

Postup operátora

- **Přijmout poruchový signál.**
- **Identifikovat objekt a konkrétní detektor.**
- **Telefonicky informovat odpovědnou osobu.**
- **Doporučit výměnu baterie servisní organizací.**
- **Evidovat průběh řešení.**

Vzor záznamu

20.06.2026 14:32 hod.

Objekt: Administrativní budova Delta

Přijat poruchový signál:

SLABÁ BATERIE – bezdrátový prostorový pohybový detektor

Detektor č. 08 – sklad 1. NP.

Informována odpovědná osoba objektu

p. Petr Novák v 14:35 hod.

Doporučeno objednání servisního zásahu

a výměna baterie detektoru.

Objekt nadále střežen, bez dalších závad.

Zapsal: Operátor DC Marek Bílek

3. Záznam události – porucha akumulátoru ústředny I&HAS (EZS)

Postup operátora

- **Přijmout poruchový signál.**
- **Ověřit, že se jedná o poruchu záložního zdroje.**
- **Informovat kontaktní osobu a servis.**
- **Monitorovat další stav systému.**
- **Zapsat veškeré úkony do evidence.**

Vzor záznamu

20.06.2026 16:05 hod.

Objekt: Výrobní areál Beta

Přiját poruchový signál:

PORUCHA AKUMULÁTORU ÚSTŘEDNY I&HAS

Nízké napětí záložního napájecího zdroje.

Vyrozuměna odpovědná osoba objektu

p. Jana Svobodová v 16:08 hod.

Informována servisní organizace ABC Security.

Doporučena kontrola a výměna akumulátoru ústředny.

**System v době hlášení funkční, napájen ze
síťového zdroje 230 V.**

Událost evidována a dále monitorována.

Zapsal: Operátor DC Jiří Švácha

Zobrazit více řádků

Stručná odpověď ke zkoušce

**Operátor musí vždy zaznamenat datum, čas, objekt, typ události,
přesné znění poruchy, provedená opatření, informované osoby,**

případné přivolání servisu a čas ukončení události. Zápis musí být stručný, věcný, přesný a umožnit zpětnou kontrolu průběhu události.

Otázka č. C 22

Vyjmenujte zásady elektronického záznamu událostí ARC. Čím se záznam událostí řídí? Jaké podmínky musí splňovat záznam komunikace a přijatých signálů? Popište povinný záznam každého zákazníka, resp. střeženého objektu. Jaké další evidence o obsluze dohledového centra musí záznamy obsahovat?

Odpověď:

Zásady elektronického záznamu událostí ARC(PCO)

Elektronický záznam musí být:

- **průběžný a nepřetržitý,**
- **přesný, úplný a pravdivý,**
- **vedený v chronologickém pořadí,**
- **zabezpečený proti ztrátě, poškození a neoprávněným změnám,**
- **dohledatelný zpětně po celou dobu stanovené archivace,**
- **opatřený časovou značkou (datum a čas vzniku záznamu).**

2. Čím se záznam událostí řídí?

Záznam událostí se řídí zejména:

- **normou ČSN EN 50518 – Dohledová a poplachová přijímací centra (ARC),**
- **interními provozními předpisy provozovatele ARC,**
- **smluvními požadavky zákazníka,**
- **případně dalšími právními předpisy týkajícími se ochrany osobních údajů a bezpečnostních služeb.**

3. Jaké podmínky musí splňovat záznam komunikace a přijatých signálů?

Záznam musí obsahovat:

- identifikaci zdroje signálu,
- datum a přesný čas přijetí,
- druh zprávy (poplach, porucha, test, sabotáž, stavová zpráva apod.),
- zaznamenání veškeré komunikace související s událostí,
- identifikaci operátora, který událost zpracovával,
- přijatá a provedená opatření,
- výsledek řešení události.

Komunikace musí být archivována tak, aby bylo možné její následné přehrání nebo kontrolu a aby nebyla dodatečně neoprávněně měněna.

4. Povinný záznam každého zákazníka (střeženého objektu)

U každého zákazníka musí být evidováno zejména:

- název nebo jméno klienta,
- adresa střeženého objektu,
- identifikační číslo objektu v systému,
- kontaktní osoby a jejich telefonní spojení,
- režim střežení,
- seznam oprávněných osob,
- postupy pro řešení jednotlivých typů poplachů,

- informace o instalovaném zabezpečovacím systému,
- historie událostí a zásahů.

5. Jaké další evidence o obsluze dohledového centra musí záznamy obsahovat?

Evidence musí obsahovat také údaje o:

- službách operátorů,
- přihlášení a odhlášení operátorů do systému,
- předávání směn,
- mimořádných událostech na pracovišti,
- výpadcích technologií a komunikačních cest,
- testech a kontrolách funkčnosti systému,
- školení a oprávnění operátorů,
- zásazích administrátorů do systému.

