MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Krátky úvod do informačnej a kybernetickej bezpečnosti
a
Malý výkladový slovník

Obsah

1 Úvod

Informatizácia spoločnosti priniesla popri mnohých pozitívach aj rastúcu závislosť spoločnosti od jej informačných a komunikačných technológií a potrebu systematicky riešiť ich ochranu, t.j. zaistiť dostatočnú úroveň kybernetickej a informačnej bezpečnosti. Slovenská republika v posledných rokoch prijala niekoľko zákonov, ktoré stanovujú povinnosti v kybernetickej a informačnej bezpečnosti pre relatívne široký okruh subjektov. Problém je s implementáciou požadovaných opatrení, spôsobený tým že informačná (kybernetická) bezpečnosť je nová, rýchle sa rozvíjajúca multidisciplinárna oblasť ľudskej činnosti a na Slovensku (podobne ako v iných krajinách) je nedostatok odborníkov, ktorí by požiadavky zákonov na zaistenie kybernetickej a informačnej bezpečnosti v dotknutých organizáciách vedeli riešiť. Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky na pomoc správcom informačných systémov verejnej správy, ale aj ostatným záujemcom, vydáva sériu metodických materiálov, ktoré vypracovali vysokoškolskí odborníci dlhodobo pôsobiaci v oblasti informačnej a kybernetickej bezpečnosti.
Tento dokument predstavuje tak ako to vyjadruje jeho názov, úvod do informačnej a kybernetickej bezpečnosti pre laikov, ktorí sa zatiaľ s touto problematikou nestretli. Ide o upravený text úvodnej kapitoly z učebnice, ktorý bol vydaný aj ako úvodná kapitola knihy a prepracovanej učebnice. Cieľom tohto textu je pomôcť čitateľovi zorientovať sa v problematike informačnej a kybernetickej bezpečnosti a vytvoriť si aspoň rámcovú predstavu o problémoch, ktoré táto disciplína rieši.
V informačnej a kybernetickej bezpečnosti sa používa množstvo špecifických odborných termínov, ktoré sa často používajú bez predchádzajúceho vysvetlenia a ešte aj v rozličných významoch. Pred 15 rokmi Ministerstvo financií iniciovalo projekt vytvorenia výkladového slovníka (vtedy ešte len) informačnej bezpečnosti, ktorý mal byť základom pre jednotnú slovenskú terminológiu v oblasti informačnej bezpečnosti. Výňatok z tohto slovníka, doplnený o pojmy kybernetickej bezpečnosti tvorí časť tohto materiálu.

2 Informačná bezpečnosť

Aby jednotlivci, organizácie, štáty aj celá ľudská spoločnosť mohli úspešne fungovať v meniacom sa prostredí, potrebujú poznať svoj stav, zdroje a možnosti, stav prostredia, vzťahy s prostredím (a subjektmi v ňom), možné tendencie a podmienky ďalšieho vývoja a na základe toho upravovať svoj vlastný stav a vzťahy s prostredím. Stav (subjektu, okolia, iných subjektov) je zachytený/vyjadrený v podobe *informácie.* Informácia môže mať rozličné formy; pre naše potreby sa stačí obmedziť na informáciu, ktorá sa dá zaznamenať v podobe *údajov*, resp. číselne kódovaných *(digitálnych) údajov*. Údaje sú konečné (spravidla neprázdne) postupnosti znakov nejakej abecedy; pre digitálne údaje je abecedou, v ktorej sa údaje zapisujú, množina číslic, napr. {0,1,2,3,4,5,6,7,8,9}. Dôležitým špeciálnym prípadom digitálnych údajov sú binárne údaje; t.j. konečné neprázdne postupnosti znakov z abecedy {0,1}. Údaj a informácia sa často používajú ako synonymá, ale je medzi nimi rozdiel – tá istá informácia sa dá zaznamenať pomocou rôznych údajov, napr. údaje “100”, “10^2”, “sto”, “C”, “one hundred” reprezentujú tú istú informáciu, ale zjavne nie sú syntakticky totožné. Budeme predpokladať, že údaje sú *formou záznamu informácie* a informácia je *obsahom údajov*. Aby sa informácia dala používať, musí sa spracovať. Pod *spracovaním informácie* rozumieme *získavanie* (napr. fotografovanie, slovný popis nejakého objektu), *prenos* (posielanie MMS), *vlastné spracovanie* (orezanie obrázku, grafické úpravy, napísanie článku, vytlačenie, vystavenie na webovej stránke), *využitie* (čítanie článku, používanie

informácií uvedených v článku na vlastné účely), *uchovávanie* (uloženie obrázku, textu, článku na pamäťové médium, kde je bezprostredne k dispozícii pre ďalšie použitie), *archivácia* (uloženie údajov obsahujúcich informáciu na pamäťové médium schopné dlhodobo uchovať zaznamenané údaje), *zničenie informácie* (zničenie nosičov, na ktorých boli príslušné údaje zaznamenané, alebo vymazanie údajov z pamäťových nosičov). Vznik/získavanie, prenos, spracovávanie, využívanie, uchovávanie, archivovanie a ničenie informácie predstavujú *životný cyklus informácie*.

Človek nemá dostatočné kapacity na to, aby si pamätal a vedel rýchlo spracovávať veľké množstvá potrebných informácií. Preto si už v dávnej minulosti vytváral pomôcky na zaznamenávanie a spracovanie informácie (tabuľky, počítadlá, abakus, astroláb), využíval zvukové a vizuálne signály na prenos informácie. Hlinené tabuľky, kosti s vrypmi, počítadlá, signálne ohne a neskôr sofistikovanejšie zariadenia na zaznamenávanie, spracovanie a prenos informácie, predstavujú informačné a komunikačné technológie (IKT). Tie súčasné informačné a komunikačné technológie vznikli spojením masovokomunikačných prostriedkov, telekomunikačných sietí a počítačov. Na rozdiel od predchádzajúcich IKT sa vyznačujú tým, že

a) spracovávajú informáciu v digitálnej forme,
b) na prenos informácie využívajú tie isté komunikačné kanály[1],
c) informácia sa spracováva automatizovane, na základe programov.

Najpriliehavejšie označenie pre súčasné IKT by bolo *digitálne IKT.* Keďže digitálne IKT sú cenovo dostupné, mimoriadne výkonné a spracovávať informácie je potrebné v akejkoľvek oblasti ľudskej činnosti, digitálne IKT nachádzajú široké uplatnenie. Využitie ich potenciálu si však vyžiadalo zmeny tradičných postupov (o.i. nahradenie papierových dokumentov elektronickými). Prispôsobenie procesov digitálnym IKT (*informatizácia*) viedlo k takému nárastu objemu spracovávanej informácie, že návrat k ručnému spracovaniu informácie nie je možný. Digitálne IKT sa stali *kritickou infraštruktúrou* spoločnosti[2], resp. spoločnosť sa dostala do závislosti od svojich digitálnych IKT. Digitálne IKT tvoria globálny systém[3] s bohatými väzbami medzi jednotlivými subsystémami a prvkami, sú z technického hľadiska veľmi komplikované, pracuje s nimi veľké množstvo ľudí bez patričného odborného vzdelania a spracovávajú sa v nich dôležité informácie. Existuje veľa spôsobov ako narušiť digitálne IKT a informácie, ktoré sa pomocou nich spracovávajú. Aby bolo možné zabezpečiť primeranú ochranu digitálnych IKT a informácií (v štáte, inštitúcii, komerčnej firme, ďalej len organizácii), je potrebné identifikovať, čo treba chrániť, pred čím a ako. Čokoľvek, čo má pre organizáciu cenu (súvisí s plnením poslania organizácie) a vyžaduje si ochranu, sa nazýva *aktívum (asset[4]) organizácie.* Aktíva organizácie sú podľa charakteru fyzické (budovy, zariadenia, technologická infraštruktúra, informačné systémy, siete), nehmotné (informácie, programové vybavenie počítačov, know-how, finančné prostriedky, organizačná štruktúra, dobré meno organizácie, lojalita zamestnancov, vzťahy s partnermi a zákazníkmi) a iné. Z hľadiska informačnej bezpečnosti sú zaujímavé predovšetkým tie aktíva organizácie, ktoré súvisia so spracovaním informácie. Možnosť narušenia aktíva sa nazýva *hrozba (threat).* Hrozbami sú

a) prírodné/environmentálne vplyvy (záplava, znečistenie, požiar, výbuch sopky, úder blesku, zemetrasenie, pád nebeského telesa, choroba...),

[1] komunikačný kanál je akékoľvek médium, v ktorom sa môžu šíriť signály prenášajúce údaje/informáciu
[2] kritická infraštruktúra spoločnosti je infraštruktúra, bez ktorej spoločnosť nie je schopná plniť niektoré zo svojich základných funkcií
[3] označuje sa aj pojmom digitálny ekosystém
[4] v odbornej literatúre sa často používajú pojmy prebraté z angličtiny, preto v texte a vo výkladovom slovníku uvedieme popri slovenských aj pôvodné anglické termíny

b) technické poruchy, chyby v programoch, ľudské chyby, nedostatok zdrojov, rozpor s legislatívou, ale aj

c) úmyselná ľudská činnosť (krádež, sabotáž, prienik do systému, škodlivý softvér, a i.).

Hrozby vyjadrujú, čo by sa **mohlo** stať organizácii alebo konkrétnemu aktívu; ale aby k tomu naozaj došlo, musí existovať *nositeľ hrozby*, prostredníctvom ktorého sa možnosť realizuje (napr. nositeľom hrozby záplavy je prasknuté kanalizačné potrubie, rozvodnená rieka, prietrž mračien) a aktívum (organizácia, výpočtové stredisko, počítač) musí mať *zraniteľnosť (vulnerability),* vďaka ktorej sa voči nemu môže uplatniť hrozba (deravá strecha). Zraniteľnosť môže byť chyba, nedostatok, alebo aj spôsob použitia aktíva (na počítač, ktorý nie je pripojený k počítačovej sieti sa hrozba útok hackera z Internetu nemá ako uplatniť). Špecifickým typom hrozby je cieľavedomá ľudská činnosť zameraná na narušenie aktíva organizácie. Pokus o naplnenie takejto hrozby sa nazýva *útok* a nositeľom hrozby je *útočník* (útočníkom môže byť človek, skupina ľudí, organizácia, inštitúcia, štát).
Naplnenie hrozby voči aktívu môže mať pre organizáciu negatívne dôsledky, ktoré označujeme ako *dopad (hrozby).* Dopadom môže byť poškodenie alebo zničenie aktíva, dočasné zníženie jeho funkčnosti, pozastavenie, obmedzenie rozsahu alebo kvality služieb, ktoré dané aktívum využívajú, finančná strata, poškodenie dobrého mena, strata klientov, ohrozenie zdravia a života ľudí a pod. Dopad hrozby sa v niektorých prípadoch dá vyjadriť kvantitatívne (cena ukradnutého počítača), ale najmä dopad na nehmotné aktíva sa ťažko kvantifikuje (strata obchodných príležitostí, poškodenie dobrého mena). Preto sa často používa kvalitatívne hodnotenie dopadu, napríklad na trojúrovňovej škále sa dopad hrozby (na aktívum) pre organizáciu považuje za

a) nízky, ak sú finančné straty pre organizáciu zanedbateľné, nedošlo k ohrozeniu zdravia a života ľudí, narušeniu zmluvných záväzkov a povinností organizácie a organizácia je schopná plniť úlohy vyplývajúce z jej poslania bez obmedzenia;

b) vysoký, ak (napr.) finančné straty v dôsledku naplnenia hrozby organizácia nie je schopná vykryť z vlastných zdrojov (napr. nie je schopná v dostatočne krátkom čase nahradiť a spustiť do prevádzky kľúčový systém organizácie), došlo k vážnemu ohrozeniu zdravia, prípadne smrti ľudí, organizácia nie je schopná dlhodobo (dni, týždne, mesiace) plniť svoje základné úlohy a plniť záväzky;

c) stredný, ak je závažnosť dopadu vyššia ako nízka a nižšia ako vysoká.

