LUŇÁČEK

Pojednejte o problematice kybernetické bezpečnosti

Definice kyberprostoru

-**Digitální prostředí** umožňující vznik, zpracování a výměnu **informací,** tvořené informačními a komunikačními systémy, a službami a sítěmi elektronických komunikací.

-Těžké definovat, mnoho definic; Nejedná se jen o PC, ale i o chytrá zařízení (mobil, hodinky), chytrou domácnost, průmysl atd.

Definice kybernetické bezpečnosti

=souhrn právních, organizačních, technických a fyzických **opatření**, která umožňují odolávat úmyslně či neúmyslně vyvolaným kybernetickým útokům a zmírňovat či napravovat jejich následky

-Kybernetická bezpečnost zahrnuje činnosti nezbytné k ochraně sítí a informačních systémů, uživatelů těchto systémů a dalších osob dotčených kybernetickými hrozbami.

Kybernetický bezpečnostní incident

-Narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události

-Musí se **nahlašovat** (kdy, kde, kdo, jak, co bylo cílem, co bylo narušeno (triáda), charakter (úmyslné, neúmyslné), překonané opatření, narušené aktivum, pravděpodobnost opakování)

Kybernetická bezpečnostní událost

-Událost je něco, co hrozí a může narušit bezpečnost informací, služeb nebo sítí.

-Neohlašuje se, **detekuje** se

Kybernetický útok

-Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.

-**Úmyslné jednání** člověka prováděné za účelem narušení bezpečnosti informaci v IS

Opatření v oblasti KB

-schopnost zabránit kybernetickým útokům, detekovat je, bránit se jim (odolávat), zmírnit jejich následky

-**prevence** =ochrana před hrozbami
-**detekce** = odhalení neoprávněných (skrytých) činností a slabých míst v systému
-**náprava** = odstranění slabého místa v systému

Oblasti působení hrozeb a rizik KB

-**vojenské** = odposlouchávání, sledování pozic, omezení schopnosti komunikace
-**civilní** = ohrožení obyvatelstva (elektrárny, doprava, komunikace), stabilita státu
-**osobní** = odcizení soukromých dat, financí, poškození počítače, monitorování

Pojednejte o kybernetické bezpečnosti

Definujte pojem kybernetická kriminalita a její aspekty

-**Trestná činnost**, v níž figuruje určitým způsobem:

-počítač jako souhrn technického a programového vybavení (včetně dat),

-nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo připojených do počítačové sítě

buď jako **předmět zájmů** této trestné činnosti, jako **prostředí** a nebo jako **nástroj** této trestné činnosti.

-projevuje se v podobě kybernetických útoků, páchá jí jednotlivec nebo skupina

Sociální inženýrství

-**ovlivňování, přesvědčování či manipulaci** s lidmi s cílem je donutit provést určitou akci, či od nich získat informace, které by jinak neposkytli

-sběr volně dostupných dat, fyzický útok (vydávání se za někoho), psychologický útok

Malware

-Jakýkoliv software využitý k narušení standardní činnosti počítačového systému, zisku informací (dat), či využití k získání přístupu k počítačovému systému.

Internetové pirátství (počítačové) - duševní vlastnictví a autorské právo

-**Kriminalita**, která porušuje práva duševního vlastnictví

-právo duševního vlastnictví = majetek nehmotné povahy, které jsou **výsledkem** tvůrčí činnosti člověka, rozděluje se na **autorská práva** (skladby, filmy) a **průmyslová práva** (patenty, vzory)

-**softwarové pirátství** a **audiovizuální pirátství** (šíření, zveřejnění)

Pojednejte o kybernetických útocích a jaký je mezi nimi rozdíl

Kyberšikana - nebezpečné komunikační jevy (ponižování, nadávání, vyhrožování) realizované prostřednictvím informačních a komunikačních technologií

Kybergrooming - psychickou manipulaci dítěte dospělým prostřednictvím moderních komunikačních technologií s cílem získat důvěru oběti, vylákat ji na osobní schůzku a zpravidla sexuálně zneužít

Kyberstalking - útočník využívá informační a komunikační technologie k dlouhodobému, opakovanému a stupňovanému kontaktování – pronásledování své oběti, ve které chce úmyslně vyvolat pocit strachu o své soukromí, zdraví nebo život

Pojednejte o managementu bezpečnosti

Pojednejte o řízení bezpečnosti (čeho se týká a kdo ji zajišťuje)

-oblast řízení, která řeší **bezpečnost aktiv** (zdrojů) v organizaci (fyzická i elektronická)

-**soustavná, opakující** se sada navzájem provázaných činností, jejíž cílem je zajistit bezpečný provoz a zamezit bezpečnostním rizikům a hrozbám

-je zajišťována **odbornými útvary a odborníky**, primárně je součástí každodenní práce vedoucího zaměstnance a statutárního orgánu

Jaké instituce (úřady) se podílí na ochraně informací v ČR a jaká je jejich působnost

Úřad pro ochranu osobních údajů (ÚOOÚ)

-ústřední správní úřad pro oblast **ochrany osobních údajů** a je nezávislým orgánem

-provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů

Národní bezpečnostní úřad (NBÚ)

-nejvyšší bezpečnostní autorita v oblasti **ochrany utajovaných informací** (OUI)

-zpracovává koncepci rozvoje a zajišťuje jednotné provádění OUI, vede ústřední registry UI v rámci mezinárodních styků, připravuje vládní návrhy zákonů a prováděcích předpisů

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

-nejvyšší bezpečnostní autorita v oblasti **bezpečnosti IS a KS a kryptografické ochrany**

-provádí certifikace, výzkum, vývoj a výrobu kryptografických prostředků

Úloha a místo CERT, CSIRT, CIRC – jejich účel a oblast působení

CERT

-tým, reagující na vyjímečné počítačové **situace**

> **Národní CERT**
>
> -**metodická podpora subjektů**, které projeví zájem o kolektivní ochranu před incidenty
>
> -jeho provozovatel jakožto soukromý subjekt má možnost v situacích **reagovat operativně** a činit vše co není zákonem zakázáno

Vládní CERT

-působící jako součást NÚKIB disponuje **nařizovací a sankčními pravomocemi** a zajišťuje uplatňování státní moci v oblasti kyberbezpečnosti

CSIRT

-tým, reagující na **incidenty** v oblasti počítačové bezpečnosti

-polem působnosti týmu *CSIRT.CZ* je celá Česká republika

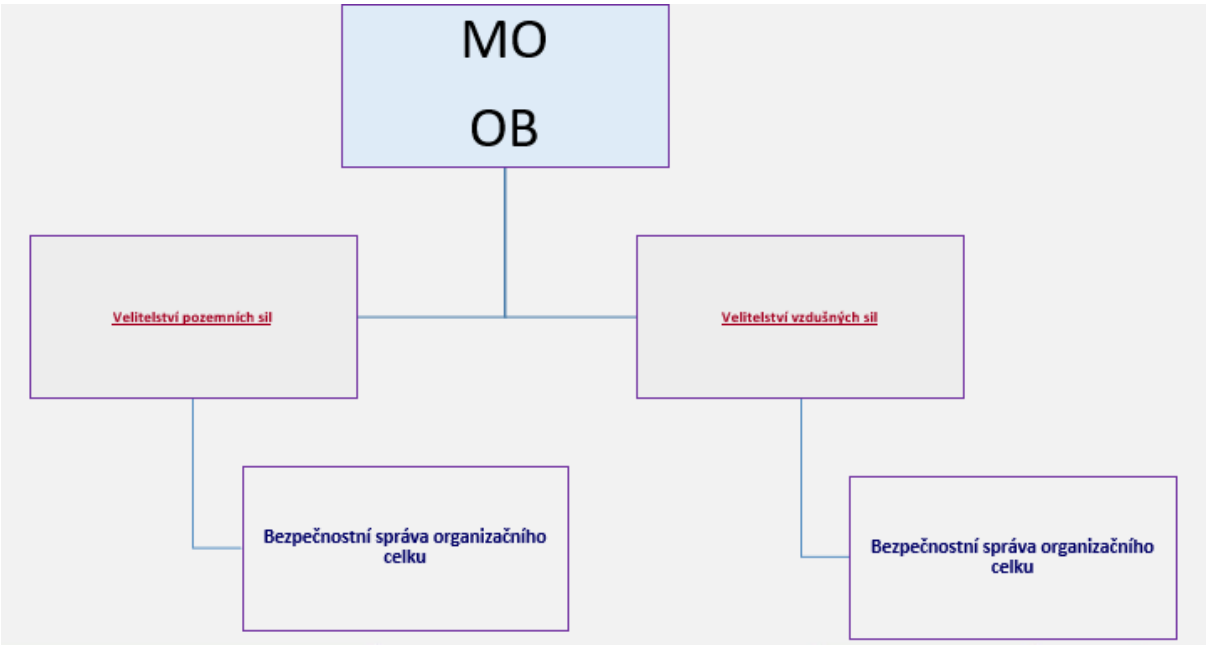
CIRC

-úkolem Centra CIRC je proaktivní identifikace kybernetických bezpečnostních hrozeb a incidentů pomocí **nepřetržitého monitoringu důležitých segmentů** datových sítí resortu MO, a jejich následná analýza, vyhodnocování a reportování relevantním partnerům