Shrnutí: Elektronický záznam ARC musí umožnit úplnou rekonstrukci události – od přijetí signálu přes komunikaci operátora až po konečné vyřešení situace, včetně identifikace osob, času a provedených opatření.

Otázka C 22

Vysvětlete význam vedení dokumentace operátorem/operátorkou o průběhu služby, o mimořádných událostech, o kontrolách a o poskytovaných službách. Jaké náležitosti musí splňovat a obsahovat záznam o mimořádné události?

Odpověď:

Význam vedení dokumentace operátorem/operátorkou DC

Vedení dokumentace je jednou ze základních povinností operátora dohledového centra (DC).

Slouží k zajištění průkaznosti, kontroly a vyhodnocování poskytovaných služeb a umožňuje zpětně doložit všechny činnosti provedené během služby. Požadavky na evidenci a záznamy vycházejí z provozních pravidel dohledových a poplachových přijímacích center podle ČSN EN 50518.

Dokumentace o průběhu služby

Záznam o průběhu služby slouží k:

- evidenci všech důležitých činností během směny,
- předávání informací mezi směnami,
- doložení řádného výkonu služby,
- kontrole práce operátorů,
- řešení případných reklamací nebo sporů,
- zpětnému vyhodnocení bezpečnostních událostí.

Obvykle obsahuje:

- datum a čas služby,
 - jméno operátora,
 - převzetí a předání směny,
 - přijaté signály a jejich řešení,
 - technické závady,
 - důležité pokyny nadřízených,
 - mimořádné události vzniklé během služby.
-

Dokumentace o mimořádných událostech

Evidence mimořádných událostí slouží k:

- prokázání správnosti postupu operátora,
 - následnému šetření události,
 - vyhodnocení bezpečnostních rizik,
 - komunikaci se zákazníkem, Policií ČR, HZS nebo dalšími složkami IZS,
 - zlepšování bezpečnostních opatření.
-

Dokumentace o kontrolách

Záznamy o kontrolách jsou důležité pro:

- ověřování funkčnosti technických zařízení,
- kontrolu spojení mezi objektem a DC,
- plnění zákonných a smluvních povinností,
- prokazování pravidelné údržby a testování systémů.

Dokumentace o poskytovaných službách

Tato evidence slouží k:

- doložení rozsahu poskytovaných služeb zákazníkovi,
- fakturaci služeb,
- vyhodnocení kvality poskytované ochrany,

- statistickému zpracování událostí a zásahů.

Obsahuje například:

- počet přijatých poplachů,
- výjezdy zásahové jednotky,
- kontrolní činnosti,
- komunikaci s kontaktními osobami,
- další provedené úkony.

Náležitosti záznamu o mimořádné události

Záznam o mimořádné události musí být přesný, úplný, pravdivý, časově dohledatelný a musí umožňovat zpětnou rekonstrukci celé události.

Povinné údaje

Záznam by měl obsahovat zejména:

1. Datum a čas vzniku události.
2. Identifikaci střeženého objektu (název, adresa, identifikační číslo).
3. Druh mimořádné události, například:
 - vloupání,
 - požár,
 - přepadení,
 - technická porucha,
 - sabotáž,

- výpadek spojení.
4. Způsob zjištění události (signál, telefonické oznámení, kamerový systém apod.).
 5. Jméno operátora, který událost řešil.
 6. Průběh řešení události v časové posloupnosti.
 7. Provedená opatření (vyrozumění zákazníka, výjezd zásahové jednotky, přivolání Policie ČR nebo HZS).
 8. Jména a kontakty osob, které byly informovány.
 9. Výsledek řešení události.
 10. Datum, čas a způsob ukončení události.
 11. Podpis nebo elektronickou identifikaci operátora, který záznam pořídil.

Požadavky na záznam

Záznam musí být:

- čitelný,
- jednoznačný,
- chronologický,
- bez dodatečných neoprávněných úprav,
- archivovaný po stanovenou dobu,
- dostupný pro kontrolu a audit.

Vzor stručného zápisu

Datum: 20. 6. 2026

Objekt: Sklad ABC, Praha

Čas přijetí signálu: 02:14:26

Typ události: Poplach – narušení objektu

Operátor: Jan Novák

Průběh: Přijat poplach z detektoru pohybu. Ověření kamerovým systémem. Kontaktována zásahová jednotka a odpovědná osoba objektu.

Výsledek: Na místě zjištěn neoprávněný vstup pachatele. Událost předána Policii ČR.

Ukončení události: 03:05 hod.