Pád lietadla na budovu by mal pre organizáciu katastrofálne následky, ale takáto udalosť je tak zriedkavá, že sa ňou reálne treba zaoberať len vo výnimočných prípadoch (ropná rafinéria, atómová elektráreň, dopravný uzol). Na identifikáciu závažnosti bezpečnostných problémov, ktoré organizácia potrebuje riešiť, samotný dopad hrozieb nestačí a namiesto neho sa používa riziko. *Riziko* je veličina, ktorá zohľadňuje pravdepodobnosť naplnenia hrozby voči aktívu a jeho dopad. *Hodnota rizika* z matematického hľadiska predstavuje strednú hodnotu dopadu (danej hrozby). Hoci je možné vyjadriť hodnotu rizika kvantitatívne, v praxi sa viac používa kvalitatívne hodnotenie rizika, pretože je problém určiť hodnotu pravdepodobnosti naplnenia hrozby (najmä takej, ktorá sa v organizácii ešte nikdy nenaplnila) a často aj kvantitatívne vyjadriť dopad. Preto sa aj pre odhad pravdepodobnosti (naplnenia hrozby) používa kvalitatívne vyjadrenie. Pravdepodobnosť naplnenia hrozby je

- nízka, ak k naplneniu hrozby ešte nedošlo, alebo došlo raz za niekoľko rokov,[5]
- stredná, ak k naplneniu hrozby dochádza raz za niekoľko mesiacov,
- vysoká, ak naplneniu hrozby dochádza každý týždeň.

K týmto trom hodnotám pridáme ešte nulovú, aby sme ošetrili prípady, keď sa hrozba na niektoré z

[5] Tieto hodnoty nie sú záväzné, organizácia si ich môže upraviť podľa vlastného uváženia.

aktív nevzťahuje (a teda sa nemôže naplniť). Hodnota rizika sa potom určuje skombinovaním hodnôt pravdepodobnosti naplnenia hrozby a dopadu, napr. tak, ako je uvedené v tabuľke 1.

dopad→ pravdepodobnosť ↓	nízky	stredný	vysoký
nulová	nulové	nulové	nulové
nízka	nízke	nízke	stredné
stredná	nízke	stredné	vysoké
vysoká	stredné	vysoké	vysoké

Tabuľka 1. Výpočet hodnoty rizika

Aby organizácia dokázala dostatočne a pritom efektívne ochrániť svoje aktíva, bude musieť zistiť, ktoré hrozby sú pre ňu relevantné a aké riziko z nich pre ňu vyplýva. To je predmetom *analýzy rizík*.
Analýza rizík začína stanovením rozsahu – či sa má týkať celej organizácie, jej časti, konkrétneho (informačného) systému alebo systémov, v ktorých sa spracovávajú napr. osobné údaje. Nech je predmetom analýzy rizík (veľký) informačný systém organizácie. Ten pozostáva z technických prostriedkov (počítače, periférne zariadenia, počítačové siete), programového vybavenia (systémového a aplikačného) a údajov. Obsluhujú ho ľudia a jeho činnosť je súčasťou procesov prebiehajúcich v organizácii. Analyzovaný systém komunikuje s inými informačnými systémami, závisí od podpornej infraštruktúry (zdroj energie, klimatizácia) a vstupujú doň údaje z vonkajšieho prostredia a *vice versa*. Všetko, čo nie je súčasťou systému, ale má vplyv na jeho činnosť, tvorí jeho bezpečnostné okolie/prostredie (budova, priestory, v ktorých je systém umiestnený, obslužný personál, používatelia, podporná infraštruktúra, externé systémy, s ktorými analyzovaný systém komunikuje, vnútorná legislatíva organizácie a pod.) Prvým krokom samotnej analýzy rizík je identifikácia hrozieb, ktoré sú pre systém relevantné, inventarizácia aktív systému, zraniteľností aktív a existujúcich bezpečnostných opatrení. *Bezpečnostné opatrenia* sú technické, organizačné, fyzické, personálne a iné riešenia, ktorých úlohou je eliminovať riziká (vyplývajúce z hrozieb voči aktívam systému alebo jeho bezpečnostného okolia) alebo aspoň znížiť ich hodnotu na akceptovateľnú úroveň. Existujú rozsiahle katalógy hrozieb aj zraniteľností, ktoré sa dajú použiť pri identifikácii hrozieb a zraniteľností relevantných pre analyzovaný systém. Ďalším krokom analýzy rizík je ohodnotenie rizík, pri ktorom sa používa metodika uvedená vyššie alebo podobná. Pri stanovovaní pravdepodobnosti naplnenia hrozieb sa vychádza zo štatistík o *bezpečnostných incidentoch* (narušeniach aktív organizácie v minulosti), zo zoznamu existujúcich zraniteľností aktív a z informácií o implementovaných bezpečnostných opatreniach. Neošetrené zraniteľnosti zvyšujú a implementované bezpečnostné opatrenia znižujú pravdepodobnosť narušenia príslušného aktíva. Výsledkom ohodnotenia rizík je zoznam rizík usporiadaný podľa závažnosti, ktorý býva spravidla príliš dlhý na to, aby sa organizácia mohla zaoberať všetkými jeho položkami. Navyše, eliminácia niektorých rizík by si vyžiadala vyššie náklady, ako je hodnota rizík. Organizácia preto stanoví hranicu *akceptovateľného rizika,* čím rozdelí zoznam rizík na dve časti – tie, ktoré bude ďalej riešiť, a tie, ktoré bude akceptovať (t.j. neprijme na ich elimináciu alebo zmiernenie žiadne opatrenia, ale bude „len“ sledovať). Pre riziká, ktoré sa ocitli “nad čiarou”, má organizácia tri možnosti – *prijať opatrenie na elimináciu, alebo zníženie rizika na akceptovateľnú úroveň*, *vyhnúť sa riziku* (nahradiť rizikové riešenie iným) alebo *preniesť riziko* (poistenie). Ďalšie kroky (ktoré už formálne nespadajú do analýzy rizík) sú *návrh a implementácia opatrení*[6] a potom *monitoring*

[6] Opatrenia sa z hľadiska pôsobnosti delia na tri skupiny; tie, ktoré vzťahujú na samotný systém, tie, ktoré sa vzťahujú na jeho bezpečnostné okolie, a napokon tie, ktoré sa vzťahujú aj na systém aj na jeho bezpečnostné

systému, aby sa zistilo, či sú opatrenia účinné, či hodnota niektorého zo *zostatkových rizík* (neošetrených rizík, resp. rizík, ktorých pôvodnú hodnotu znížili prijaté opatrenia) nevzrástla nad akceptovateľnú úroveň, resp. či sa neobjavili nové zraniteľnosti alebo hrozby, ktoré neboli v čase analýzy rizík známe. Tento proces (analýza rizík, prijatie opatrení, monitoring systému, revízia opatrení) prebieha kontinuálne a nazýva sa *správa rizík (risk management).*

Pri rozsiahlych systémoch býva problém s identifikáciou relevantných aktív a so skúmaním možných dopadov hrozieb. Tu je potrebné uvedomiť si, že z hľadiska organizácie je podstatné zaistiť podmienky a zdroje potrebné na to, aby mohla poskytovať služby a vykonávať činnosti, pre ktoré bola vytvorená. Informácia je jedným z kľúčových zdrojov, bez ktorých organizácia nemôže vykonávať svoju činnosť a v súčasnosti sa v prevažnej miere spracováva pomocou digitálnych IKT. Cieľom ochrany digitálnych IKT je ochrana informácie, ktorá sa pomocou nich spracováva, aby ju organizácia mohla využívať na plnenie svojho poslania. Ochrana informácie má viacero aspektov, ktoré sa premietajú do bezpečnostných požiadaviek na údaje v podobe ktorých je informácia zaznamenaná, na spôsob ich použitia, resp. na samotný systém. Najdôležitejšie z nich sú *dôvernosť, integrita, dostupnosť, autentickosť, súkromnosť, nepopretie pôvodu, nepopretie prijatia, anonymita, pseudonymita, zodpovednosť za činnosť v systéme.*

Zaistenie *dôvernosti údajov* znamená, že k informácii obsiahnutej v údajoch majú prístup len tie osoby, ktorým je určená (oprávnené osoby). Zdôrazňujeme rozdiel medzi prístupom k údajom a prístupom k obsahu údajov. Zaistenie prvej požiadavky by znamenalo, že sa údaje spracovávajú spôsobom, pri ktorom je vylúčená prítomnosť nepovolaných osôb, čo je nerealistický predpoklad.[7] V druhom prípade „stačí“, aby boli bola informácia zapísaná prostredníctvom takých údajov, že pre všetky osoby okrem oprávnených bude nezrozumiteľná; t.j. aby nebolo možné získať z údajov ich informačný obsah. Ochrana dôvernosti údajov sa zabezpečuje riadením prístupu k údajom a šifrovaním.

Zaistenie *integrity údajov* znamená, že údaje nemôžu byť nepozorovane modifikované bez toho, aby si to oprávnená osoba všimla. Ideálne by bolo, keby bolo možné vylúčiť akýkoľvek neoprávnený zásah do údajov počas ich spracovania, ale to sa vzhľadom na charakter a zložitosť systémov, v ktorých sa údaje spracovávajú, nedá garantovať. Ak oprávnená osoba zistí, že údaje boli neoprávnene upravované, nebude sa spoliehať na informáciu, ktorú obsahujú, ale môže si ich od toho, kto jej ich poskytol, vyžiadať ešte raz.[8] Požiadavka na integritu sa dá zmysluplne použiť aj na integritu technických zariadení, sietí; narušením integrity by bolo fyzické poškodenie zariadenia, ale aj napr. pripojenie malého zariadenia (*keylogger*) medzi klávesnicu a počítač, ktoré by zaznamenávalo, ktoré klávesy používateľ stlačil.