-organizační celek VeKySIO

Management bezpečnosti v rezortu MO

Struktura bezpečnostního managementu v rezortu MO – MO…organizační celek



-**hierarchická struktura** organizace bezpečnosti
-odpovědná osoba = **ministr obrany** (odpovídá za rezort MO, za vše co je požadováno)

-Odbor bezpečnosti (OB MO) => organizační útvar MO pro plnění úkolů stanovených z. 412 a 499
-v čele **Bezpečnostní ředitel MO-ředitel odboru** (podřízen ministru obrany)

-**Organizační celek (OC)** a v čele **Vedoucí organizačního celku** (např. rektorka-velitelka)

Bezpečnostní správa KIS (rozdělení na provozní a bezpečnostní správu, role)

-**provozní správa** systému
- -gestor
- -manažer
- -provozovatel
- -správce
- -místní správce

-provozní bezpečnostní správa systému (role vystupují z rolí bezpečnostní správy OC)
- -bezpečnostní správce
  - -místní bezpečnostní správce systému
    - -bezpečnostní správce KO systému
- -bezpečnostní správce terminálové oblasti systému
  - -místní bezpečnostní správce KO systému

Pojednejte o problematice „standardizace – akreditace – certifikace“

Jaká je náplň jednotlivých činností a čím se liší

Certifikace - atestace, **zkoušení**, testování jakosti produktů a služeb, ale i způsobilosti (kompetence) pracovníků realizované v autorizovaných zkušebnách podle daných norem platících v jednotlivých zemích
Akreditace - akreditace má význam pověření, zplnomocnění, **potvrzení**, schválení potřebné úrovně
Standardizace - **definice** charakteristických vlastností zabezpečující, že materiály, výrobky, procesy, služby apod. jsou takové, jaké se zamýšlelo, že mají být

Standardizační instituce základní dělení

ISO(International Organization for Standardization)
- -posláním ISO je standardizace se zaměřením na usnadnění mezinárodního obchodu
- -pole působnosti není omezeno na žádné prum. odvětví/vědní obor
- -pokrývá všechny **technické oblasti** kromě elektrotechnických a elektronických norem, které jsou v působnosti IEC

IEC(International Electrotechnical Commission)
- -vydává normy z oblasti **elektrotechniky, elektroniky a jim příbuzným**

ITU(International Telecommunications Union)
- -hraje vedoucí roli ve správě sektorů **radiokomunikace, telekomunikačního vývoje a standardizace**

Kdo vykonává certifikace pro oblast KIS a krypto a kdo pro fyzickou bezpečnost (technické prostředky)

-KIS a krypto **=> NÚKIB**
-Fyzická bezpečnost (technické prostředky) **=> NBÚ**

-technické prostředky = MZP, EZS, EPS, fyzické ničení nosičů informací atd.

-zjistí-li NBÚ/NÚKIB způsobilost, vydává **certifikát TP (KIS, KO)**
-obsahuje = evidenční číslo, název a typ, identifikace výrobce, identifikace držitele, datum vydání a platnosti, stupeň utajení

-nelze se odvolat při neudělení certifikátu

-**zánik** uplynutím doby, rozhodnutím NBÚ/NÚKIB

Pojednejte o bezpečnostní politice

Účel BP

-**základní východisko** pro řízení bezpečnosti IS organizace (forma **písemného** dokumentu)
-určitý soubor pravidel, **nejvyšší netechnická úroveň** definice obranných mechanismů systému
-definuje **základní postupy a metody** řešení bezpečnostní problematiky
-**redukuje rizika** výskytu nebezpečí

-co chránit, proti čemu a jakým způsobem => analýza aktiv, analýza hrozeb, analýza rizik, návrh protiopatření

Co je obsahem BP

-popis IS
-cíle bezpečnostní politiky
-legislativní východiska
-definice citlivosti informací
-definice hrozeb na IS
-definice bezp. služeb, které má IS splňovat
-zásady personální politiky
-zásady organizační politiky
-technicko-provozní zabezpečení
-politiku zálohování
-plán obnovy po havárii
-metodiku řešení krizových stavů

Druhy BP

-lze rozdělit podle jemnosti konkretizace

-**Státní** -> tvoří ji především zákony (412/2005, 499/2004)
-**Resortní** (podniková) -> v rezortu MO je tvořena především rozkazy, předpisy a normativní výnosy
-**Systémová** -nejnižší a nejpodrobnější stupeň, např. konkrétní IS politika
-zpracovává se globální sys. bez. pol. a následně detailní sys. bez. pol.

Pojednejte o bezpečnostní analýze

-je zaměřena na **vytvoření** komplexních bezpečnostních **protiopatření** vedoucích k celistvé ochraně aktiv organizace
-použijeme obecné schéma bezpečnostní analýzy

Definujte jednotlivé kroky a jejich obsah

1. **Určení bezpečnostní správy organizace**
   -definice týmu specialistů
   -jsou zodpovědní za řízení bezpečnosti organizace
   -vedoucí pracovník týmu určená osoba (MO-bezpečnostní manažer OC)
2. **Stanovení rozsahu analýzy**
   -ohraničení rozsahu analýzy v závislosti na důvěrnost, dostupnost a celistvost
   -musíme si stanovit, jakých cílů chceme v bezp. dosáhnout
   -znaky nastavené úrovně bezpečnosti: nezávislost, řízení, ocenitelnost

3. **Identifikace aktiv**
   a. **lidské zdroje** (osoby podílející se na bezpečnosti organizace)
   b. **procesy** (periodicky prováděné děje)
   c. **informace** (dokumenty)
   d. **majetek** (hmotné a nehmotné statky)
   -aktivum = všechno, co má pro subjekt **hodnotu** (hmotná/nehmotná)
   -provádíme výčet aktiv+jejich ocenění (nízká, střední, vysoká, kritická)

4. **Identifikace hrozeb**
   -hrozba = síla, událost, aktivita nebo osoba, která **může způsobit škodu**
   -zjišťujeme, které jsou reálné a mohou narušit OUI + jejich pravděpodobnost
   -dělíme na: náhodné/úmyslné vnitřní/vnější
   -techniky analýzy hrozeb: strom hrozeb, graf elementárních hrozeb (vrchol grafu hrozba, pod ní 3 vrstvy)

5. **Identifikace a ocenění zranitelnosti**
   -zranitelnost = **nedostatek** analyzovaného aktiva, **stav** kdy se hrozba naplní
   -působením zranitelnosti a hrozby zároveň dochází k **incidentu**

6. **Návrh protiopatření**
   a. **procedurální** (postupy, styl řízení)
   b. **technické** (technické prostředky)
   -protiopatření = postup, proces, procedura, technický prostředek, nebo cokoliv, co je navrženo pro **zmírnění působení** hrozby a snížení zranitelnosti

Pojednejte o bezpečnostní a provozní dokumentaci KIS (náplň a účel zpracování)

-**IS** rozumíme 1 nebo více počítačů, jejich programové vybavení, periferie, správa tohoto IS a procesy nebo prostředeky umožňujcí práci s UI

-**KS** nakládající s UI se rozumí koncové komunikační zařízení - přenosové prostředí - kryptografické prostředky a dále obsluha, provozní podmínky a postupy

-IS i KS musí k používání a nakládání s UI schválit NÚKIB

-globální bezpečnostní dokumentace (**upravuje podmínky** pro nakládání s informacemi v systémech): zákon č. **412/2005** Sb., č. **184/2014** Sb. o KB, č. **110/2019** Sb. o ochraně osobních údajů, vyhlášky NBÚ/NÚKIB/ÚOOÚ, (v resortu ještě rozkazy MO)

Projektová bezpečnostní dokumentace IS

-**obsahuje:** bezpečnostní politiku, návrh bezpečnosti IS, dokumentaci k testům bezpečnosti, vyhodnocení analýzy rizik