Takto vedená dokumentace umožňuje prokázat, že operátor postupoval správně, včas a v souladu s interními předpisy i požadavky zákazníka

Otázka C 23

Popište zásady ochrany osobních údajů při zpracování v dohledovém centru, zejména pojmy správce, zpracovatel, archivace a předávání osobních údajů.

Odpověď:

Zásady ochrany osobních údajů při zpracování v dohledovém centru (DC)

Při provozu dohledového centra se zpracovávají osobní údaje zákazníků, kontaktních osob, zaměstnanců, návštěvníků objektů i osob zachycených kamerovými systémy. Operátor DC je povinen dodržovat zásady ochrany osobních údajů podle nařízení Evropské komise – tzv. GDPR (General data protection regulation) a interních předpisů organizace.

1. Správce osobních údajů

Správce je fyzická nebo právnická osoba, která určuje účel a prostředky zpracování osobních údajů.

V prostředí DC bývá správcem například:

- bezpečnostní agentura provozující dohledové centrum,
- vlastník střeženého objektu,
- společnost, která objednala službu monitorování.

Správce odpovídá za:

- zákonnost zpracování osobních údajů,
 - zabezpečení údajů,
 - informování subjektů údajů,
 - stanovení doby uchování údajů,
 - určení osob oprávněných s údaji pracovat.
-

2. Zpracovatel osobních údajů

Zpracovatel je osoba nebo organizace, která zpracovává osobní údaje pro správce na základě jeho pokynů.

V oblasti DC může být zpracovatelem například:

- provozovatel dohledového centra pro klienta,
- poskytovatel cloudového úložiště,
- servisní firma zajišťující provoz bezpečnostních systémů.

Zpracovatel:

- nesmí používat údaje pro vlastní účely,
 - zpracovává údaje pouze podle pokynů správce,
 - musí zajistit jejich technické a organizační zabezpečení,
 - zachovává mlčenlivost o získaných informacích.
-

3. Zásady zpracování osobních údajů v DC

Operátor DC musí dodržovat tyto základní zásady:

Zákonnost

Osobní údaje lze zpracovávat pouze na zákonném základě (smlouva, zákonná povinnost, oprávněný zájem apod.).

Účelové omezení

Údaje lze využívat pouze pro účely, pro které byly získány:

- ochrana osob a majetku,
- monitoring objektů,
- řešení poplachů,
- evidence zásahů.

Minimalizace údajů

Zpracovávají se pouze údaje nezbytné pro výkon služby.

Přesnost údajů

Vedené údaje musí být aktuální a správné.

Důvěrnost a bezpečnost

Operátor nesmí poskytovat údaje neoprávněným osobám a musí chránit přístupová hesla, databáze i dokumentaci.

4. Archivace osobních údajů

Archivace znamená uchovávání osobních údajů a záznamů po stanovenou dobu.

Archivují se například:

- záznamy o poplachu,

- telefonní hovory,
- provozní deníky,
- kamerové záznamy,
- záznamy o výjezdech a zásazích.

Při archivaci musí být splněny podmínky:

- ochrana před ztrátou a zneužitím,
- omezený přístup pouze oprávněným osobám,
- evidence doby uchování,
- bezpečná likvidace po uplynutí archivační lhůty.

Operátor musí respektovat stanovené retenční (archivační) doby a nesmí údaje uchovávat déle, než je nutné.

5. Předávání osobních údajů

Osobní údaje lze předávat pouze oprávněným subjektům.

Nejčastěji se předávají:

- **Policii ČR,**
- **Hasičskému záchrannému sboru,**
- **zdravotnické záchranné službě,**
- **smluvním zásahovým jednotkám,**
- **oprávněným zástupcům zákazníka.**

Při předávání musí operátor:

- **ověřit totožnost příjemce,**
- **předat pouze nezbytný rozsah údajů,**

- zaznamenat komu, kdy a jaké údaje byly předány,
- dodržovat interní bezpečnostní postupy.

Údaje se nesmí poskytovat:

- nepovolaným osobám,
- médiím,
- známým a rodinným příslušníkům,
- jiným zákazníkům.

6. Povinnosti operátora DC

Operátor dohledového centra je povinen:

- zachovávat mlčenlivost,
- chránit přístupová hesla a identifikační údaje,
- pracovat pouze s údaji nezbytnými k výkonu služby,
- nepořizovat neoprávněné kopie dokumentů či záznamů,
- hlásit bezpečnostní incidenty a úniky dat,
- dodržovat GDPR a interní předpisy organizace.

Shrnutí ke zkoušce

- Správce určuje účel a způsob zpracování osobních údajů.
- Zpracovatel údaje zpracovává jménem správce podle jeho pokynů.