Zaistenie *dostupnosti údajov* znamená, že údaje sú k dispozícii oprávneným osobám kedykoľvek, keď o to požiadajú. Táto absolútna požiadavka sa dá zovšeobecniť tak, že sa stanoví maximálny čas od požiadavky na sprístupnenie údajov až po okamih, keď žiadateľ má údaje k dispozícii; alebo sa dostupnosť definuje časom, kedy sú údaje k dispozícii.[9] Podobne ako v predchádzajúcom prípade, aj dostupnosť sa nevzťahuje len na údaje, ale má zmysel stanoviť úroveň dostupnosti akéhokoľvek zdroja, ktorý organizácia potrebuje na svoju činnosť . Z hľadiska používateľa zahŕňa aj dostupnosť služby, ktorú mu organizácia má poskytovať.

Naplnenie požiadavky na *autentickosť údajov (authenticity)* znamená, že príjemca si môže byť istý tým, že údaje sú zhodné s tými, ktoré poslal odosielateľ, a s identitou odosielateľa (z akého zdroja

---

okolie. Po návrhu opatrení sa ešte posúdi, či sa opatreniami podarilo dostať všetky riziká na akceptovateľnú úroveň a ak nie, celý proces (sústredený na problematické aktíva systému) sa zopakuje.

[7] Predstavme si napríklad prenos údajov prostredníctvom bezdrôtovej siete alebo Internetu.

[8] Existujú aj metódy rekonštrukcie poškodených údajov, tzv. samoopravné kódy.

[9] Absolútna dostupnosť by sa dala vyjadriť tak, že údaje sú dostupné nepretržite alebo, že čas od požiadavky na prístup k údajom po poskytnutie údajov je nulový (resp. daný technickými parametrami – rýchlosť vyhľadania údajov a doba prenosu od zdroja k žiadateľovi); populárne 24 x 7 znamená (nerealistickú) požiadavku na to, aby údaje (služby) boli k dispozícii 24 hodín denne a 7 dní v týždni, t.j. nepretržite.

pochádzajú). Autentickosť teda v sebe spája integritu údajov a jednoznačné/garantované určenie identity tvorcu údajov.

Súkromnosť (privacy) sa vzťahuje na osobné údaje a znamená, že človek má možnosť stanoviť, ktoré **jeho** osobné údaje, komu a za akých podmienok budú sprístupnené. Súkromnosť je slabšia požiadavka ako dôvernosť; na zaistenie súkromnosti napr. zdravotnej dokumentácie stačí oddeliť osobné údaje, ktoré umožňujú určiť identitu pacienta od výsledkov vyšetrení. Ak sa útočník/narušiteľ dostane k anonymným údajom, nevie, na koho sa vzťahujú.

Ďalšie dve bezpečnostné požiadavky sa vzťahujú na komunikáciu: *nepopretie pôvodu* (*non repudiation of origin*) správy znamená potvrdenie toho, že tvorca/odosielateľ správy správu poslal a *nepopretie prijatia (non repudiation of receipt)* zasa, že príjemca správy správu preukázateľne dostal.

Na vysvetlenie ďalších pojmov potrebujeme definovať základné pojmy týkajúce sa *identifikácie*. Ľubovoľná vec, údaje, dokument, človek, alebo dokonca niečo také abstraktné ako je myšlienka, sa nazýva *entita.* Entita sa vyznačuje nejakými vlastnosťami (*atribútmi*[10]). Množina atribútov, ktoré umožňujú jednoznačne odlíšiť danú entitu od podobných entít, sa nazýva *identita* danej entity. Všetky atribúty, ktoré prislúchajú danej entite, tvoria *absolútnu (úplnú) identitu* danej entity. Absolútna identita môže byť veľmi rozsiahla a na jednoznačné určenie entity v nejakej menšej oblasti bude stačiť aj podmnožina atribútov absolútnej identity. Preto sa pojem identity viaže na *oblasť použitia* a identitou entity je ľubovoľná množina atribútov, ktorá stačí na jednoznačné určenie entity v danej oblasti použitia identity. Napríklad, ak sú v miestnosti dvaja ľudia, matka a dieťa, tak na určenie dieťaťa stačí ktorýkoľvek z atribútov rok narodenia, výška, váha, rodinný vzťah, zamestnanie a i. Na rýchle určenie entity možno vytvoriť aj umelú identitu, *identifikátor*, špeciálny atribút, ktorého jedinou úlohou je plniť funkciu identity danej entity v presne definovanej oblasti použitia. Identifikátorom je napríklad rodné číslo osoby, IČO, DIČ, sériové číslo výrobku, číslo spisu a pod. Na identitu sa často viažu jedinečné oprávnenia, napríklad prístup k službe, alebo ku zdrojom. Aby napr. niekto nemohol prebrať zásielku určenú inému, musí doručovateľovi preukázať svoju identitu. Tento úkon sa skladá z dvoch častí: *identifikácie* a *autentifikácie/autentizácie*. Pri identifikácii entita deklaruje svoju identitu (alebo v inom prípade človek deklaruje identitu nejakej entity, napríklad vo forme tvrdenia „toto je moje auto“). Identifikácia sama o sebe na stanovenie identity nestačí, pretože môže byť falošná. (Človek sa môže vydávať za niekoho iného.) Druhá strana si preto musí overiť pravdivosť deklarovanej identity (tento úkon sa nazýva *autentizácia*). To sa v prípade osôb robí tromi rôznymi spôsobmi alebo ich kombináciou:

a) na základe toho, čím človek je (biometrické charakteristiky ako sú odtlačky prstov, obraz sietnice, DNA, výzor),

b) toho, čo človek má (identifikačný/autentizačný token: preukaz totožnosti, preukaz zamestnanca), alebo

c) toho, čo človek vie (heslo, PIN, prístupový kód, osobné údaje[11]).

Pri autentizácii musí mať overovateľ identity možnosť overiť, či poskytnuté autentizačné údaje sa viažu na danú identitu. V bežnom živote na overovanie identity (totožnosti) slúžia rôzne preukazy (občiansky preukaz, pas), ktoré vydala dôveryhodná autorita (*poskytovateľ identity*), pri prihlasovaní do informačných systémov sa človek identifikuje prihlasovacím menom a na autentizáciu používa heslo, kartu, alebo odtlačok prsta.

[10] Keby sme mali byť úplne korektní, museli by sme rozlišovať medzi atribútmi a ich hodnotami, napr. atribút dátum narodenia má hodnotu 1.1.1980. Kvôli zjednodušeniu výkladu však tam, kde to nepovedie k nedorozumeniu, budeme pod pojmom atribút rozumieť aj názov atribútu aj jeho hodnotu.

[11] Napr. meno starej matky z matkinej strany.

Bezpečnostná požiadavka *zodpovednosť za činnosť v systéme (accountability*[12]*)* znamená, že k jednotlivým činnostiam v systéme je možné jednoznačne priradiť entitu (človeka, proces), ktorá ich vykonala alebo spôsobila. Na zaistenie možnosti vyvodzovať zodpovednosť za činnosť v systéme je potrebná jednak spoľahlivá identifikácia a autentifikácia osôb a tiež záznamy o činnosti (tzv. záznamy auditu) obsahujúce minimálne informáciu o tom, ktorá entita (človek alebo proces, ktorý človek spustil), kedy (dátum a čas), s čím (údaje a iné zdroje systému) a čo vykonala (napr. vymazala nejaký súbor, poslala e-mail).

Anonymita a *pseudonymita* sú bezpečnostné požiadavky, ktoré chránia súkromie človeka a sú v istom zmysle opačné k požiadavke na *accountability*. *Anonymita* znamená, že zo získaných atribútov nie je možné jednoznačne určiť entitu (osobu), ktorej prislúchajú (situácie, v ktorých je anonymita žiaduca, sú napr. surfovanie po Internete, nakupovanie). *Pseudonymita* je slabšou požiadavkou ako anonymita; entita vystupuje pod identitou, ktorú vo všeobecnosti nie je možné priradiť konkrétnej osobe (prezývka, pseudonym, nick), ale obmedzený okruh (dôveryhodných) osôb vie jednoznačne identifikovať osobu na základe jej pseudonymu (a prípadne ďalších atribútov, ktoré má k dispozícii).

Základom pre analýzu rizík a návrh opatrení sú prvé štyri (najvšeobecnejšie) bezpečnostné požiadavky[13] – *dôvernosť, integrita, dostupnosť, autentickosť*. Pri analýze rizík skúmame, aký vplyv by malo narušenie jednotlivých aktív na dôvernosť, integritu, dostupnosť a autentickosť informácie v systéme (organizácii) a aj požiadavky na ochranu informácie sú formulované v podobe úrovne záruk na zaistenie dôvernosti, integrity, dostupnosti a autentickosti typov informácie spracovávaných v systéme (organizácii). V špecifických prípadoch (ochrana osobných údajov) sa uplatňuje požiadavka na súkromnosť, pre elektronickú úradnú komunikáciu budú dôležité požiadavky na nepopretie pôvodu a prijatia dokumentu.

Vyššie opísané riešenie (analýza rizík, prijatie opatrení vrátane vytvorenia formálnej dokumentácie, správa rizík) predstavuje *bezpečnostný projekt systému*. Pre organizáciu, ktorá má viacero informačných systémov je výhodnejšie zaviesť *systém riadenia informačnej bezpečnosti (information security management system, ISMS)* pre celú organizáciu, alebo jej podstatnú časť ako riešiť bezpečnosť jednotlivých informačných systémov pomocou individuálnych bezpečnostných projektov. Ak má organizácia vyhovieť všetkým bezpečnostným požiadavkám a naplniť svoje potreby v informačnej bezpečnosti efektívnym spôsobom, mala by od riešenia čiastkových bezpečnostných problémov prejsť k systematickému riešeniu, kde mnohé bezpečnostné problémy svojich jednotlivých systémov vyrieši spoločnými preventívnymi opatreniami, na podobné problémy bude využívať rovnaké, už raz vyvinuté riešenia, opatrenia sa budú vzájomne dopĺňať a ich účinnosť bude organizácia priebežne monitorovať, pravidelne vyhodnocovať a v prípade potreby ich bude aktualizovať a prípadne prijímať nové.

Systém riadenia informačnej bezpečnosti je opísaný v norme ISO/IEC[14] 27001. Jeho základom je *politika informačnej bezpečnosti (bezpečnostná politika)* a na ňu nadväzujúce špecifické bezpečnostné politiky a procedúry upravujúce spôsob riešenia problémov, ktoré sú relevantné z hľadiska informačnej bezpečnosti. Bezpečnostná politika (dokument vydaný vedením organizácie)

1. definuje oblasť pôsobnosti, (*scope*) bezpečnostnej politiky, hlavné aktíva, hlavné bezpečnostné ciele organizácie v informačnej bezpečnosti a úroveň informačnej bezpečnosti, ktorú v organizácii považuje za primeranú,

[12] Možné preklady by boli napr. dosledovateľnosť, zúčtovateľnosť.
[13] Organizácia samozrejme môže požadovať aj zohľadnenie ďalších bezpečnostných požiadaviek, ale tým narastá zložitosť analýzy rizík.
[14] An Information Security Management System (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, managed in concert by an organization, in the pursuit of protecting its information assets.