-je tvořena souborem norem, pravidel a postupů, kterými se zajišťuje CIA UI

-zpracovává se zejména ve fázích plánování, vývoje, pořízení a implementace IS

Provozní bezpečnostní dokumentace IS

-pro **utajované IS** se zpracovává provozní bezpečnostní dokumentace **v plném rozsahu**

-pro **neutajované IS** se vyžaduje zpracování provozní dokumentace, která zahrnuje **základní opatření** pro zajištění bezpečnosti

-**obsahuje:**

- **-bezpečnostní směrnice IS**, které předepisují činnost **bezpečnostních správců IS** v jednotlivých rolích zavedených v IS pro zajištění bezpečnostní správy IS
- -**bezpečnostní směrnice IS**, které předepisují činnost **správců IS** v jednotlivých rolích zavedených v IS pro správu informačního systému
- -**bezpečnostní směrnice IS**, které předepisují činnost **uživatelů IS**

Projekt bezpečnosti KS

-**obsahuje:** bezpečnostní politiku KS, organizační a provozní postupy, provozní směrnice pro bezpečnostní *správu* KS, provozní směrnice *uživatele* KS

KOZAK

Role kryptografie v ochraně informací

-Kryptografie se používá k ochraně informací tím, že ji šifruje a umožňuje tak tak její bezpečný přenos nebo uložení

-Potřeba ochrany informací **vznikla kvůli:** schopnosti a potřebě ukládat informace, vytváření velkých státních celků, rozvojem společnosti, komunikace na stále větší vzdálenosti

-**Steganografie** je předchůdce kryptografie, zabývá se utajením komunikace prostřednictvím ukrytí zpráv

-**Hash funkce** = ověření digitálních podpisů a datové integrity (porovnávání otisků)

Proudové šifry

-**symetrická** šifra; datový tok je **kombinován** tokem **pseudonáhodné** posloupnosti
-používá se funkce **XOR**
-výsledkem je **zašifrovaný datový proud**
-dochází k neustále se měnící transformaci (u blokové šifry transformace konstantní)
-proudové šifry typicky **rychlejší** než **blokové,** ale náchylnější ke kryptoanalytickým útokům
-typicky chybné použití => počáteční stav nesmí být použit dvakrát

-pracují s **bitovými** (bajtovými) **proudy** => šifra při každém šifrování transformuje jeden stejný bit otevřeného textu do různých bitů šifrovaného textu

-využívá se klíč **pevné délky** (nejčastěji 128 bitů) vyráběný pseudonáhodným generováním bitů
-používají se v **systémech přenosu proudů informací** (začátek a konec přenosu kdykoli)
-vhodné pro šifrování **nepřetržitých proudů dat** (hlas, video)

-čím více se výstup generátoru klíčů blíží k náhodnému generátoru, tím delší prolomení
-**chyba počátečního stavu** = při zapnutí vytváří generátor jeden a týž bitový proud

Skramblování (změna bitů pomocí XOR)

-nejjednodušší realizace, procházejícímu datovému proudu se paralelně generuje klíčový proud
-problémem je **synchronizace** přenášejícího a přijímajícího zařízení (při vynechání nebo špatném vložení jednoho bitu synchronizace se veškerá informace ztrácí)
-řešení **přidáním předem známe syn. značky** nebo **pomocí vysoce přesných generátorů**
-po určité době se začne bitová kombinace **opakovat** (N bitů, 2N kombinací, max 2n-1 cyklů)
-nestabilita vůči falzifikace

Synchronní proudové šifry

-proud klíčů se generuje nezávisle na proudu zprávy
-při šifrování generátor proudu klíčů vydává neustále bity proudu klíčů
-při dešifrování druhý generátor vydává identické proudy, oba generátory **musí být synchronizovány** (po chybě při přenosu bude každý symbol nesprávně rozšifrován)
-příjemce i odesílatel musí pracovat synchronně, při ztrátě se hledá hodnota posunu
-generátor proudu klíčů musí mít **mnohem delší periodu** než velikost otevřeného textu
-pro zlepšení synchronizace se vkládají **synchronizační značky** (ne cyklicky)
-vsuvka nebo odstranění symbolu v šifrovaném textu způsobí porušení synchronizace

Samosynchronizující proudové šifry

-každý bit proudu klíčů je funkcí **n** počtu **předcházejících bitů** šifrovaného textu
-dešifrující generátor proudu klíčů se automaticky synchronizuje s šifrovacím generátorem pomocí přijetí **n bitů** šifrovaného textu
-slabou stránkou je šíření chyby (každý nesprávný bit **n nesprávných bitů** proudu klíčů)

-většina proudových šifer založena na **lineárních posuvných registrech se zpětnou vazbou / posuvných registrech se zpětnou při přenosu**
-počet bitů definován délkou posuvného registru
-nový krajní levý byt funkcí všech ostatních bitů registru
-**lineární** = zpětná vazba XOR některých bitů registru (bity odváděcí posloupnosti)
-**při přenosu** = bity odvádějící posloupnosti sčítány jeden s druhým a s obsahem registru

Blokové šifry

-**symetrická** šifra pracující s bloky **pevně stanovené délky** (např. 128 bitů)
-pokud je dat více, rozdělí se výplň na více bloků, přičemž zbylé místo v posledním je vyplněno
-při (de)šifrování je každý blok **transformován** pomocí šifrovacího algoritmu utajeným klíčem
-hlavní slabinou je opakované použití stejného klíče na všechny bloky
-přípustné operace = součet, XOR, vynásobení podle modulu, bitové posuny

-pro odstranění této nevýhody se používají **provozní režimy**
-použije se další proměnný parametr na vstupu (**inicializační vektor**) => zašifrovaná data vypadají jako náhodná sekvence
-rázem se **bloková** šifra chová jako **proudová**

-první bloková šifra -> **DES (Data Encryption Standard)**, nástupce **AES (Advanced E. S.)**

Typy algoritmů:
-**substituční** = samotné bloky informací se **mění** podle zákonů algoritmu, většina algoritmů
-**přestavující** = bloky informací (bajty, bity) se samy od sebe **nemění**, mění se pořadí/poloha ve srovnání s původní zprávou

-kryptografické transformace **nezvětšují** objem informace, pokud ano, je neoptimální algorit.
-zmenšení objemu je možné pouze kompresními mechanismy
-dříve se měnily symboly, dnes bity; dobré algoritmy stále **kombinují** substituci a transpozici

Substituční šifry

-každý symbol v otevřeném textu se v šifrovaném nahrazuje jiným symbolem
-příjemce invertuje substituci

-jednoduchá sub. šifra (monoabecední šifra) = jeden symbol nahrazuje jeden symbol
-homofonická sub. šifra = jeden symbol nahrazuje několik symbolů
-polygramová sub. šifra = bloky symbolů nahrazují taktéž bloky symbolů
-polyabecední sub. šifra = více monoabecedních šifer spolu, každý znak podle jedné šifry
- používají se množstevní jednopísmenné klíče (1. symbol 1. šifra, 2. symbol 2. šifra, …)
- po použití všech klíčů se cyklicky opakují = **perioda šifry**

Přestavující šifry

-např. **jednoduchá sloupcová přestavující šifra** (otevřený text napsaný horizontálně o fixované šířce a šifrovaný text se odečítá vertikálně)

Výhody:
-možnost opakovaného použití jednoho klíče
-libovolná velikost zpracovávaného textu
-možnost modifikace klíče bez úpravy algoritmu

Nevýhody:
-koeficient množení chyby je roven délce bloku
-jedna chyba v šifrovaném textu vyvolá zkreslení asi **poloviny** otevřeného textu
-blokovost šifrování = dva stejné otevřené bloky dají dva stejné bloky šifrovaného textu
-výrazně **nižší** rychlost oproti proudovým šifrám

Základní matematické postupy v kryptografii

1. **Funkce** (surjekce, injekce, bijekce, inverze)
2. **Operace nad množinou**
    a. permutace -> počet možností přeskupení množiny
3. **Teorie čísel** (dělitelé, NSD, NSN, provočísla, modulo = zbytek po dělení)
4. **Konečná tělesa** - kryptografie na bázi eliptických křivek
5. **Euklidův algoritmus** -> nalezení společného dělitele pomocí zbytku po celočíselném dělení + inverzního prvku
6. **Složitost** - horní odhad složitosti
    a. časová = funkce, která každé množině dat přiřazuje počet oprací
    b. paměťová = závislost paměťových nároků algoritmu vzhledem k datům
7. **Eliptické křivky**
    -eliptická křivka poskytuje jedinečný způsob jak vytvořit dva klíče - **veřejný a soukromý** - které jsou matematicky propojené, ale neinvertovatelné
    -dále -> **faktorizace celého čísla, testování prvočíselnosti**
    -kvůli matematické obtížnosti je většina útoků na eliptické křivky velmi obtížná