- Archivace je bezpečné uchovávání osobních údajů po stanovenou dobu.
- Předávání osobních údajů je možné pouze oprávněným osobám a v nezbytném rozsahu.
- Operátor DC musí zajistit důvěrnost, integritu a bezpečnost všech osobních údajů, se kterými při výkonu služby pracuje.

Otázka C 24

Jaké postupy musí být v souladu s ČSN při zpracování údajů o zákaznících v ARC dodrženy, vypracovány a zavedeny? Jak se zaznamenávají, aktualizují, uchovávají a likvidují údaje o zákaznících?

Odpověď:

Podle normy ČSN EN 50518 – Dohledová a poplachová přijímací centra (ARC/PCO) musí mít provozovatel ARC (PCO) vypracovány, zavedeny a udržovány dokumentované postupy pro správu zákaznických informací a účtů.

Norma výslovně požaduje postupy pro:

- vytváření, změny a rušení služeb nebo zákaznických účtů,
- správu informací,
- zálohování údajů,
- důvěrnost a klasifikaci informací,
- administrativní postupy,
- zaznamenávání (logování) událostí a změn dat.

Zaznamenávání údajů o zákaznících

Údaje o zákaznících se vedou v systému správy poplachů (databázi ARC) formou zákaznických záznamů. Norma vyžaduje evidenci a protokolování změn („logování“) tak, aby bylo možné dohledat:

- kdo změnu provedl,
- kdy byla provedena,
- jaká data byla změněna.

Součástí systému jsou i protokoly matričních údajů a protokoly událostí.

Aktualizace údajů

Aktualizace zákaznických údajů musí probíhat podle schváleného postupu pro:

- vytváření nových záznamů,
- editaci stávajících záznamů,
- potvrzení provedených změn,
- řízení přístupových práv oprávněných osob.

Norma rovněž upozorňuje na řízení vzdáleného přístupu a autorizaci osob provádějících změny.

Uchovávání údajů

Údaje o zákaznících musí být:

- chráněny proti ztrátě, neoprávněné změně a zneužití,
- pravidelně zálohovány,
- uchovávány v souladu s pravidly důvěrnosti a klasifikace informací,
- přístupné pouze oprávněným pracovníkům ARC.

Likvidace údajů(skartace)

Při ukončení služby nebo zrušení zákaznického účtu musí být údaje odstraněny řízeným způsobem podle administrativních postupů ARC. Likvidace důvěrných informací má být provedena bezpečně tak, aby nebylo možné jejich obnovení nebo zneužití; norma odkazuje také na zásady bezpečného ničení důvěrných materiálů.

Stručná odpověď do zkoušky

V ARC (PCO) musí být podle ČSN EN 50518 vypracovány a zavedeny postupy pro vytváření, změny a rušení zákaznických účtů, správu informací, zálohování dat, ochranu důvěrných informací a administrativní činnosti. Údaje o zákaznících se evidují v databázi ARC, všechny změny se logují a autorizují. Data se pravidelně aktualizují, zálohují a chrání před neoprávněným přístupem. Po ukončení služby se údaje likvidují bezpečným a dokumentovaným způsobem.

Otázka C 25

Vysvětlete, jaké podmínky musí splňovat přijatý signál z I&HAS dohledovým centrem. Jakým způsobem jsou chráněny přijímané signály proti ztrátě způsobené poruchou nebo poškozením přijímacího zařízení? Jakým způsobem se signály chrání v průběhu přenosu?

Odpověď:

Podle ČSN EN 50518 musí být signály z I&HAS (Intruder and Hold-up Alarm System – EZS) přijímány v ARC/PCO takovým způsobem, aby byla zajištěna jejich správná identifikace, zpracování a ochrana proti

ztrátě. Norma současně stanovuje požadavky na spolehlivost přijímacího zařízení i přenosové cesty.

1. Jaké podmínky musí splňovat přijatý signál z I&HAS (EZS)

Přijatý signál musí:

- **být jednoznačně identifikovatelný,**
- **obsahovat informaci o zdroji (objektu, účtu nebo zařízení),**
- **umožnit určení typu události (poplach, tísňový poplach, sabotáž, porucha, zapnutí/vypnutí systému apod.),**
- **být správně zobrazen operátorovi ARC,**
- **být zaznamenán do systému správy poplachů a uložen do protokolu událostí,**
- **být zpracován podle stanovených operačních postupů ARC.**

2. Ochrana proti ztrátě signálu při poruše nebo poškození přijímacího zařízení

Norma požaduje vysokou provozní dostupnost ARC(PCO). Z tohoto důvodu jsou přijímané signály chráněny zejména:

- **použitím záložních přijímacích zařízení,**
- **redundantní konfigurací kritických částí systému,**
- **záložním napájením (UPS a náhradní zdroje),**
- **nepřetržitým dohledem nad funkčností přijímacích zařízení,**
- **automatickou detekcí poruch a jejich hlášením obsluze,**
- **zálohováním provozních a zákaznických dat.**

Pokud dojde k poruše některé části systému, musí být zachována schopnost přijímat a zpracovávat poplachové zprávy prostřednictvím záložního zařízení nebo redundantního systému.