2. stanoví zodpovednosť zamestnancov organizácie za presadzovanie a dodržiavanie bezpečnostnej politiky (a dokumentov na ňu nadväzujúcich),
3. uvedie štruktúru bezpečnostných dokumentov nadväzujúcich na danú bezpečnostnú politiku a ich obsah (špeciálne bezpečnostné politiky, alebo bezpečnostné štandardy, bezpečnostné praktiky – aké oblasti pokrývajú a akou formou budú vydané)
4. definuje, na základe čoho sa bude informácia v organizácii klasifikovať,
5. definuje spôsob analýzy rizík (kvantitatívna/kvalitatívna) a hranicu akceptovateľného rizika v závislosti od úrovne informačnej bezpečnosti, ktorú vedenie organizácie považuje za primeranú,
6. stanoví
    a. zásady pre monitoring, kontrolu a audit informačných a komunikačných systémov organizácie
    b. zásady riešenia bezpečnostných incidentov,
    c. stratégiu pre zaistenie kontinuity činnosti informačných a komunikačných systémov organizácie,
    d. správu bezpečnostnej politiky (ako často sa budú robiť pravidelné a z akých dôvodov mimoriadne revízie bezpečnostnej politiky).

Špecifické bezpečnostné politiky upravujú napríklad riadenie prístupu do informačných systémov organizácie, klasifikáciu informácie, fyzickú bezpečnosť, používanie elektronickej pošty, prístup na Internet, ochranu pred škodlivým softvérom, prácu na diaľku, používanie šifrovania a pod. Povinnosti vedenia organizácie sa vydaním bezpečnostnej politiky nekončia; musí vytvoriť primerané personálne, organizačné, materiálne, technické, právne, finančné a iné podmienky na implementáciu bezpečnostnej politiky v organizácii a premietnuť bezpečnostné požiadavky do činnosti organizácie (napr. pri obstarávaní nových systémov špecifikovať nielen funkcionálne a výkonnostné, ale aj bezpečnostné požiadavky, ktoré musia tieto systémy spĺňať, v zmluvách s externými dodávateľmi ošetriť napr. spracovanie citlivých údajov, dostupnosť služieb, zakomponovať povinnosti v informačnej bezpečnosti do pracovnej náplne zamestnancov a pod.). Hoci bezpečnostnú politiku vydáva vedenie organizácie, po odbornej stránke jej realizáciu bude zabezpečovať *manažér informačnej bezpečnosti* (*bezpečnostný manažér)* prípadne spolu s ďalšími bezpečnostnými špecialistami a budú sa ňou povinne riadiť všetci zamestnanci organizácie (vrátane vedenia) a externí spolupracovníci. Cieľom manažmentu informačnej bezpečnosti v organizácii je zabrániť vzniku udalostí s negatívnym dopadom na (informačné) aktíva organizácie.
Hoci základné princípy deklarované v bezpečnostnej politike majú dlhodobú platnosť, aj bezpečnostná politika si bude vyžadovať správu a revízie. Bezpečnostnú politiku vydáva vedenie organizácie, v ktorom by mal byť človek zodpovedný za informačnú bezpečnosť, správu bezpečnostnej politiky, predkladanie správ o stave informačnej bezpečnosti v organizácii a návrhov (zmien, projektov) vyžadujúcich si schválenie vo vedení organizácie. Odbornú a organizačnú stránku informačnej bezpečnosti v organizácii zabezpečuje manažér informačnej bezpečnosti, ktorý o.i. pripravuje správy o stave informačnej bezpečnosti v organizácii (napr. raz ročne), hlavné úlohy organizácie v informačnej bezpečnosti na ďalší rok a prípadne návrhy na zmeny bezpečnostnej politiky organizácie. Veľké bezpečnostné incidenty, výsledky auditov, zmeny IKT (zavedenie nových systémov), organizačné zmeny v organizácii si budú vyžadovať mimoriadne revízie bezpečnostnej politiky.
Akákoľvek udalosť, ktorá môže ovplyvniť bezpečnosť informačných a komunikačných systémov organizácie sa nazýva *bezpečnostne relevantná udalosť*. Bezpečnostne relevantná udalosť, ktorá môže

mať negatívny dopad na bezpečnosť informačných a komunikačných systémov organizácie, sa nazýva *bezpečnostný incident*. Aby sa organizácia vyhla bezpečnostným incidentom, resp. minimalizovala ich dopad, prijíma

a) opatrenia preventívneho charakteru (predtým ako incident nastal; ich cieľom je minimalizovať pravdepodobnosť toho, že k incidentu dôjde a/alebo minimalizovať jeho dopad). Analógiu tu predstavujú protipožiarne opatrenia, preventívne školenia zamestnancov, hasičské cvičenia, kontroly hasiacich prístrojov a pod.,

b) operatívne opatrenia na riešenie prebiehajúceho bezpečnostného incidentu, ktorých cieľom je čo najskôr ohraničiť incident, obmedziť jeho vplyv na ďalšie aktíva organizácie a minimalizovať jeho dopad. Analógiou je hasenie požiaru, evakuácia priestorov,

c) opatrenia po skončení bezpečnostného incidentu, ktorých cieľom je zistiť príčiny a vyvodiť dôsledky z bezpečnostného incidentu, ktoré majú organizácii pomôcť odstrániť slabiny, ktoré viedli k bezpečnostnému incidentu a zvýšiť úroveň ochrany jej aktív. Analógiou je analýza príčin požiaru a prehodnotenie protipožiarnych opatrení, zákaz fajčenia a manipulácie s otvoreným ohňom, požiarne cvičenia pre zamestnancov, inštalácia elektronickej signalizácie, revízia elektrických zariadení a pod.

Množstvo a rôznorodosť hrozieb a slabín digitálnych IKT presahuje kapacitu jedného človeka. Bezpečnostný manažér nemôže ani pri maximálnej snahe sám zvládať riešenie všetkých potenciálnych bezpečnostných incidentov a mnohé bezpečnostné incidenty presahujú rámec jednej organizácie. Podobne ako na hasenie požiarov existujú hasičské stanice, aj na riešenie bezpečnostných incidentov existujú špecializované organizácie. Prvá takáto organizácia, [15] CERT, vznikla na Carnegie Mellon University v roku 1988 ako reakcia na červa Morris, ktorý zamoril značnú časť vtedajšieho Internetu; v súčasnosti existuje niekoľko sto tímov a sú združené v organizácii *Forum of Incident Response and Security Teams (FIRST).*[16] Skratka *CERT* znamená *Computer emergency response team*, a keďže CERT je registrovaná značka (ochranná známka), inštitúcie s rovnakým zameraním pôsobia pod mierne modifikovaným názvom *CSIRT - Computer security incident response team (tím na riešenie počítačových bezpečnostných incidentov)*. Podrobné návody na zriadenie a prevádzku organizácie CSIRT sú všeobecne dostupné,[17] ale na to, aby CSIRT dosiahol medzinárodné uznanie a stal sa plnoprávnym členom FIRST, musí nielen deklarovať, ale aj preukázať odbornú spôsobilosť[18] a splnenie požiadaviek, ktoré na CSIRT kladie FIRST.

CSIRT je organizácia (jednotka, útvar) pozostávajúci z odborníkov na informačnú bezpečnosť, ktorej úlohou je reagovať na počítačové bezpečnostné incidenty. V okruhu svojej pôsobnosti poskytuje služby potrebné na zvládnutie bezpečnostných incidentov a podporu pri zotavení sa z ich následkov. Aby CSIRT minimalizoval riziká a tiež počet potrebných zásahov, poskytuje svojim klientom aj preventívne služby a vzdeláva ich. CSIRT však nemôže byť najmä z kapacitných dôvodov zodpovedný za prevádzku a zabezpečenie konkrétnych systémov; to je úloha správcov systémov a bezpečnostných manažérov, resp. iných bezpečnostných špecialistov organizácie.

Bezpečnosť aktív organizácie však nezávisí iba od bezpečnostných manažérov a bezpečnostných tímov, ale od všetkých ľudí, ktorí k aktívam organizácie majú prístup. Preto sa povinnosti v informačnej bezpečnosti nevzťahujú len na informatikov, bezpečnostného manažéra a jeho tím, ale všetkých zamestnancov, externistov a zamestnancov tretích strán, ktorí pristupujú k aktívam organizácie. Každý

[15] Vo verejnom sektore, štátne, najmä vojenské a podobné organizácie mali špecializované tímy na riešenie bezpečnostných problémov zrejme už predtým.
[16] V júni 2021 FIRST evidoval 585 tímov, pozri https://www.first.org/members/teams/
[17] A step-by-step approach on how to set up a CSIRT, Deliverable WP2006/5.1 (CERT-D1/D2), ENISA.
[18] Dostupné na internete: https://www.first.org/members/application/

z nich by mal vedieť, ako má s aktívami pracovať, čo s nimi nesmie robiť a čo má spraviť v prípade, ako odhalí nejakú anomáliu (zraniteľnosť, bezpečnostne relevantnú udalosť, resp. bezpečnostný incident). Tieto povinnosti musia byť zachytené v pracovných náplniach, zamestnanci musia byť zaškolení (podobne ako pri školeniach bezpečnosti práce) primerane úlohe, ktorú v informačnej bezpečnosti organizácie zohrávajú a organizácia musí mať zavedené aj opatrenia pre prípad, keď zamestnanci svoje povinnosti v informačnej bezpečnosti porušia. Povinnosti zamestnancov tretích strán a postupy v prípade ich porušení by mali byť dopredu zmluvne dohodnuté.

Najmä väčšie organizácie mávajú príliš veľa aktív na to, aby sa s každým z nich bolo možné zaoberať individuálne. Kľúčovým aktívom sú z hľadiska informačnej bezpečnosti informácie . Aby sa zjednodušila ich ochrana, organizácia používa *klasifikáciu informácií*, umožňujúcu rozdeliť informácie podľa požiadaviek na ich ochranu do tried. (V jednej triede sú informácie, ktoré majú porovnateľné požiadavky na ochranu, napr. tie, ktorých bezpečnostné požiadavky sú dôvernosť: vysoká, integrita: stredná, dostupnosť: nízka, autentickosť: stredná). Organizácia stanoví **bezpečnostné požiadavky pre jednotlivé typy informácií** (napr. úradné formuláre zverejnené na webe nie je potrebné chrániť z hľadiska dôvernosti, dôležité je zaistenie integrity a autentickosti, dostupnosť stačí zabezpečiť na strednej úrovni). Potom namiesto individuálneho stanovovania bezpečnostných požiadaviek pre konkrétnu informáciu stačí zistiť, o aký typ informácie ide, do ktorej klasifikačnej triedy patrí a vybrať opatrenia[19] zodpovedajúce úrovni bezpečnostných požiadaviek na ochranu dôvernosti, dostupnosti, autentickosti; prípadne na pokrytie iných požiadaviek. Bezpečnostné požiadavky na systémy sú odvodené od najvyšších bezpečnostných požiadaviek na informáciu, ktorá sa v nich spracováva.[20] Organizácia môže stanoviť podrobné postupy spracovania informácií pre jednotlivé triedy (napr. triedu, do ktorej patria utajované skutočnosti stupňa tajné), pravidlá pre klasifikáciu, prehodnocovanie klasifikácie informácie a pod.