Určování prvočísel

-prvočísla využíváme na použití dvojice klíčů veřejný-privátní
-nejjednodušší generování velkého prvočísla = **vygenerovat kladné liché a otestovat**

1. **Algoritmus Trial division**
   -využívá zkušební dělení
   -neomylný, efektivní pro malé hodnoty
   -dělení čísla ***n*** všemi ***m*** kde ***1<m<n*;** pokud vyjde něco beze zbytku, ***n*** není prvočíslo
   -vylepšení = dělí se pouze ***m*** **<** √***n***, vynechání **sudých** čísel, dělí se pouze **prvočísly**
2. **Wheel Factorization**
   -není dokonale spolehlivý, není třeba znát všechna prvočísla až do √n
   -nejdříve se dělí nekolika **prvními *k* prvočísly**, pak čísly nesoudělnými s ***k*** prvočísly do √n
3. **Pravděpodobnostní testy**
   -jsou efektivnější
   -vygenerování lichého kandidáta, otestování zda je prvočíslo, pokud ano tak znovu
   a. Fermatův test - vychází z malé Fermatovy věty a schopnosti efektivního modulárního umocňování
   b. Miller-Rabinův test- vytváří se tzv. kvadratický zbytek
4. **Testy dokazující prvočíselnos**t
   a. Lucas-Lehmerův test - pro speciální Mersennova čísla

Metody kryptoanalýzy

Kryptoanalýza = věda, která se zabývá prolomením šifer

Monoalfabetická substituční šifra
-u monoalfabetických substitučních šifer je založena na **porovnávání četnosti** výskytu znaků v textu a obecné platné četnosti znaků (v českém jazyce nejvíce písmeno o)

Postup frekvenční analýzy:
-**určíme četnos**t znaků v zašifrovaném textu
-předpokládáme, že **nejvyšší** četnost v šifrovaném textu je nejvyšší četnost českého znaku
-soustředíme se i na **stavbu výrazů** (za - většinou následuje li => máme další dva znaky)
-vybereme slova co obsahují **co nejvíce již známých** písmen
-zjistíme slovo které by **"mohlo"** vzniknout a **doplníme** podle něj neznámá písmena
-postup **opakujeme**, doplňujeme známá písmena a odhalujeme neznámá tak dlouho dokud nemáme celý text

-čím je text delší, tím více odpovídá četnosti znaků
-problém je, že některé hypotézy slov mohou být špatné => je potřeba ověřovat dalšími slovy

Historický vývoj postupů utajování

Období klasické kryptografie

-vyvíjejí se postupy, není založena na specializovaných zařízeních
-počátky už za Řecko - Perských válek

Lingvistická steganografie = předem domluvené znaky, slova textu
Technická steganografie = technologické postupy, fyzické ukrytí zprávy

-např. psaní na bílek, tetování na hlavu otroka

Utajování zpráv = převod do podoby, která je čitelná jen se speciální znalostí
-vzniká tak obor **kryptografie**

-Kryptologie zahrnuje kryptografii a kryptoanalýzu

-**Caesarova šifra** = monoalfabetická substituční šifra, nahrazuje symbol 3. následujícím symbolem v abecedě
-**Albertiho šifra** = polyalfabetická substituční šifra se dvěma abecedami
-**Viginèrova šifra** = symetrická polyalfabetická substituční šifra, využívá viginèrův čtverec
-**Vernamova šifra** = v principu nerozluštitelná, posun každého znaku o náhodně zvolený počet míst v abecedě

Kombinované šifry - nevýhody šifer je možné částečně odstranit kombinací různých šifer

Moderní kryptografie

-1. polovina 20. století - vývoj sofistikovaných zařízení pro utajování

-nárůst objemu informací, efektivnější přenosy informací, pro utajování se využívá specializovaný HW i SW
-šifrování strojem přineslo zcela nové možností - velký počet operací v krátkém čase, stroje narozdíl od humanoidní obsluhy nemluví

Enigma - název zařízení i algoritmu, správné použití odolává i dnes, využívala rotory
-Meziválečný rozvoj bankovnictví, propojení ekonomik Evropy a USA
-Přenos citlivých informací telegrafem, mezikontinentální spojení podmořskými kabely

Digitální steganografie = změnila podobu s rozmachem informačních technologii
-např. schování zprávy do šumu v souborech se zvukem, obrázky, videi
-v obrázcích manipulace s nejméně významným bitem v každé osmici RGB

Orwellian printers = žluté tečky viditelné pod modrým světlem

Steganografie v IP datagramu = využití flag fieldu (3 bity v záhlaví)

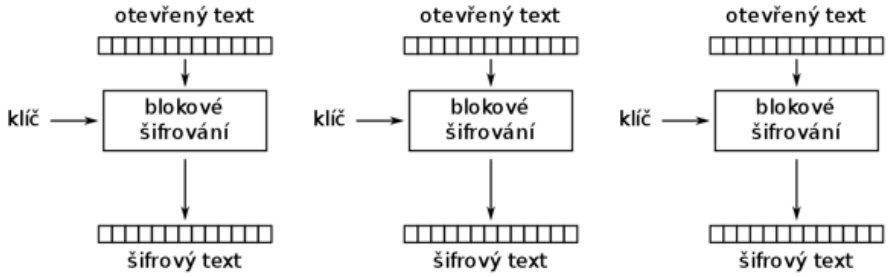
Kvantová kryptografie = dvě přenosové cesty (klasická + skrytá kvantová pro klíč)

Pracovní režimy blokových šifer

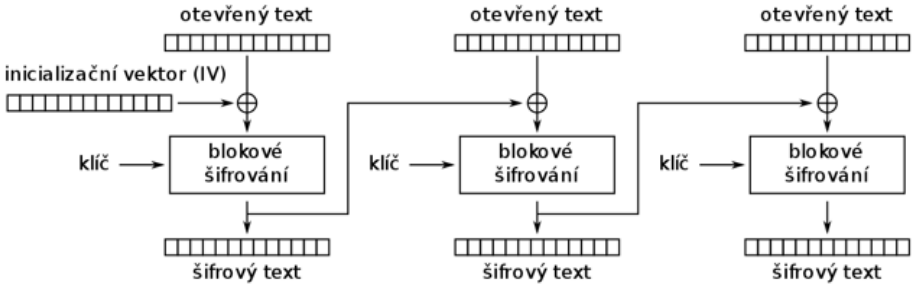
Pracovní režim (operační mód blokové šifry)
-**způsob**, kterým je bloková šifra používána (především pro umožnění bezpečného šifrování **textů delších** než blok šifry)

-umožňuje bezpečné opakované užití stejného klíčů
-většina režimů používá kromě klíče **inicializační vektor =>** jedinečný náhodný soubor bajtů o délce blokové šifry, předcházíme stejnému šifrovému textu použitím stejného klíče

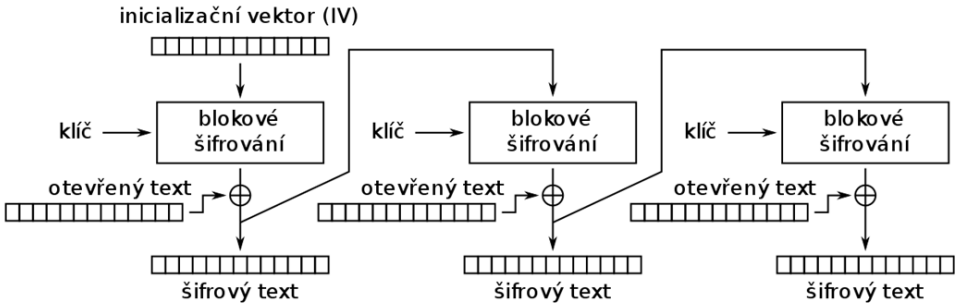
ECB - režim kódové knihy
-základní režim
-šifra se **přímo** aplikuje nezávisle na jednotlivé bloky
-při daném klíči blok šifrového textu odpovídá bloku otevřeného textu
-při používání na šifrování protokolu s pevně danou délkou, lze po jisté době rozlišovat obsah
-přenesení bloku s šifrou nemá vliv na dešifrovatelnost jiných bloků
-jednoduchý, ale v moderní kryptografii se **nepoužívá**



CBC - řetězení šifrových bloků
-každý **následující** blok je **xorován zašifrovaným předchozím** blokem (první blok xorován inicializačním vektorem)
-nevýhodou je, že šifrový blok závisí na všech předcházejících (poškozením šifrového bloku nelze dešifrovat blok přímo následující), i tak se ale široce **používá**
-šifrování nelze paralelizovat, dešifrování ano