3. Jak se chrání signály během přenosu

Při přenosu mezi EZS a ARC jsou signály chráněny několika způsoby:

- dohledem nad přenosovou cestou (monitorování spojení),
- pravidelnými testovacími přenosy,
- detekcí výpadku komunikace,
- použitím více přenosových cest (např. IP + GSM/GPRS/LTE),
- autentizací komunikujících zařízení,
- kontrolou integrity přenášených dat,
- šifrováním přenosu, pokud je použito daným přenosovým systémem.

ARC musí být schopno rozpoznat přerušení komunikace nebo manipulaci s přenosovou cestou a vyhlásit odpovídající poruchový či sabotážní stav.

Redundance znamená zdvojení nebo vícenásobné zajištění důležité části systému, aby při poruše jedné části systém fungoval dál.

V prostředí PCO/ARC se používá proto, aby nebyly ztraceny poplachové signály a centrum zůstalo v provozu i při závadě. ČSN EN 50518 vyžaduje vysokou dostupnost a používání záložních řešení pro kritické funkce ARC.

Příklady redundance v ARC(PCO)

1. Redundance přijímačů

- **Hlavní přijímač** přijímá poplachové zprávy.
- Pokud se porouchá, automaticky jej nahradí **záložní přijímač**.

2. Redundance napájení

- Sít' 230 V.
- **UPS** (záložní zdroj).
- Případně **dieselagregát**.

Při výpadku elektřiny pracuje centrum dále.

3. Redundance komunikačních cest

Objekt může odesílat poplach:

- přes **internet (IP)**,
- současně přes **GSM/LTE síť**.

Pokud jedna cesta selže, zpráva dorazí druhou cestou.

4. Redundance serverů

- **Hlavní server** ukládá data.
- **Záložní server** má stejná data a převezme práci při poruše hlavního serveru.

Stručná odpověď ke zkoušce

Přijatý signál z EZS musí být identifikovatelný, správně zaznamenaný a přiřazený ke konkrétnímu objektu a typu události. Proti ztrátě je chráněn redundantními přijímači, záložním napájením, monitorováním poruch a zálohováním dat. Během přenosu jsou signály chráněny dohledem nad přenosovou cestou, testovacími přenosy, více komunikačními cestami, autentizací, kontrolou integrity dat a případně šifrováním.

Redundance je zdvojení nebo vícenásobné zajištění důležitých zařízení, přenosových cest nebo zdrojů tak, aby při poruše jedné části systému nebyla přerušena činnost ARC a nedošlo ke ztrátě poplachových signálů

Otázka C 26

Popište zásady ochrany přijímaných signálů, zpráv, obrazových a zvukových záznamů, jejich uchování, a způsob likvidace v dohledovém centru

Odpověď:

Podle ČSN EN 50518 musí být v dohledovém a poplachovém přijímacím centru (ARC/PCO) zajištěna ochrana všech přijímaných informací – tedy poplachových signálů, zpráv, obrazových i zvukových záznamů. Součástí ochrany je jejich bezpečný přenos, ukládání, přístupová ochrana, zálohování a následná likvidace.

1. Ochrana přijímaných signálů a zpráv

Přijímané signály a zprávy musí být chráněny proti:

- ztrátě,
- neoprávněné změně,
- poškození,
- zneužití,
- neoprávněnému přístupu.

Ochrana je zajišťována zejména:

- redundantními(zdvojenými) přijímacími zařízeními,
- záložním napájením UPS,dieselagregát),
- monitorováním provozuschopnosti systému,

- dohledem nad komunikačními cestami,
- protokolováním (logováním-či šifrováním) všech událostí a změn.

2. Ochrana obrazových a zvukových záznamů

Pokud ARC (PCO) přijímá obrazové nebo zvukové informace (např. CCTV (televizní analogový nebo digitální okruh), musí být:

- ukládány v zabezpečených systémech,
- přístupné pouze oprávněným osobám,
- chráněny před kopírováním a zneužitím,
- evidovány a klasifikovány jako důvěrné informace.

Každý přístup k těmto údajům by měl být dohledatelný prostřednictvím záznamů systému.

3. Uchovávání údajů

Norma požaduje, aby byly údaje:

- evidovány a ukládány v databázi ARC,
- pravidelně zálohovány,
- uchovávány po stanovenou dobu podle provozních a právních předpisů,
- chráněny proti ztrátě a neoprávněnému přístupu.