Rozdelenie úloh, vytvorenie dokumentácie a zavedenie technických opatrení nestačí na zaistenie dostatočnej úrovne informačnej bezpečnosti v organizácii. Organizácia jednak nikdy nebude schopná eliminovať všetky riziká a jednak musí rátať s tým, že sa časom budú meniť podmienky, z ktorých vychádzala analýza rizík – objavia sa nové zraniteľnosti systémov, vymenia sa ľudia v organizácii, zavedú nové systémy, objavia nové hrozby; bezpečnostné opatrenia môžu strácať na účinnosti, zmení sa legislatíva, štandardy a i. Aby organizácia minimalizovala pravdepodobnosť bezpečnostných incidentov, musí sledovať stav svojich systémov, monitorovať účinnosť implementovaných opatrení, kontrolovať, či sa v organizácii dodržiavajú požiadavky bezpečnostnej politiky. Priebežnú kontrolu by mal vykonávať nielen bezpečnostný manažér a jeho tím, ale v okruhu svojej pôsobnosti aj ostatní vedúci/poverení pracovníci. Norma ISO/IEC 27004 obsahuje návody na monitorovanie a meranie úrovne informačnej bezpečnosti, posudzovanie efektívnosti ISMS organizácie a tiež návod ako analyzovať a vyhodnocovať výsledky získané monitorovaním a meraním.

Pravidelne za určené obdobie (stanovené v bezpečnostnej politike) by mal v organizácii prebehnúť interný alebo externý audit bezpečnosti, zameraný aspoň na kľúčové aktíva organizácie. *Audit* je nezávislé posúdenie stavu systému/časti organizácie/organizácie oproti vopred stanovenému požadovanému stavu. Nezávislosť auditu znamená to, že audit by nemali robiť ľudia, ktorí sú na posudzovanom stave nejako zainteresovaní (napr. bezpečnostný manažér organizácie), ale na druhej strane, títo budú s audítormi musieť spolupracovať a poskytovať im potrebné informácie. Existujú tri ISO normy, zaoberajúce sa auditom informačnej bezpečnosti – norma ISO/IEC 27006 stanovuje požiadavky na organizácie, vykonávajúce audit, ISO/IEC 27007 sa zameriava na audit ISMS (teda riadenie informačnej bezpečnosti v organizácii) a ISO/IEC 27008 na bezpečnostné opatrenia.

[19] NIST aj BSI definujú štandardné súbory opatrení, organizácia však môže vychádzať zo zoznamu opatrení normy ISO/IEC 27002 a vytvoriť bezpečnostné riešenie zodpovedajúce jej potrebám.
[20] Opísaný systém klasifikácie informácie vychádza z amerických noriem FIPS 199 a FIPS 200.

Organizácia by mala stanoviť rozsah auditu (napr. či sa bude vzťahovať na kľúčové systémy organizácie, špecifickú oblasť – osobné údaje, súlad s legislatívou) a môže stanoviť, čo je vzor, z ktorého má audit vychádzať. Ak audit hodnoverne preukáže, že organizácia riadi informačnú bezpečnosť v súlade s normou ISO/IEC 27001, môže si svoj ISMS nechať aj formálne *certifikovať*; t.j. nechať si vystaviť potvrdenie[21] o tom, že jej ISMS spĺňa požiadavky medzinárodného štandardu ISO/IEC 27001.
Napriek všetkej snahe organizácie sa nedá zaručiť, že v organizácii nedôjde k bezpečnostnému incidentu. V bezpečnostnej politike by mala byť stanovená povinnosť každého zamestnanca hlásiť spozorovaný bezpečnostný incident, resp. každú podozrivú okolnosť, ktorá môže znamenať začínajúci bezpečnostný incident nadriadenému alebo priamo bezpečnostnému manažérovi a poskytnúť potrebnú pomoc pri riešení bezpečnostného incidentu. Bezpečnostný manažér spolu so svojím tímom a zainteresovanými pracovníkmi organizácie by mali rozpracovať ustanovenia bezpečnostnej politiky ohľadne bezpečnostných incidentov; v predstihu by mali analyzovať možné scenáre bezpečnostných incidentov (ako by k takému niečomu mohlo dôjsť a čo by sa stalo, keby napr. do systému prenikol hacker, keby vypadlo napájanie, prístup na Internet, v lete vypadla klimatizácia serverovne, došlo k technickej poruche kľúčového servera, ochorel správca systému, anonym nahlásil teroristický útok a pod.) a navrhnúť postupy na rýchlu detekciu bezpečnostného incidentu, aktivizáciu ľudí schopných riešiť daný bezpečnostný incident, postupy na ohraničenie, zastavenie a likvidáciu následkov incidentu, dokumentovanie incidentu, informovanie dotknutých osôb o následkoch incidentu. Na úspešné riešenie bezpečnostných incidentov bude organizácia potrebovať vyhradiť zdroje (personálne, technické, finančné) a keď už k incidentu dôjde, možno bude potrebovať aj externú odbornú pomoc. O bezpečnostných incidentoch, ktoré majú dosah na tretie strany, resp. tam, kde to určuje zákon, je organizácia povinná informovať dotknuté osoby/organizácie a prípadne nahlásiť bezpečnostný incident príslušným štátnym orgánom. Bezpečnostné incidenty majú na organizáciu nepriaznivý dopad, a preto keď už k nejakému závažného bezpečnostnému incidentu došlo (alebo sa často opakujú drobné bezpečnostné incidenty), bezpečnostný manažér by mal (sám alebo s externou pomocou) analyzovať príčiny a priebeh bezpečnostného incidentu, informovať o tom vedenie organizácie a navrhnúť opatrenia, ktoré by podobným udalostiam v budúcnosti zabránili alebo zmiernili ich dopad.
Popri „bežných“ bezpečnostných incidentoch organizáciu môžu postihnúť bezpečnostné incidenty síce málo pravdepodobné, ale zato katastrofických rozmerov (požiar, teroristický útok, záplava, epidémia a pod.), ktoré môžu ohroziť samotnú existenciu organizácie. Podobne ako v prípade bežných bezpečnostných incidentov sa organizácia snaží identifikovať možné katastrofické hrozby a eliminovať alebo znížiť riziko, ktoré z nich vyplýva. Kým však bežné bezpečnostné incidenty majú prevažne lokálny dopad a organizácia ich dokáže riešiť vlastnými silami (alebo s dočasnou externou pomocou), katastrofické bezpečnostné incidenty môžu mať rozsah presahujúci pôsobnosť organizácie a dôsledky, ktoré by organizácia nebola schopná znášať. Organizácia sa musí pripraviť aj na riešenie takýchto katastrofických udalostí. Bezpečnostná politika obsahuje aj požiadavku na zachovanie kontinuity činnosti; t.j. požaduje, aby organizácia mala vypracované (nacvičené a aktualizované) plány na zachovanie kontinuity činnosti, resp. zavedený *manažment kontinuity činnosti (business continuity management, BCM)*. BCM je manažérsky proces, ktorého úlohou je zaistiť, aby ani v kritických situáciách nedošlo k prerušeniu významných činností organizácie, resp., keď už k prerušeniu dôjde, aby trvalo čo najkratšie a postihlo organizáciu v čo najmenšej možnej miere. Napríklad, organizácia má záložné kapacity, na ktorých je schopná spustiť prevádzku kľúčových systémov v prípade, ak dôjde k vyradeniu primárnych kapacít. Aby bola schopná okamžite prepnúť na náhradné zdroje, musí mať k dispozícii aktuálne údaje, a to znamená, že organizácia prevádzkuje v dvoch rozličných lokalitách paralelne dve kópie systému, vrátane programov a údajov, čo môže byť mimoriadne nákladné. Ak je prípustné krátkodobé prerušenie činnosti systému, organizácia môže použiť lacnejšie riešenia, napr.

[21] Oprávnenie vydávať certifikáty však nemá každá audítorská spoločnosť.

presunúť činnosť, ktorá prebiehala na znefunkčnenom systéme dočasne na iný systém, obmedziac menej dôležité činnosti, ktoré tento systém pôvodne vykonával. Zaistenie kontinuity činnosti organizácie v kritických situáciách si tak vyžaduje analýzu rizík (čo sa môže stať a aký by to malo dopad), analýzu dopadov na činnosť organizácie (*business impact analysis*, BIA), prípravu náhradných riešení (náhradné kapacity, zálohovanie údajov), vyhradenie zdrojov, a napokon stanovenie a nacvičenie postupov počas a po katastrofickej udalosti. Keďže katastrofickým udalostiam sa celkom nedá vyhnúť, manažment kontinuity činnosti je povinnou súčasťou systému riadenia informačnej bezpečnosti. Je však potrebné pripomenúť, že narušiť dôležité činnosti organizácie môže nielen výpadok IKT, a preto manažment kontinuity činnosti IKT predstavuje iba časť celkového manažmentu kontinuity činnosti organizácie.