CFB - šifrová zpětná vazba
-velmi podobný CBC, prohazuje pořadí operací
-**zašifruje se předchozí** šifrový blok a **s výsledkem xoruje otevřeny blok**
-šifrování paralelizovat nelze, dešifrování ano
-poškození šifrového bloku znemožní dešifrování bloku **samého a následujícího**, další nepoškozeny



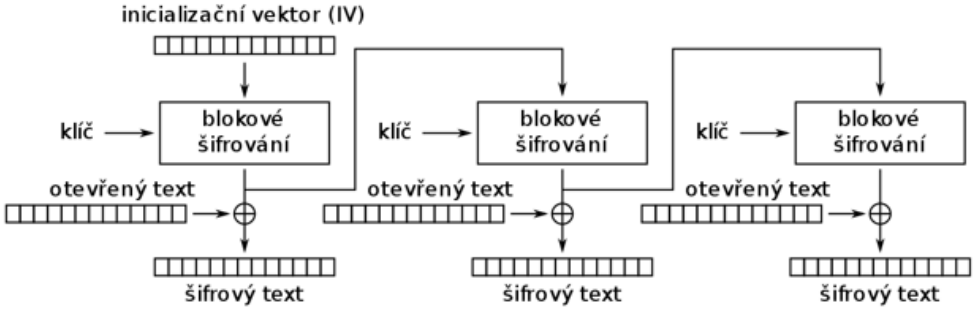
Šifrování v režimu šifrové zpětné vazby (CFB)

OFB - výstupní zpětná vazba

-převádí blokovou šifru na šifru proudovou

-šifrování probíhá pouhým **xorováním otevřeného bloku klíčem předchozího bloku zašifrovaným blokovou šifrou**

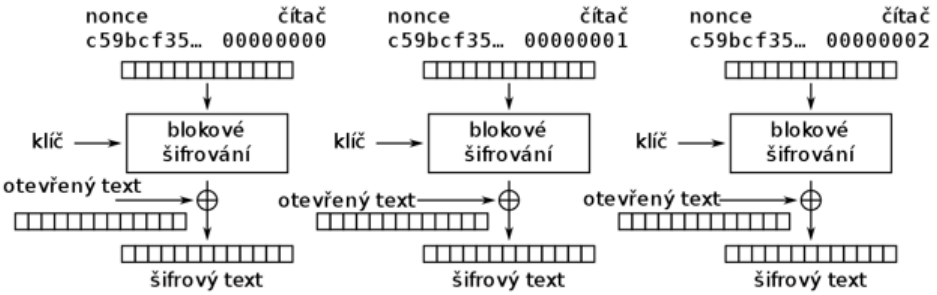
-první blok klíče získán zašifrováním inicial. vektoru



CTR - čítačový režim

-převádí blokovou šifru na proudovou

-klíč, se kterým se **blok otevřeného textu xoruje** se získává **zašifrovaním čítače**, který se každou iterací zvětšuje o pevně danou hodnotu (obsah čítače nastaven inicial. vektorem)



HALOUZKA

Pojednejte o legislativě (z. 412/2005, vyh. 528/2005) z oblasti fyzické bezpečnosti (znát základní pojmy). Rozdíl mezi PFB pro objekt kategorie V a D.

Utajovaná informace (UI)
-informace v jakékoliv **podobě** na jakémkoliv **nosiči označena** v souladu se zákonem 412/2005 Sb. jejíž vyzrazení nebo zneužití může **způsobit újmu** zájmům ČR nebo může být pro tento zájem **nevýhodné** a je uvedena **v seznamu** utajovaných informací

-**zpracovává/ukládá** se v zabezpečpečné oblasti příslušné **kategorie** nebo vyšší (případně v trezoru, uzamykatelné skříni za podmínek stanovených prováděcím právním předpisem)

Zabezpečení ochrany utajovaných informací
-určují se objekty, zabezpečené oblasti a jednací oblasti

Objekt = budova nebo ohraničený prostor kde se nachází zabezpeč. nebo jednací oblast
Hranice objektu = plášť budovy, fyzická bariéra nebo jinak viditelně vymezená hranice
Hranice ZO nebo JO = stavebně nebo jinak viditelně ohraničený prostor

Zabezpečená oblast (ZO)
-ohraničený prostor v objektu, kde dochází k ukládání UI
-kategorie = PT, T, D, V
-třídy podle možnosti přístupu k UI:
- -**třída I.** = vstupem do oblasti **dochází** k se seznámení se s UI
- -**třída II** = vstupem do oblasti **nedochází** k se seznámení se s UI
- -v odůvodněných případech s písemným souhlasem lze **změnit třídu I na třídu II**

-kontrolní opatření na vstupu a výstupu = ostraha, režimové opatření, technické prostředky

Jednací oblast (JO) = ohraničený prostor v objektu určený k projednávání T a PT informací

Ostraha = zajišťuje se nepřetržitě v objektu se ZO

Hrozba = možnost vyzrazení nebo zneužití UI při narušení fyzické bezpečnosti

Riziko = pravděpodobnost, že se určitá hrozba uskuteční

Mimořádná situace = stav, kdy **bezprostředné hrozí**, že dojde k vyzrazení/zneužití UI

Režimové opatření = stanovuje **oprávnění** osob a dopravních prostředků pro vstup a vjezd do objektu, ZO a JO

Technické prostředky = bezpečností prvek jeho použitím se zabraňuje, ztěžuje, omezuje nebo zaznamenává narušení ZO nebo JO nebo ničí UI

Uschovný objekt = trezor nebo jiná uzamykatelná schránka stanovená v příloze č.1

Technické zařízení = vojenský materiál (elektronický, chemický, fotochemický, optický, mechanický - výstroj a technika) který obsahuje utajovanou informaci

Rozdíl mezi PFB na úrovni V a D

-**V** obsahuje:
  -určení objektu a zabezpečených oblastí včetně hranic a určení kategorií a tříd ZO
  -způsob použití opatření fyzické bezpečnosti
-**D (+ T, PT)** obsahuje:
  -vše co obsahuje V + vyhodnocení rizik, provozní řád objektu, plán zabezpečení objektu a ZO v krizových situacích

Pojednejte o mechanických zábranných systémech – obecně význam MZS, průlomová odolnost, bezpečnostní třídy, cylindrické vložky, bezpečnostní dveře a bezpečnostní mříže. Jaký je význam MZS při zabezpečení objektů.

Význam MZS

-základ každého zabezpečení
-bezpečnostní dveře, vrata a stavební kování, mechanické závory, trezory a trezorové skříně, zavazadla na přepravu cenin, okna

Průlomová odolnost

-hranice definovaná určitým **odporem proti destrukčnímu narušení** pachatelem
-odolnost je dána počtem **odporových jednotek** (RU) určenými na zakladě typových fyzických zkoušek za použití optimální kategorie nástrojů

-Koeficient rizikovosti **R = $T_{vloupaní}$: ti** **R > 1**
  -R = koeficient rizikovosti
  -T = doba průlomové odolnosti
  -ti = doba příjezdu policie

-Aby měla ochrana účel musí být hodnota koeficientu větší než 1
-Minimální čas potřebný k překonání je u bezpečnostní třídy určen normou EN 1627

Bezpečností třídy dle EN 1627

1) základní ochrana
2) zvýšená ochrana
3) vysoká ochrana
4) velmi vysoká ochrana
5) nadstandardně vysoká ochrana
6) speciální nadstandardní ochrana

Cylindrické vložky

-hlavní součástí běžných dveřních a visacích zámků
-válec s **otvorem** pro klíč**, stavítky a blokovacími kolíky různé výšky** a **uzamykacím nosem**

-zuby klíče posouvají stavítka a blokovací kolíky do optimální polohy, v níž se může **válec cylindrické vložky** volně otáčet
-hrot klíče pak vysune kovovou spojku, kterou se vložka propojí se zubem, ten se zapře do pně závory a může jí pohybovat
-zub **dlouhý** -> vložku brzdí **stavítko**
-zub **krátký** -> vložku brzdí **blokovací kolík**

-mezistavítko vložené mezi stavítko a blokovací kolík -> vložka lze otočit ve 2 různých polohách stavítka -> možnost vytvořit i generální klíč, který může otevřít více různých zámků

Bezpečnostní dveře

-souhrn spec. stavebních, technických a bezpeč. prvků a uprav dveřního prostoru
-základ tvoří **rám** z tvrdého dřeva, ve kterém je uložen **x-bodový bezpečnostní zámek** s vnitřním rozvorovým systémem
-dveře mohou obsahovat **výplň** s požární odolností a ocelovou mříží proti průniku
-využívají **bezpečnostních závěsů** se zesíleným hřebenem proti vysazení
-součástí mohou být **aktivní čepy** pro zvýšení bezpečnosti

Části dveří:
Zárubeň:
-rámová konstrukce sloužící k zavěšení dveřního křídla
-překonání pomocí jejich roztažení

Závěsy
-jsou součástí jak zárubně, tak dveřního křídla
-slouží k otáčení dveří
-zárubně musí být řádně ukotveny, aby je nešlo vypáčit

Dveřní křídlo
-musí být, tuhé a nesmí se působením vnější síly v žádném místě pohnout -> znemožnění nasazení páčidla

Dveřní zámek
-zabezpečovací zařízení ovládané klíčem a pojištěné závorníkem, jedním a více stavítky nebo zábranami

Cíl konstrukce bezpečnostních dveří:
-zesílení pevnosti dveřního křídla proti proražení, prořízntutí a jiným způsobům páčení
-rozšíření počtu uzamykacích míst po celém obvodu
-vybavení uzamykatelnými systémy odolnými proti všem způsobům překonávání
-vyztužit/zesílit zárubně

Bezpečnostní mříže

-Používají se k **zabezpečení prosklených otvorových výplní** proti násilnému vniknutí do chráněného objektu.