Součástí uchovávání je také:

- vedení protokolů událostí,
- archivace záznamů,

- možnost zpětného dohledání událostí a provedených změn.

4. Likvidace údajů (tzv. skartace údajů)

Po uplynutí doby uchování nebo při zrušení služby musí být data odstraněna bezpečným způsobem tak, aby nebylo možné jejich obnovení nebo zneužití. Norma odkazuje na zásady bezpečného ničení důvěrných materiálů.

Likvidace zahrnuje:

- mazání elektronických záznamů,
- fyzické zničení datových médií, pokud je to nutné (skartační komisi)
- skartaci tištěných dokumentů,
- dokumentaci provedené likvidace.

Stručná odpověď ke zkoušce

Přijímané signály, zprávy, obrazové a zvukové záznamy musí být v ARC(PCO) chráněny proti ztrátě, poškození, změně a neoprávněnému přístupu. Uchovávají se v zabezpečených databázích s omezeným přístupem a pravidelně se zálohují. Veškeré události a změny se protokolují. Po skončení doby uchování nebo zrušení služby se údaje likvidují bezpečným a dokumentovaným způsobem tak, aby nemohlo dojít k jejich zneužití.

Otázka D 27

Zaznamenal/a jste poplach z prostorového pohybového detektoru a zároveň signál o úniku plynu z hlásiče únikuplynu. Předejte zprávy, komu smíte, komu musíte, na koho nesmíte zapomenout zůstane-li po mimořádné události hlásič úniku plynu v poruše. Kdo obdrží informaci o zaznamenaném poplachu jako první?

Odpověď:

V této situaci pracovník ARC (PCO) přijal současně:

- 1. Poplach z prostorového pohybového detektoru (EZS).**
- 2. Signál o úniku plynu z hlásiče úniku plynu.**

Postupuje podle stanovených zásahových a vyzumívacích postupů.

Kdo obdrží informaci jako první?

Jako první se řeší událost představující bezprostřední ohrožení života a zdraví osob, tedy únik plynu. Proto musí být neprodleně vyzuměny složky určené v poplachových směrnících (typicky Hasičský záchranný sbor) a kontaktní osoby zákazníka.

Komu musíte zprávu předat

- Hasičskému záchrannému sboru (pokud to stanoví postupy nebo smlouva) na č. 150
- Odpovědné osobě zákazníka uvedené v databázi ARC (PCO).
- Případně zásahové jednotce nebo bezpečnostní službě vyslané na objekt.
- Dalším osobám uvedeným v poplachovém plánu objektu.

Komu smíte zprávu předat

Pouze:

- oprávněným kontaktním osobám uvedeným u zákazníka,
- složkám IZS,
- osobám a organizacím určeným provozními postupy ARC.

Komu nesmíte zprávu předat

- Neoprávněným osobám.

- Náhodným volajícím.
- Médiím.
- Osobám, které nejsou uvedeny v seznamu oprávněných kontaktů.

Na koho nesmíte zapomenout, zůstane-li hlásič plynu v poruše

Pokud po zásahu zůstane hlásič úniku plynu nefunkční nebo v poruše, je nutné informovat:

- zákazníka (provozovatele objektu),
- odpovědnou osobu objektu,
- servisní organizaci odpovědnou za opravu systému,
- případně vlastníka objektu, pokud je odlišný od uživatele.

Zároveň musí být porucha zaznamenána do evidence ARC(PCO) a sledována až do odstranění.

Stručná odpověď ke zkoušce

Při současném přijetí poplachu EZS a signálu o úniku plynu má přednost řešení úniku plynu, protože představuje bezprostřední ohrožení života a majetku. Informace se předává HZS, oprávněným kontaktním osobám zákazníka a případně zásahové jednotce. Nesmí být sdělována neoprávněným osobám. Pokud po mimořádné události zůstane hlásič plynu v poruše, musí být informován zákazník a servisní organizace a porucha musí být evidována až do odstranění.

Otázka D 28

Komunikujte pomocí příslušných spojovacích prostředků s pracovníkem výjezdové skupiny. Jaké způsoby komunikace a spojovací prostředky je možné použít, jsou-li součástí vybavení ARC? Jaké informace je nezbytně nutné správně a neprodleně předat pracovníkovi výjezdové skupiny o zaznamenaném poplachu?

Odpověď:

U zkoušky byste měl odpovídat prakticky, jako byste skutečně seděl na pracovišti **Alarm Receiving Centre (ARC)** a komunikoval s výjezdovou skupinou.