Máloktorá organizácia je uzavretá a izolovaná od negatívnych vplyvov okolitého sveta. Preto ani informačnú bezpečnosť organizácie nemožno zaistiť len pomocou lokálnych opatrení vzťahujúcich sa na samotnú organizáciu. Základnou charakteristikou súčasných digitálnych IKT je ich vzájomná prepojenosť. Tá ich používateľom na jednej strane umožňuje využívať distribuované informačné zdroje a globálne služby, na druhej strane komunikácia s neznámym systémom, využívanie služieb poskytovaných neidentifikovateľným subjektom predstavuje bezpečnostné hrozby. Aby bola zaistená bezpečnosť systémov v organizácii, je potrebné zaistiť aspoň základnú úroveň ochrany širšieho prostredia, v ktorom pôsobia. Na medzinárodnej úrovni je problematické zavádzať bezpečnostné opatrenia právnou cestou, pretože medzinárodné organizácie nemajú nástroje na ich presadzovanie a kontrolu dodržiavania. Úspešným prostriedkom na masové presadzovanie dobrých riešení je normalizácia. ISO spolu s IEC zriadili v roku 1987 spoločný technický výbor JTC 1 - Information technology, ktorý vyvíja medzinárodné normy pre IKT. V JTC 1 pôsobí podvýbor TC 27 – IT security ktorý spravuje (pripravuje, vydáva, ruší a reviduje) približne 200 medzinárodných noriem z oblasti informačnej bezpečnosti. Ďalšími medzinárodnými štandardizačnými organizáciami sú IETF[22], vydávajúca nezáväzné[23] štandardy upravujúce fungovanie Internetu a ITU. Štáty tiež využívajú možnosť regulovať svoju informačnú a komunikačnú infraštruktúru a jej bezpečnosť pomocou vlastných alebo preberaných medzinárodných technických noriem a odporúčaní (podobne ako v prípade IETF viaceré z národných noriem stali de-facto a niektoré aj de-iure medzinárodnými normami). Normy riešia špecifické problémy, ale jednak neexistuje norma, ktorá by upravovala, ako má štát zaistiť dostatočnú úroveň informačnej bezpečnosti v oblasti svojej pôsobnosti a jednak majú samy o sebe nezáväzný charakter. Na zaistenie informačnej bezpečnosti na úrovni štátu musia štáty upravovať existujúcu legislatívu a prijímať nové zákony upravujúce práva a povinnosti subjektov vo vznikajúcom virtuálnom priestore a poskytujúce štátu prostriedky na reguláciu aktivít, ktoré v ňom prebiehajú. Prehlbujúca sa informatizácia spoločnosti prináša ďalšie závažné problémy, na ktoré bude musieť štát reagovať – o.i. stanovením základných bezpečnostných požiadaviek minimálne na informačné systémy v pôsobnosti štátu a systémy k nim pripojené, stanovením znalostných štandardov pre pracovníkov verejnej správy pracujúcich s ISVS, zvyšovaním bezpečnostného povedomia obyvateľstva, zavedením informačnej bezpečnosti v pregraduálnom aj celoživotnom vzdelávaní, podporou výskumu v informačnej bezpečnosti, budovaním terminológie, medzinárodnou spoluprácou a pod[24].

Informačná bezpečnosť ako oblasť ľudskej činnosti sa veľmi rýchlo vyvíja a neexistuje všeobecne akceptovaná medzinárodná terminológia. To spôsobuje problémy už pri bežnej komunikácii ale zvlášť vypuklo sa prejavuje pri preklade právnych aktov EÚ aj tvorbe vlastnej legislatívy. Ministerstvo

[22] Internet Engineering Task Force
[23] napriek neoficiálnemu statusu ide o de-facto štandardy, z ktorých viaceré sa stali aj oficiálnymi medzinárodnými normami.
[24] pozri Legislatívny zámer zákona o informačnej bezpečnosti, Národnú stratégiu informačnej bezpečnosti v SR a Akčný plán koncepcie kybernetickej bezpečnosti

financií v rámci riešenia úloh definovaných v Národnej stratégii informačnej bezpečnosti v SR iniciovalo pred 15 rokmi projekt systematického budovania terminológie informačnej bezpečnosti, ktorého výsledkom bol pomerne rozsiahly výkladový slovník. V tretej časti uvádzame stručný výber aktualizovaných základných pojmov informačnej bezpečnosti z uvedeného slovníka, doplnený o pojmy zavedené v ZoKB a smernici NIS. Na ilustráciu zložitosti úlohy vytvoriť konzistentnú terminológiu informačnej bezpečnosti uvedieme, že už základný pojem *informačná bezpečnosť* sa používa minimálne v troch rozličných významoch.

- Označuje ideálny stav systému, keď všetko funguje tak ako má, nedochádza k poruchám, chybám, alebo narušeniam systému a/alebo informácií a prostredia, v ktorom systém pôsobí. V tomto význame sa pojem používa, keď sa hovorí o úrovni informačnej bezpečnosti alebo stave informačnej bezpečnosti systému alebo organizácie.
- Informačná bezpečnosť označuje činnosť zameranú na dosiahnutie ideálneho stavu; podstatou tejto činnosti je správa rizík. Manažér informačnej bezpečnosti neorganizuje stav systému, ale činnosti na jeho ochranu, odrážanie útokov, rekonštrukciu systému po havárii alebo útoku.
- Napokon, informačná bezpečnosť predstavuje multidisciplinárnu oblasť, ktorej predmetom je skúmanie hrozieb voči informácii (ktorá sa môže vyskytovať v rozličných etapách svojho životného cyklu, byť zaznamenaná v rôznych formách a spracovávaná pomocou rozličných zariadení, pričom na spracovávaní sa môžu priamo či nepriamo podieľať aj ľudia) a hľadanie riešení, ktoré chránia informáciu pred naplnením hrozieb.

Pojem informačná bezpečnosť sa bez explicitného rozlíšenia používa vo všetkých troch významoch, najčastejšie však na označenie činnosti zameranej na zaistenie ochrany systému, informácií a okolia systému.

V posledných rokoch sa okrem informačnej bezpečnosti sa čoraz častejšie hovorí o kybernetickej bezpečnosti. Pojem kybernetická bezpečnosť je odvodený od pojmu *kybernetický priestor* (*cyberspace*), ktorý prvýkrát použil začiatkom 80-tych rokov 20. storočia spisovateľ Wiliam Gibson v poviedke Burning Chrome a neskôr v románe Neuromancer. Podľa Gibsonovho vlastného vyjadrenia[25] slovo *cyberspace* síce znelo dobre, ale nemalo konkrétny význam. V súvislosti s rozvojom Internetu sa pôvodne bezobsažný pojem kybernetický priestor úspešne ujal a začal sa používať na označenie Internetu, resp. globálnej technickej informačnej a komunikačnej infraštruktúry[26] (počítačov prepojených sieťou). Keďže informačná bezpečnosť má veľmi široký záber a väčšina informácií sa spracováva pomocou digitálnych IKT, ktoré sa v porovnaní so svojím prostredím vyvíjajú extrémne rýchlo,[27] pozornosť informačnej bezpečnosti sa sústreďuje najmä na ochranu informácie v elektronickej forme, spracovávanej pomocou digitálnych IKT, (t.j. v kybernetickom priestore) pred cielenými útokmi. Niekde tam treba hľadať pôvod pojmu kybernetická bezpečnosť, ktorý síce nemá jednoznačne stanovený význam,[28] ale v kľúčovom dokumente EÚ (Stratégia kybernetickej bezpečnosti) sa používa vo význame informačnej bezpečnosti kybernetického priestoru. V pripravovanej terminologickej norme ISO/IEC 27100[29] sa rozlišujú dve základné interpretácie

[25] *All I knew about the word "cyberspace" when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page.*

[26] Cyberspace–the globally interconnected information infrastructure that includes the Internet, telecommunications networks, computer systems, and industrial control systems. In: *Trustworthy cyberspace: Strategic plan for the Federal cybersecurity Research and Development program, Executive Office of the President National Science and Technology Council, December 2011*.

[27] Spracovanie informácií zaznamenaných v listinnej/papierovej podobe ručne.

[28] Definition of Cybersecurity – Gaps and overlaps in standardisation v1.0, ENISA, December 2015.

[29] ISO/IEC NP 27100 Information technology -- Cybersecurity -- Overview and concepts

kybernetickej bezpečnosti. Prvá sa sústreďuje na príčiny a druhá na dôsledky narušenia IKT. Podľa prvej interpretácie je kybernetická bezpečnosť podmnožinou informačnej bezpečnosti, t.j. aktivít zameraných na zachovanie dôvernosti, integrity, dostupnosti a autentickosti informácií v kybernetickom priestore alebo definovanej časti siete. Informácia má hodnotu a je potrebné ju chrániť, narušenie informačnej bezpečnosti je príčinou kyberneticko-bezpečnostných incidentov. Pri tomto chápaní kybernetickej bezpečnosti sa pozornosť sústreďuje na hrozby, ktorých naplnením je úspešný útok na informačné systémy, siete alebo informácie, ktoré sa pomocou nich spracovávajú a prenášajú. Druhá interpretácia kybernetickej bezpečnosti sa zameriava na dôsledky ako sú strata obchodných príležitostí, výpadok kritickej infraštruktúry, poškodenie zdravia alebo straty na životoch, majetková ujma, poškodenie dobrého mena a pod. Časť kyberneticko-bezpečnostných incidentov je spôsobená narušením informačnej bezpečnosti, ale pripravovaná norma vyčleňuje z hrozieb informačnej bezpečnosti poruchy zariadení, neúmyselné ľudské chyby a uvádza nedostatky v kvalite produktov a služieb, ktoré môžu spôsobiť kyberneticko-bezpečnostné incidenty bez toho, aby došlo k narušeniu informačnej bezpečnosti.
Smernica NIS nehovorí o kybernetickom priestore ani o kybernetickej bezpečnosti; namiesto kybernetického priestoru používa pojem „siete a informačné systémy“ a nepriamo definuje kybernetickú bezpečnosť nasledovne:
„bezpečnosť sietí a informačných systémov“ je schopnosť sietí a informačných systémov odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov[30];

t.j. chápe ju ako informačnú bezpečnosť (časti) kybernetického priestoru.

Z praktického hľadiska je rozlišovanie kybernetickej a informačnej bezpečnosti nepodstatné. Organizácia[31] potrebuje pre plnenie svojich úloh spoľahlivo fungujúce informačné systémy a informácie, na ktorých dostupnosť, dôvernosť a autentickosť sa môže spoľahnúť. Hoci sa väčšina informácií spracováva automatizovane v informačných systémoch, je potrebné chrániť aj informáciu, ktorá nie je v elektronickej forme, riešiť fyzickú, personálnu bezpečnosť, právne vzťahy, štandardy, chrániť bezpečnostné okolie systému a neobmedzovať sa len na cielené útoky na infraštruktúru. Kybernetická bezpečnosť preberá terminológiu a riešenia informačnej bezpečnosti. Momentálne existuje cca. 200 noriem venovaných rozličným aspektom informačnej bezpečnosti a len dve (ISO/IEC 27032 a ISO/IEC 27103) venované kybernetickej bezpečnosti. Prvá sa hneď v preambule odvoláva na základnú terminologickú normu informačnej bezpečnosti ISO/IEC 27000 a druhá uvádza, že ISMS je overený spôsob, ako v organizácii implementovať na riziku postavený prístup ku kybernetickej bezpečnosti[32] . Striktné odlíšenie kybernetickej a informačnej bezpečnosti by sťažilo až znemožnilo používanie terminológie a štandardov informačnej bezpečnosti a viedlo k nutnosti vypracovať vlastné štandardy pre kybernetickú bezpečnosť, čo vzhľadom na rozsah a možnú nekompatibilitu nie je reálne. Vzhľadom na už spomenutý význam IKT v dnešnej spoločnosti predstavujú digitálne IKT jednak súčasť prvkov/systémov kritickej infraštruktúry spoločnosti (riadiace systémy v doprave, výrobných linkách, bankové, finančné systémy, nemocničné informačné systémy, informačné systémy poisťovní, kľúčové

[30] V origináli: ‘security of network and information systems’ means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the *availability*, *authenticity*, *integrity or confidentiality* of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.
[31] v primeranej miere to platí aj pre štát
[32] Information Security Management System (ISMS) as described in ISO/IEC 27001 is a well proven way for any organization to implement a risk-based approach to cybersecurity.