Dělení:
Dle konstrukce:
-Pevně kotvené
-Odnímatelné
-Otevírací
    •Otočné
    •Sklopné
    •Posuvné
        -Pevné
        -Nůžkové
-Rolovací
    •S průhledným výpletem
    •S neprůhledným výpletem

Dle umístění:
-Vnější
    •Ploché
    •Předsazené
-Vnitřní
-Meziokenní

Podle materiálu:
-Ocelové
-Duralové

Podle ovládání:
-Ruční
-Elektrické

Konstrukce mříží
-tuhá, stabilní
-ve své ploše se nesmí dát prohnout a pruty dát roztáhnout
-spoje prutu a příčníku jsou svařeny v celek
-u posuvných nůžkových mříží spojují pruty a nůžky nerozebíratelné čepy
-doporučená velikost oka 15x15cm, min průřez tyče 1cm²

Ukotvení pevných mříží
-ovlivňuje jejich stabilitu
-technicky nejjednodušší

Způsoby ukotvení mříží
-přímé = kotvící tyče jsou rovné a zapuštěné rovnoběžně se stěnou
-kolmé = kotvící tyče jsou na konci ohnuty do pravého úhlu a zasazeny do čela zdi

Závěsy a uzamykací systém mříží
-Nedílná součást mříží
-Závěsy musí být masivní a zajištěné proti uražení, odřezání, vysazení
-Pokud použiju visací zámek -> musí být odolný proti uražení, přeštípnutí či přeřezání a musí mít vytvrzené třmeny (průměr 12 mm)

Pojednejte o systémech EKV.

Přístupový systém (ACS)

=soubor opatření (režimová, fyzická, technická) k zajištění řízení a evidence přístupu do zabezpečeného objektu nebo prostor na základě jednoznačně přidělených práv

-**základní funkce:**
- -identifikace
- -zpracování dat
- -ovládání přístupového místa
- -programovatelnost
- -stavová hlášení
- -komunikace (ostatní systémy)
- -styk s uživatelem (opticky, akusticky)
- -napájení
- -samoochrana

-**přístupový bod** = uspořádání všech prvků, které umožní **kontrolovaný přístup**
- -místa přístupu (dveře, turnikety)
- -rozhraní místa přístupu (řídící jednotka - ovládání otevření)
- -snímače místa přístupu (čtečka, klávesnice, biometrie)
- -APAS (ovládací prvky a senzory)

-**struktura přístupového systému**
- -jeden nebo více přístupových bodů
- -hlavní řídící jednotka
- -napájení
- -komunikační síť
- -řídící a obslužné pracoviště

-**rozdělení identifikačních prvků** (3 způsoby = něco co známe, něco co máme, námi)
- -manuální =pasivní a vyžadují vstup (vypínače, kódové zámky)
- -čipové = identifikátor v integrovaném obvodu (kontaktní, bezkontaktní, kombinované)
- -magnetické (karty s magnetickým proužkem)
- -optické (laserové nebo CCD čtečky)
- -radiofrekvenční (bluetooth identifikace)
- -biometrické (papilární linie, oční duhovka, 3D model obličeje, DNA)

Biometrie

-vychází z předpokladu, že některé charakteristiky člověka jsou **jedinečné a neměnné**

Nejpoužívanější:
-otisk prstů
- -optické
- -kapacitní
- -ultrazvukové
- -teplotní

-otisk sítnice
-oční duhovka
-obličej

Popis základních principů detektorů EZS. Detektory typu NO a NC. Ústředny EZS.

Základní principy detektorů EZS

=vyhlášení poplachu v případě napadení prostoru, který EZS střeží
-komplex vnitřních a vnějších **technických prostředků** (ústředna, zdroj elektrické energie, poplachové smyčky, zařízení k aktivaci a deaktivaci systému, detektory, signalizační zařízení)

Detektory EZS - PIR (pasivní infračervené)
-detektor reagující na **pohyb** v chráněném prostoru, základem je **pyroelektrický senzor**

-principem metody pasivního snímání je detekce **přítomnosti infračerveného záření**, které narušitel vyřazuje

-senzor je uzpůsoben tak, aby pouze registroval tepelné záření charakteristické pro člověka – **okolo 36°C (9,4 μm)**

-celý střežený prostor je rozdělen pomocí segmentace na **aktivní a neaktivní zóny** (pomocí Fresnelovy čočky)

Detektory EZS - Mikrovlnné
-mikrovlnné záření se snadno pohltí okolními objekty nebo se od nich odráží

-mikrovlnné záření je charakterizováno:
-frekvencemi **f = 0,3 - 300 [GHz]**
-vlnovými délkami **λ = 0,001 – 1 [m]**

Metoda Fresnelovy zóny
-fyzikálním principem činnosti je **změna energie** přijímací antény mezi vysílací a přijímací parabolickou anténou

Metoda Dopplerova jevu
-vysílací anténa emituje mikrovlnný signál, který je přijímán anténou přijímací
-podstatou detekce pohybu je **narušení** Fresnelovy zóny

Detektory EZS - Kombinované
- Kombinovaný pohybový detektor s detektorem tříštění skla
  - oba detektory mohou vyhodnocovat poplachové události společně, nebo nezávisle na sobě
- Kombinovaný pohybový detektor PIR s mikrovlnným detektorem
  - k vyhlášení poplachu dojde pouze v případě, že obě detekční části vyhlásí poplachový signál současně
  - zvyšuje se spolehlivost detekce a snižuje se náchylnost k planým poplachům

Detektory EZS - Kontakty otevření
- kontaktní detektor, který slouží k plášťové ochraně objektů na hlídání otevření dveří, oken atd.
- funkce magnetického kontaktu je založena na principu jazýčkového relé spínaného magnetickým polem permanentního magnetu
- nejjednodušší provedení magnetického detektoru je založeno na tzv. Reedově senzoru

    - ten je tvořen dvěma vzájemně se překrývajícími jazýčkovými kontakty, které jsou uloženy a zataveny ve skleněné baňce z olovnatého skla průměru 2 až 4 mm a délky 15 až 40 mm

Detektory EZS - Detekory tříštění skla

- rozbití skla ma typický průběh akustického signálu, doprovázené rozbitím nebo tříštěním skla
- fáze rozbit:
    - 1. fáze - úder a následný průhyb skleněné tabule
        - doprovazený nízkofreknčním zvukem(100-300Hz) s vysokou akustickou energií
    - 2. fáze - praskání, lámání a tříštění skla
        - vzniká akustická vlna s menší energií, ale vysokou frekvencí
        - trvá déle než první fáze
- rozdělení:
    - pasivní detektory
        - detekce tříštění a lámání skla pomocí kontaktního snímače s vodivou fólií
        - tlaková vlna se šíří po povrchu skleněné tabule a je detekována piezoelektr. detektroem
        - akustická vlna je detekována akustickým detektorem
    - aktivní detektory
        - ultrazuvkové
        - infračervené
    - v obou případech jsou vyhodnocovany vibrace chráněné sleněné plochy na zakládě odrazu vlnění vyslaného detektorem k chráněné ploše