Ukázka komunikace operátora DC s výjezdovou skupinou

Operátor DC (radiostanice):

„Výjezdová skupino 1, zde DC (dohledové centrum). Provedte výjezd na objekt **Hypermarket Anděl**, Praha 4, ul. **Novodvorská 125**. Na objektu byl v **02:15 hod.** zaznamenán poplach – narušení objektu. Aktivováno čidlo pohybu ve skladu v zadní části budovy. Kamerový systém zaznamenal pohyb jedné neznámé osoby. Policie ČR byla informována. **Potvrďte příjem.**“

Výjezdová skupina:

„Výjezdová skupina 1, příjem. Vyjíždíme na místo.“

Operátor DC:

„Rozumím. Předpokládaný příjezd za 8 minut. Po příjezdu proveďte kontrolu objektu a informujte DC o situaci.“

Možné způsoby komunikace v ARC(PCO)

Jsou-li součástí vybavení ARC, lze použít zejména:

1. Radiostanice

- nejčastější spojení mezi operátorem a výjezdovou skupinou,
- rychlá a nepřetržitá komunikace.

2. Mobilní telefon

- hlasové hovory,

- SMS zprávy.

3. Pevná telefonní linka

- komunikace s výjezdovou skupinou,
- kontaktování klienta,
- spojení se složkami IZS.

4. Datové přenosy

- GPRS/LTE komunikátory,
- aplikace pro výjezdové skupiny,
- GPS monitoring vozidel.

5. PCO/ARC software

- textové zprávy,
- předávání událostí prostřednictvím monitorovacího systému.

6. Kamerový a audio systém

- dálkové ověření poplachu,
- přenos informací z objektu.

Jaké informace musí operátor neprodleně předat výjezdové skupině

Pracovník výjezdové skupiny musí obdržet všechny důležité údaje potřebné k bezpečnému zásahu:

Identifikace objektu

- název objektu,
- přesná adresa,
- číslo objektu v evidenci.

Druh poplachu

- narušení objektu,
- tísňový poplach,
- požární poplach,
- technický poplach,
- sabotáž systému apod.

Čas vzniku události

- přesný čas přijetí poplachu,
- případně opakované aktivace.

Místo aktivace

- konkrétní zóna,
- číslo čidla,
- dveře, okno, sklad, kancelář apod.

Ověřené informace

- záznam z kamer,
- přítomnost osob,
- viditelné poškození objektu,
- další zjištěné skutečnosti.

Přijatá opatření

- zda byla informována Policie ČR,
- zda byl kontaktován klient,
- zda na místo míří další výjezdová skupina.

Bezpečnostní informace

- podezření na pachatele,
 - počet osob,
 - případná nebezpečí na místě.
-

Stručná odpověď ke zkoušce

Operátor DC může s výjezdovou skupinou komunikovat prostřednictvím radiostanice, mobilního telefonu, pevné telefonní linky, datových přenosů nebo prostřednictvím systému ARC. Při vyhlášení výjezdu musí neprodleně předat adresu objektu, druh poplachu, čas a místo aktivace, výsledky ověření poplachu, přijatá opatření a další informace důležité pro bezpečný a účinný zásah výjezdové skupiny.

Otázka D 29

Komunikujte se zákazníkem narušeného objektu. Vysvětlete a domluvte se zákazníkem servis I&HAS z důvodu ztráty komunikace s ARC, z důvodu poruchy záložního akumulátoru v ústředně systému.

Odpověď:

komunikace operátora ARC (PCO) se zákazníkem

„Dobrý den, zde operátor PCO (ARC) společnosti [název]. Volám ohledně vašeho zabezpečovacího systému na objektu [adresa nebo název objektu]. Na našem dohledovém centru jsme zaznamenali ztrátu komunikace mezi ústřednou EZS a ARC(PCO) a současně poruchu záložního akumulátoru ústředny.

To znamená, že zabezpečovací systém nemusí být schopen spolehlivě předávat poplachové informace na PCO a při výpadku síťového napájení nemusí být zajištěna jeho správná funkce.

Doporučujeme co nejdříve zajistit servisní zásah odborné servisní firmy. Je potřeba prověřit přenosovou cestu, obnovit komunikaci s PCO a zkontrolovat, případně vyměnit záložní akumulátor v ústředně.

Můžeme vám zajistit kontakt na servisní organizaci nebo servis objednáte vlastní cestou? Prosím o potvrzení, že jste informaci převzal/a.“

Informace, které musí operátor sdělit

- **druh poruchy:**
 - ztráta komunikace s ARC (PCO),
 - porucha záložního akumulátoru (např. vybitá baterie),
- **možné důsledky:**
 - omezená schopnost přenášet poplachy,
 - nefunkčnost systému při výpadku elektrické energie,
- **doporučení k neodkladnému servisu,**
- zaznamenání informace do **provozního deníku** ARC (PCO),
- potvrzení převzetí informace zákazníkem.