štátne registre a pod.), ale aj samotné tvoria kritickú informačnú a komunikačnú infraštruktúru spoločnosti. Vďaka tomu sa stávajú potenciálnymi cieľmi útokov hackerov, zločineckých skupín, teroristických organizácií, ale aj cudzím štátom podporovaných inštitúcií. Kybernetický priestor sa stal bojiskom rovnocenným klasickým bojovým priestorom (zem, voda, vzduch, kozmický priestor) a nepriateľské aktivity, ktoré v ňom prebiehajú, sa rozsahom a charakterom podobajú vojenským operáciám. Vojna v kybernetickom priestore je asymetrická, prostriedky postačujúce na útok sú ďaleko menšie ako prostriedky potrebné na ochranu pred ním a útočník nemusí byť počítačový génius aby odhalil využiteľnú dieru v systéme, pretože potrebné informácie spolu s nástrojmi na využitie odhalenej zraniteľnosti nájde na Internete.

Informačná revolúcia posunula ľudstvo do novej etapy jeho vývoja, informačnej spoločnosti. Informačná spoločnosť už v súčasnej fáze svojho vývoja poskytuje ľuďom nebývalé možnosti prakticky vo všetkých tradičných oblastiach činnosti a otvára nové oblasti. Využívanie týchto možností závisí od spoľahlivého fungovania technologickej infraštruktúry, t.j. zaistenia informačnej/kybernetickej bezpečnosti. (To je však len nutná podmienka, lebo dobre fungujúce a zabezpečené IKT možno použiť aj na poškodenie až zničenie spoločnosti. Ošetrenie rizík vyplývajúcich z hrozby zneužitia IKT na nekalé ciele však presahuje možnosti informačnej aj kybernetickej bezpečnosti).

Ale aj plnenie (z tohto hľadiska) podstatne menej ambicióznej úlohy, ktorou je zaistenie dostatočnej úrovne informačnej bezpečnosti si vyžaduje systematické riešenie a efektívnu spoluprácu na všetkých úrovniach – medzinárodnej, štátnej, organizácie i jednotlivcov.

3 Referencie

[1] FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

[2] FIPS 200 Minimum Security Requirements for Federal Information and Information SystemsISO/IEC 27000 -- Information security management system -- Overview and vocabulary

[3] ISO/IEC 27001 — Information security management systems — Requirements.

[4] ISO/IEC 27002 — Code of practice for information security management.

[5] ISO/IEC 27004 (2016) — Information security risk management. Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation

[6] ISO/IEC 27005 — Information security risk management.

[7] ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems

[8] ISO/IEC 27007 — Guidelines for information security management systems auditing (focused on auditing the management system)

[9] ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (focused on auditing the information security controls)

[10] ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity

[11] ISO/IEC 27032:2012 — Information technology — Security techniques — Guidelines for cybersecurity

[12] ISO/IEC 27035-1 — Information security incident management - Part 1: Principles of incident management

[13] ISO/IEC 27035-2 — Information security incident management - Part 2: Guidelines to plan and prepare for incident response

[14] ISO/IEC NP 27035-3 [vo vývoji] Information technology -- Security techniques -- Information security incident management -- Part 3: Guidelines for incident response operations

[15] NIST SP 800 – 30 Risk Management Guide for Information Technology Systems.

[16] NIST SP 800 – 61 Computer Security Incident Handling Guide

[17] NIST SP 800 – 83 Guide to Malware Incident Prevention an Handling

[18] BSI Standard 100-1 Information Security Management System (ISMS)

[19] BSI Standard 100-2 IT-Grundschutz Methodology

[20] BSI Standard 100-3 Risk analysis on the basis of IT-Grundschutz

[21] BSI Standard 100-4 Business continuity management.

[22] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013.

[23] Definition of Cybersecurity – Gaps and overlaps in standardisation v1.0, ENISA, December 2015.

[24] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

[25] Tézy vykonávacích právnych predpisov k návrhu zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, NRSR tlac_0763-TVPP

[26] Vykonávací predpis podľa § 32 ods. 1 písm. d), ktorým sa ustanovujú bezpečnostné štandardy a znalostné štandardy v oblasti kybernetickej bezpečnosti [§ 5 ods. 1 písm. w), § 20 ods. 1].

[27] Dôvodová správa k zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

Malý výkladový slovník termínov informačnej a kybernetickej bezpečnosti

Táto časť obsahuje stručný výkladový slovník termínov informačnej a kybernetickej bezpečnosti. Základom je medzinárodná terminológia informačnej bezpečnosti, kybernetická bezpečnosť používa terminológiu informačnej bezpečnosti. Medzinárodná terminológia informačnej bezpečnosti je anglická, slovenská odborná verejnosť používa medzinárodnú terminológiu a len málo anglických termínov je adekvátne preložených do slovenčiny. Preto je tento slovník postavený ako výkladový a nie terminologický. Heslá slovníka sú organizované nasledovne: **slovenský termín, [jeho anglický ekvivalent]**, výklad pojmu. Ak sa vo výklade používajú iné termíny, ktoré sa nachádzajú v slovníku, sú vysádzané *kurzívou* a označené **→.** Viacslovné termíny sú usporiadané podľa kľúčového slova. Pri skratkách vo všeobecnosti a pri anglických skratkách, ktoré nemajú slovenský ekvivalent zvlášť, uvádzame odkaz na heslo vykladajúce pojem označený skratkou. Pojmy, ktoré nemajú slovenský ekvivalent, uvádzame pod pôvodným anglickým názvom.
Základom pre tento slovník je Výkladový slovník informačnej bezpečnosti, ktorý sme vypracovali pre MF SR v roku 2009 a v nasledujúcom období dopĺňali a aktualizovali. Vybrali sme z neho pojmy, ktoré sú dôležité pre pochopenie informačnej bezpečnosti a základných problémov, ktoré rieši a doplnili sme pojmy použité v ZoKB a smernici NIS.

A

akreditácia [accreditation] 1. procedúra, pomocou ktorej akreditujúci orgán overí, či je organizácia alebo osoba spôsobilá na vykonávanie špecifických úloh; 2. formálna deklarácia kompetentného (akreditačného) orgánu, že organizácia alebo osoba je spôsobilá na vykonávanie špecifických úloh; 3. formálna deklarácia kompetentného (akreditačného) orgánu, že systém je oprávnený fungovať v konkrétnom bezpečnostnom móde s použitím predpísanej množiny bezpečnostných služieb.

akreditácia CSIRT [CSIRT accreditation] 1. procedúra, pomocou ktorej NBÚ ako akreditačný orgán overuje, či jednotka CSIRT spĺňa požiadavky stanovené zákonom; 2. formálna deklarácia NBÚ ako kompetentnej akreditačnej autority, že jednotka CSIRT spĺňa požiadavky stanovené zákonom.

aktívum [asset] čokoľvek, čo má pre organizáciu hodnotu. Aktíva sú hmotné (zariadenia, infraštruktúra, personál) a nehmotné (peniaze, informácie, know-how, dobré meno). Môžu sa stať objektom →*hrozby* alebo cieľom →*útoku* a vyžadujú si ochranu.

analýza kybernetického bezpečnostného incidentu [cybersecurity incident analysis] systematická činnosť, ktorej cieľom je zistiť, ktorá hrozba spôsobila kybernetický bezpečnostný incident, na aké aktíva pôsobila, akú zraniteľnosť využila, ako jej naplnenie časovo prebiehalo, akým spôsobom bol bezpečnostný incident detegovaný, ako prebiehalo jeho riešenie a aké boli jeho dopady.

analýza rizík [risk analysis] proces pochopenia podstaty rizika a stanovenia →*úrovne rizika.*

anonymita [anonymity] 1. bezpečnostná služba umožňujúca používateľovi systému využívať zdroje systému bez prezradenia používateľovej →*identity*; 2. →*bezpečnostná požiadavka* na riešenie, systém alebo nejakú službu, aby pri interakcii používateľa so systémom (používaní riešenia, služby) nebola prezradená používateľova identita.

antivírový softvér, antivírus [antivirus software] program, ktorý monitoruje počítač alebo počítačovú sieť, aby odhalil všetky typy škodlivého kódu a zabránil bezpečnostným incidentom spôsobeným škodlivým kódom alebo ich pomáhal riešiť.

aplikačné programové vybavenie (počítača) [application software] program slúžiaci na riešenie špecifických úloh používateľa.

atribút [attribute] vlastnosť, charakteristická črta alebo prívlastok →*entity*, ktorý môže kvantitatívne alebo kvalitatívne rozlíšiť človek, technické zariadenie alebo program.

audit [audit] formálne preskúmanie, preskúšanie alebo →*verifikácia* skutočného stavu systému alebo jeho definovanej časti na zhodu alebo súlad so stanovenými očakávaniami.

audit, bezpečnostný [security audit] preskúmanie stavu a účinnosti bezpečnostných opatrení systému alebo organizácie. Pri bezpečnostnom audite sa posudzujú opatrenia zo zoznamu opatrení, ktoré mali byť implementované, alebo úroveň bezpečnosti systému alebo organizácie oproti požadovanej úrovni.

autentifikácia/autentizácia [authentication] potvrdenie deklarovanej →*identity* určitej →*entity.*

autentickosť [autenticity] vlastnosť, ktorá znamená, že deklarovaná identita entity je pravdivá.

autorizácia [authorization] udelenie →*oprávnení* určitej →*entite* na prístup k zdrojom systému/organizácie a/alebo na ich využívanie

B

bezpečnostná architektúra [security architecture] súbor princípov, ktoré popisujú (a) bezpečnostné služby, ktoré od systému požadujú jeho používatelia, (b) komponenty systému, ktoré majú implementovať dané služby, (c) výkonnostné úrovne/parametre jednotlivých komponentov potrebné na to, aby sa dokázali vysporiadať s predpokladanými →*hrozbami*.

bezpečnostná dokumentácia [security documentation] bezpečnostné politiky, štandardy, procedúry, výsledky analýzy rizík, výsledky auditov a iné dokumenty relevantné z hľadiska informačnej/kybernetickej bezpečnosti systému alebo organizácie.

bezpečnostná funkcia [security function] implementačne nezávislý spôsob realizácie →*bezpečnost-nej požiadavky*; →*bezpečnostné opatrenie* je realizáciou jednej alebo viacerých bezpečnostných funkcií.

bezpečnostná politika (inštitúcie) [security policy] formálny dokument schválený vedením inštitúcie, ktorým sa podrobnejšie rozpracovávajú bezpečnostné ciele inštitúcie, upresňuje úroveň →*bezpečnostných požiadaviek*, stanovuje zodpovednosť za →*informačnú bezpečnosť* v inštitúcii a rámcovo definujú spôsoby na dosiahnutie stanovených cieľov.