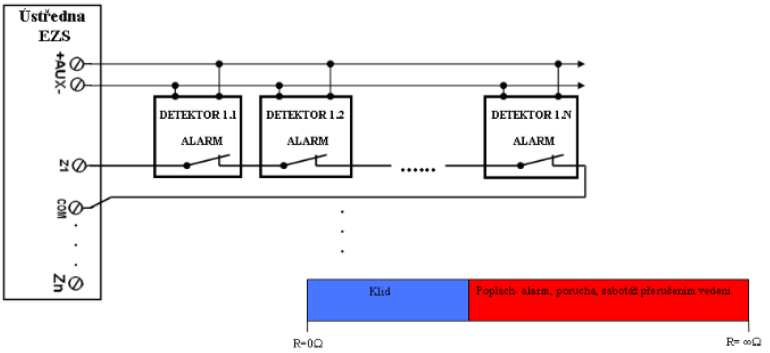
Detektory EZS - Otřesové detektory

- slouží ke střežení úschovných objektů a zdiva používá seismické detektory
- při použití nářadí se generuje vlnění, které zachytí piezoelektricko-keramickému senzoru umístěném na UO
- mechanická konstrukce umi rozeznat nežadoucí zvuky prostředí od zvuků narušitele
- detektory jsou odolné proti sabotáži
- senzor rozpozná:
    - odvrtávání
    - rozřezávání
    - řezání plamenem
    - mechanické údery

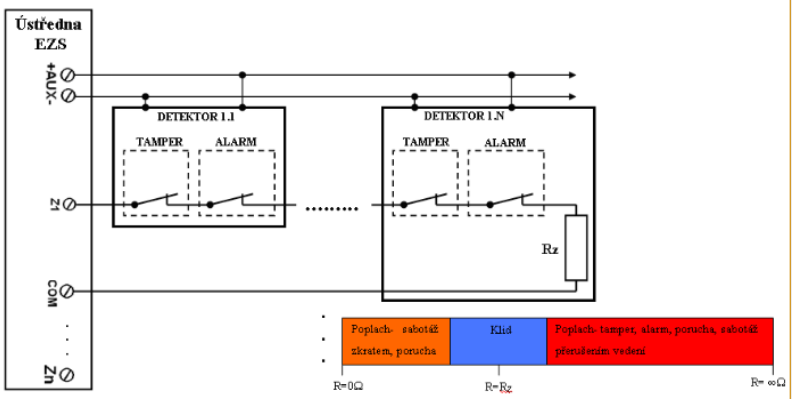
Detektory typu NC

-Kontakty v detektoru jsou v klidovém stavu sepnuty a při narušení objektu detektor rozepne kontakt a vznikne poplach (jedná se tedy o rozepínací kontakt)
-rozdělení NC:

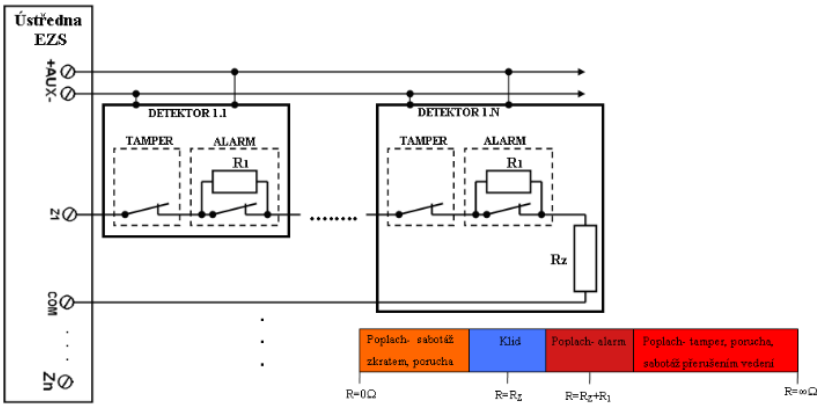
- **NC (normally closed)**



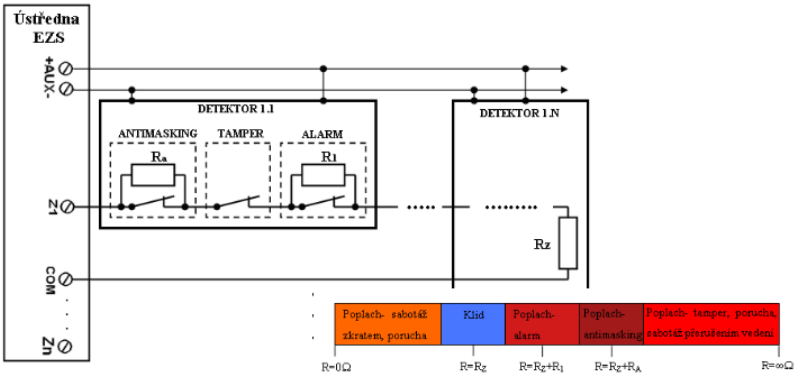
- **NC jednoduše vyvážená**



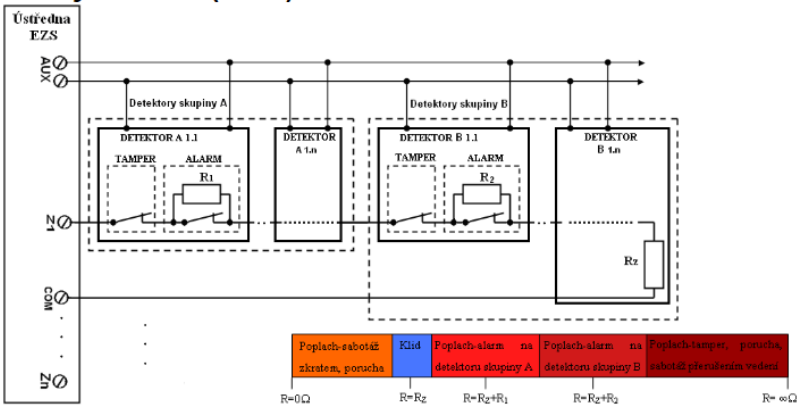
- **NC dvojitě vyvážená**



- **NC trojitě vyvážená**



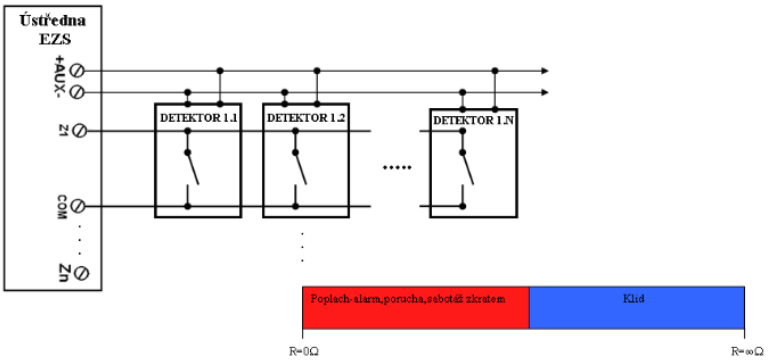
- **NC zdvojení zón (ATZ)**



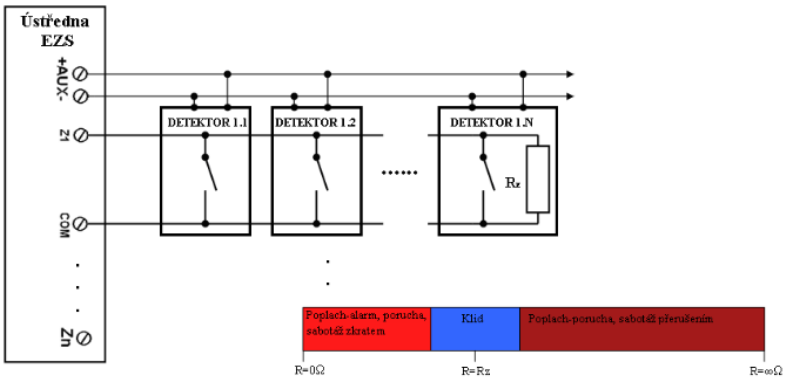
Detektory typu NO

-jedná se o spínací kontakty, které jsou ve stavu „klid“, jestliže jsou kontakty v detektoru rozepnuty. Stav „poplach“ nastane v případě, že se některý kontakt v detektoru sepne.
-rozdělení NO:

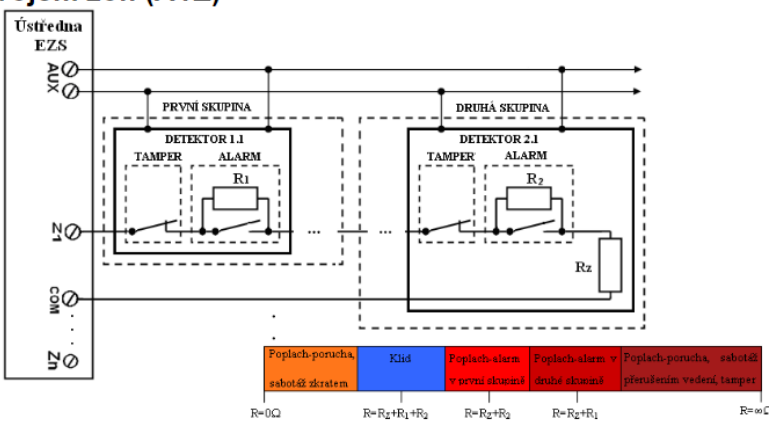
- **NO (normally opened)**



- **NO jednoduše vyvážená**



- **NO zdvojení zón (ATZ)**



Ústředny EZS

- rozdělení dle EZS(ČSN EN 50131-1)
  - drátové
  - bezdrátové
  - sběrnicové
  - kombinované
  - systémové prvky

Drátové ústředny

- každá poplachová smyčka přip. na samostatný vyhodnoc. obvod ústředny
- smyčka -
  - skupina detektorů propojené společným vedením na vstup ústř.
  - je zakončená odporem umístěným na konec vedení v posledním detektoru
-

Smyčkové ústředny(analogové)

- detektory se připojují sériově nebo paralelně dle naprogram. ústředny a typu detektorů
- princip
  - měření hodnoty odporu každé smyčku a při poklesu o více než 30% vyhlásí ústředna poplach

Sběrnicové ústředny

- využívají digit. adresné komunikace pro dat. mezi detektory a ústřednou
- ústředna je s každým detektorem propojena 4 vodiči
  - svorky RED a BLK - napájení
  - svorky GRN a YEL - komunikace
- každý detektor má komunikační modul
- ústředna periodicky aktivuje adresy jednot. detektorů a zkoumá odezvu
- hlavní ochrana proti sabotáži - detektory mají jedinečnou adresu v digit. komunikaci(detekce změny adresy)
- adresa slouží k lokalizaci narušení
- vysoká odolnost proti překonání
- používají se pro rozsáhlé objekty - až 127 modulů
- délka vedení závisí na úbytku napětí, nesmí klesnout pod 11V
- detektory se paralelně připojují pomocí 2 struktur
  - stromová
  - liniova

Kombinované ústředny

- kombinace sběrnicové a analogové
- každá ústředna má určený počet sběrnic

- pomocí linek jsou k ústředně propojený koncentrátory -> slouží jako anlogové podústředky s několika smyčkama
    - komunikace s nimi probíhá po datové sběrnici jako ústředny s přímou adresací
- na sběrnici se také připojuje klávesnice a komunikační moduly(pro PC a tiskárnu)
- koncentrátor obsahuje až 8 adresovatelných smyček(na každou lze připojit 10 detektorů) a 4 programovatelné výstupy
- délka komunikační linky max 1 km

Pojednejte o funkčním rozdělení systému EPS. Základní rozdělení hlásičů požáru.

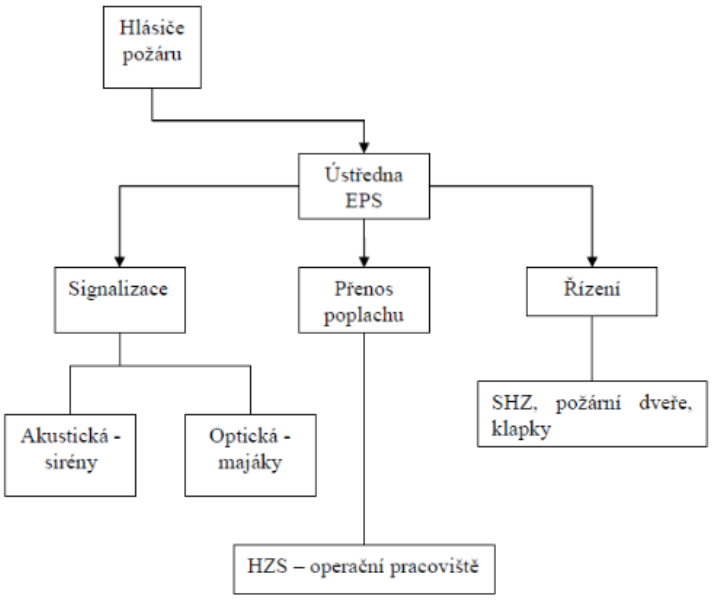
EPS = elektrická požární signalizace je systém elektronické ochrany před požárem a slouží v objektech pro zvýšení jejich požární bezpečnosti

Zásadní úkoly EPS

-včasné rozpoznání příznaků
-ohlášení obsluze
-upozornění na vzniklé nebezpečí
-aktivace ostatních požárních zařízení

Funkční rozdělení systému EPS

-Vstupní prvky - hlásiče požáru
-Ústředna EPS s ovládáním
-Vstupní prvky



Ústředna EPS slouží k:
-Vyhodnocování požární situace ve střežených prostorů
-Identifikaci místa nebezpečí s akustickou a vizuální indikací poplachu
-Sledování správné činnosti systému
-Předání požárně poplachových signáů na indikační zařízení nebo pomoci ZDP (zařízení dálkového přenosu) na další místo trvalé obsluhy

Základní rozdělení hlásičů požárů

Hlásiče tlačítkové

-hlášení vzniku požáru osobou, která identifikuje poplach. stav
-spolehlivé, tlačítko je pod rozbitným sklem
-zpětná deaktivace signálu požáru odaretováním

Hlásiče automatické

-reaguji na změnu fyzikálních parametrů bez lidského činitele

Podle detekované oblasti

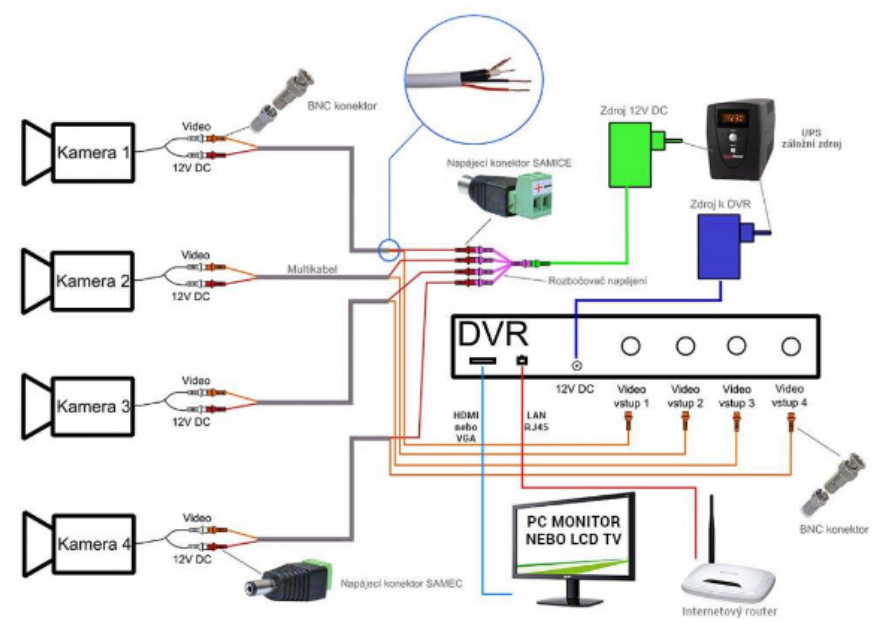
-bodové hlásiče (rovné stropy)
-lineární hlásiče na úseku (vysoké, nepravidelné stropy)

Pojednejte o významu CCTV při zabezpečení objektů a zabezpečených oblastí. Základní schéma systému CCTV.

Význam CCTV při zabezpečení objektů/oblastí

- slouží k dohlížení a kontrole i rozsáhlých prostor, identifikaci, rekognoskaci a detekci osob v reálném čase
- detekce podezřelého chování osob(vytřhnictví, opuštění zavazadel…), biometrickou verifikaci, sledování osob, identifikace reg. čísel vozidel, sledování a vyhodnocování dopravních nehod…
- provádí záznam na pásku nebo digitální médium a současné jej zobrazuje na zobrazovací zařízení

Schéma CCTV



- Kamerový bezpečnostní systém se skládá z:
  - kamer (optický snímač, objektiv, DSP procesor),
  - zařízení pro přenos a řízení videosignálu (např. kvadrátor, multiplexory, děliče obrazu, kabeláž, switch, router, web server, bezdrátové vysílače / přijímače, telemetrie),
  - záznamového a zobrazovacího zařízení (např. digitální rekordér, projekční / LCD / plazmové monitory, barevné / černobílé obrazovky),
  - příslušenství kamer (např. kryt, polohovací hlavice, konzoly, prostředky přepěťové ochrany, IR nebo halogenové reflektory).