Stručná odpověď ke zkoušce

Operátor informuje zákazníka o ztrátě komunikace mezi EZS a ARC a o poruše záložního akumulátoru. Vysvětlí, že systém nemusí spolehlivě přenášet poplachové zprávy a při výpadku napájení nemusí být funkční. Doporučí bezodkladný servisní zásah, dohodne způsob jeho zajištění a provede záznam o vyrozumění zákazníka.

Komunikujte s integrovaným záchranným systémem. Nalezena zraněná osoba v zakouřeném objektu. Bezvládná osoba v kotelně, kde unikal plyn. Zraněný pracovník výjezdové skupiny z důvodu dopravní nehody při výjezdu.

Odpověď:

Při komunikaci s Integrovaným záchranným systémem (112 nebo 150) musí operátor DC (ARC/PCO) mluvit klidně, stručně, věcně a přesně, bez domněnek a pouze s ověřenými informacemi.

Vzor hlášení na tísňovou linku 112 nebo 150

„Dobrý den, zde operátor PCO(ARC) [název společnosti].

Oznamuji mimořádnou událost na adrese [adresa objektu].

V objektu byl zaznamenán požární poplach a objekt je zakouřený. Podle získaných informací se uvnitř nachází jedna bezvládná osoba, která se nachází v kotelně, kde došlo k úniku plynu .

Dále došlo při výjezdu k dopravní nehodě vozidla výjezdové skupiny a jeden pracovník výjezdové skupiny je zraněn.

Na místě hrozí nebezpečí zplodin hoření a úniku plynu.

Kontaktní osoba na místě je pan Antonín Zahálka mobil (.....)

Žádám o vyslání potřebných složek IZS.

Jsem k dispozici pro další informace."

Jaké informace musí operátor předat

1. Kdo volá

- jméno operátora,
- název ARC/PCO,
- telefonní číslo pro zpětný kontakt.

2. Kde se událost stala

- přesná adresa,
- případně upřesnění místa v objektu.

3. Co se stalo

- zakouřený objekt,
- zraněná osoba v objektu,
- bezvládná osoba v kotelně,
- únik plynu,
- dopravní nehoda výjezdové skupiny.

4. Kolik je zraněných osob

- zraněná osoba v objektu,
- bezvládná osoba v kotelně,
- zraněný pracovník výjezdové skupiny.

5. Jaká hrozí rizika

- plyn,
- požár a kouř,
- možnost výbuchu,
- dopravní nehoda.

6. Jaká opatření již byla provedena

- vyslána výjezdová skupina,
- informovány kontaktní osoby,
- přijaté poplachové signály.

Zásady správné komunikace operátora

- **mluvit pomalu a srozumitelně,**
- **používat stručné a jednoznačné věty,**
- **nepředávat neověřené informace,**
- **nezamlčet žádné známé nebezpečí,**
- **potvrdit správnost adresy a kontaktních údajů,**
- **ukončit hovor až po pokynu operátora IZS.**

Stručná odpověď ke zkoušce

Operátor DC musí s IZS komunikovat klidně, přesně a věcně. Sdělí kdo volá, odkud volá, přesnou adresu události, charakter mimořádné události, počet zraněných osob, hrozící nebezpečí (únik plynu, zakouření, požár) a informace o zranění pracovníka výjezdové skupiny při dopravní nehodě. Hovor ukončí až po potvrzení, že IZS obdržel všechny potřebné informace.

Výklad některých zkratk :

BM - Bezpečnostní manažer

CCTV (aktuální ozn. je VSS)– kamerový systém (analogový nebo digitální televizní okruh)

DC – dohledové centrum (PCO, aktuál. ozn. ARC)

DPPC – dohledové a poplachové přijímací centrum

HZS – hasičský záchranný sbor

EZS (angl. I&HAS) – elektronický zabezpečovací systém proti pohybu neoprávněných osob

EPS (angl.FADS) – elektronický protipožární systém

IZS – integrovaný záchranný systém (HZS, Policie ČR, Záchraná zdrav. Služba)

MP – městská policie

MU – mimořádná událost

OOPP – osobní ochranné prostředky

PČR – Policie České republiky

PCO (angl. ARC) – pult centralizované ochrany

PZTS – poplachový zabezpečovací a tísňový systém (tíseň, lékař, požár, únik plynu atd.)

RDST – radiostanice

RZP – rychlá zdravotnická pomoc 155

VS – velitel směny

ZJ – zásahová jednotka

ZZS – zdravotnická záchranná služba

*Vážení uchazeči o zkoušku operátor dohledového centra,
přejeme Vám hodně štěstí u zkoušky.*

Naše motto zní :

„štěstí přeje připraveným“

V Rudolfově 21.6.2006

Ing. Antonín Zahálka – autorizovaná osoba MV ČR