bezpečnostná požiadavka [security requirement] špecifikácia ohraničení na usporiadanie →*aktíva*, spôsob jeho používania alebo na činnosť inštitúcie, ktorých cieľom je eliminácia alebo zníženie hodnoty→*rizika* spojeného s používaním aktíva, alebo činnosťou inštitúcie.

bezpečnostná udalosť [security event] udalosť, ktorá má, alebo môže mať vplyv na bezpečnosť subjektu.

bezpečnostná záruka [security assurance] miera naplnenia →*bezpečnostnej požiadavky* odvodená od spôsobu (→*bezpečnostných opatrení*), akým bola bezpečnostná požiadavka realizovaná.

bezpečnostné opatrenie [security measure/control] technické, organizačné, právne alebo iné riešenie, ktoré úplne alebo čiastočne odstraňuje → *zraniteľnosť* aktíva, a/alebo znižuje pravdepodobnosť naplnenia →*hrozby* a/alebo v prípade jej naplnenia znižuje jej dopad na aktívum a organizáciu, ktorá ho vlastní.

bezpečnostné opatrenie, sektorové [sector security

measure/control] →*bezpečnostné opatrenie* špecifické pre niektorý sektor alebo podsektor uvedený v ZoKB.

bezpečnostné opatrenie, všeobecné [general security measure/control] pozri →*bezpečnostné opatrenie.*

bezpečnostné povedomie [awareness] poznanie potreby ochrany informácie a IKT, ako aj povinnosti osobne sa na nej podieľať.

bezpečnostné prostredie [security environment] súbor externých →*entít*, procedúr, pravidiel a podmienok, ktoré majú vplyv na bezpečný vývoj, prevádzku, činnosť a údržbu systému.

bezpečnostné smernice [security directives] sú podrobnejším opisom jednotlivých →*bezpečnostných opatrení* a spravidla pozostávajú z opisu zavedených technických, organizačných, právnych, personálnych a iných riešení.

bezpečnostný incident [security incident] pozri →*incident.*

bezpečnostný mechanizmus [security mechanism] konkrétna implementácia →*bezpečnostnej funkcie.*

bezpečnostný projekt [security project] komplexné posúdenie bezpečnostných potrieb/požiadaviek na systém a návrh spôsobu, ako im efektívne vyhovieť. Pozostáva z →*bezpečnostného zámeru,* →*analýzy rizík a* →*bezpečnostných smerníc.*

bezpečnostný zámer [security target]

formálny dokument schválený vedením inštitúcie, ktorým vedenie inštitúcie deklaruje základné ciele inštitúcie v oblasti →*informačnej bezpečnosti.*

bezpečnosť, fyzická [physical security] fyzické prostriedky na ochranu systému pred krádežou, zneužitím, náhodným poškodením, technickými poruchami a prírodnými vplyvmi.

bezpečnosť, informačná [information security] 1. ideálny stav systému, kedy systém funguje v súlade s očakávaniami (→*bezpečnostnou politikou*); 2. multiodborová disciplína, ktorá sa zaoberá →*hrozbami* voči →*systémom/aktívam* a metódami, ako aktíva pred hrozbami chrániť; 3. činnosti zamerané na dosiahnutie ideálneho stavu systému.

bezpečnosť, kybernetická [cyber security] systém opatrení na zaistenie odolnosti →*kybernetického priestoru*, ako aj činností a prostriedkov zameraných na dosiahnutie požadovanej úrovne bezpečnosti prvkov

kybernetického priestoru vrátane riešenia incidentov a následných opatrení a činností.

bezpečnosť, personálna [personel security] pozri personálna bezpečnosť.

bezpečnosť prostredia [enviromental security] fyzické opatrenia na zaistenie ochrany aktív organizácie pred prírodnými katastrofami, vplyvom prostredia, útokmi alebo nehodami.

binárne údaje [binary data] údaje zapísané (kódované) pomocou dvojprvkovej abecedy - {0,1}.

citlivá informácia [sensitive information] 1. informácia, ktorej odhalenie, zmena, zničenie alebo zneprístupnenie môže mať negatívny dopad na jej vlastníka alebo používateľa; 2. informácia, ktorá je za citlivú prehlásená zákonom alebo vnútornými predpismi organizácie.

citlivá ale neklasifikovaná informácia [sensitive but unclassified information] informácia, ktorá nie je označená ako *klasifikovaná* (v SR utajované skutočnosti), ale narábanie s ktorou je upravené legislatívou alebo vnútornými predpismi organizácie.

cloud computing je paradigma IT, umožňujúca používateľom cloudu rýchly prístup k zdieľanému súboru konfigurovateľných systémových zdrojov a vysokoúrovňových služieb a poskytujúca možnosť ich využívania prakticky z ľubovoľného systému prostredníctvom počítačovej siete, najčastejšie Internetu. Používateľ pritom nepotrebuje adresovať alebo manažovať jednotlivé prvky cloudu (hardvérové a sofvérové komponenty cloudu spravuje poskytovateľ cloudu) a z toho hľadiska sa celý súbor hardvérových a softvérových komponentov javí ako amorfný oblak (cloud).

D

dekóder [decoder] systém alebo zariadenie, ktoré dekóduje prijatú kódovanú informáciu.

dekódovanie [decoding] inverzná transformácia kódovacej transformácie, ktorej úlohou je transformovať informáciu do podoby, ktorú mala pred zakódovaním. Pozn. pri dekódovaní dochádza k rozbaľovaniu komprimovanej informácie, oprave chýb, ktoré vznikli pri prenose alebo uchovávaní informácie.

demodulátor [demodulator] technické zariadenie transformujúce prijatý signál na postupnosť znakov.

Deň Jedna [Day One] deň, kedy je zverejnená záplata na odhalenú →*zraniteľnosť* systému alebo aplikácie.

Deň Nula [Day Zero] deň, keď sa odhalí nová →*zraniteľnosť* systému alebo aplikácie.

detekcia prieniku [intrusion detection] odhalenie neoprávneného prístupu do systému.

detekcia kybernetického bezpečnostného incidentu [cybersecurity incident detection] odhalenie, že v organizácii alebo systéme došlo ku →*kybernetickému bezpečnostnému incidentu*.

digitálne informačné a komunikačné technológie, IKT [digital information and communication technology] →*informačné a komunikačné technológie,* ktoré vznikli spojením počítačov, telekomunikačných sietí a masovokomunikačných prostriedkov, využívajúce digitálne kódovanie informácie a spoločné →*komunikačné kanály* pre prenos údajov.

digitálne údaje [digital data] údaje zaznamenané (kódované) pomocou postupnosti číslic.

distribuovaný útok typu denial of service [distributed denial of service attack, DDoS] →*útok typu denial of service,* vedený z viacerých počítačov na cieľový systém, so zámerom spôsobiť jeho preťaženie a zamedziť mu poskytovanie služieb.

dopad hrozby [threat impact] negatívne dôsledky naplnenia hrozby na aktívach organizácie.

dosledovateľnosť [accountability] →*bezpečnostná požiadavka* (na systém), aby bolo možné stanoviť, kto je zodpovedný za bezpečnostne relevantné aktivity v systéme.

dostupnosť [availability] požiadavka, aby zdroje systému boli k dispozícii oprávnenej osobe 1. vždy keď o to požiada; 2. do času *t* od okamihu, keď o to požiada; 3. s pravdepodobnosťou meranou podielom doby, keď sú požadované zdroje k dispozícii ku celkovej dobe (napr. 24 x 7 znamená, že systém je dostupný nepretržite 24 hodín denne a 7 dní v týždni).

dôvera [trust] 1. pocit istoty (často nepodložený), že (a) systém nezlyhá, (b) že systém robí len to, čo má robiť a nevykonáva žiadne nežiadúce činnosti; 2. vo všeobecnosti, ak entita A dôveruje entite B, znamená, že entita A predpokladá, že sa entita B bude správať presne tak, ako entita A očakáva.

dôvernosť [confidentiality] 1. →*bezpečnostná požiadavka*, ktorej naplnenie znamená, že sa informáciu obsiahnutú v správe (dokumente) nedozvedia nepovolané osoby; 2. druhý najnižší stupeň klasifikačnej schémy utajovaných skutočností.

dôveryhodná služba [trust service] nesprávny preklad anglického pojmu; služba na zabezpečenie dôveryhodnosti (bezpečnosti a právnej validity) elektronických transakcií.

dôveryhodná (overená) výpočtová báza [trusted computing base] bezpečnostné jadro systému predstavované súborom →*bezpečnostných mechanizmov* systému (hardvérových, softvérových a firmvérových), ktorých kombinácia je zodpovedná za presadzovanie →*bezpečnostnej politiky*.

dvojfaktorová autentifikácia [two-factor autentication] →*autentifikácia* →*entity* na základe dvoch nezávislých metód overenia jej proklamovanej →*identity.*

E

elektronická verejná správa [e-Government] výkon úkonov súvisiacich s verejnou správou elektronickou formou (komunikácia pomocou osobných elektronických schránok, vedenie agendy v elektronickej forme, poskytovanie informácií pomocou webových stránok, používanie elektronických formulárov a pod.).

elektronická identifikácia [electronic identification] identifikácia entity (napr. človeka, dokumentu) pomocou elektronických prostriedkov. V prípade človeka napríklad pomocou zadania prihlasovacieho mena (login-u) do systému.

elektromagnetické spektrum [electromagnetic spectrum] rozsah frekvencií elektromagnetických vĺn, ich vlnových dĺžok a energie fotónov. Frekvencie elektromagnetických vĺn siahajú od 1 Hz po 10^{25} Hz.

elektronická komunikačná sieť [electronic communication network] systém pozostávajúci z prenosových kanálov a zariadení na ich prepájanie, smerovanie signálu, umožňujúci prenos elektromagnetických signálov bez ohľadu na typ prenášanej informácie. (Na prenos

informácie sa používajú elektromagnetické vlny s vlnovou dĺžkou od rádovo 10^{-7} m (viditeľné svetlo) až po 10^{5} m (rádiové vlny).

eliminácia rizika {risk elimination] pozri *riziko, eliminácia*

entita [entity] akýkoľvek objekt (človek, zviera, vec, myšlienka, abstraktný objekt), ktorý je jedinečný a zhodný len so sebou samým (t.j. niečím sa odlišuje od podobných objektov). Entita sa vyznačuje množinou →*atribútov*, ktoré tvoria jej →*identitu*.

efektivita [efficiency] vzťah medzi dosiahnutými výsledkami a vynaloženým úsilím (vynaloženými zdrojmi).

externý kontext [external context] vonkajšie prostredie, v ktorom sa organizácia snaží dosiahnuť svoje ciele.

evidencia kybernetického bezpečnostného incidentu [cybersecurity incident registration/record] 1. zaznamenanie a

uchovávanie informácií o kybernetickom bezpečnostnom incidente; 2. záznam o kybernetickom bezpečnostnom incidente.

F

fyzická bezpečnosť [physical security] pozri →*bezpečnosť, fyzická*.

H

hacker [hacker] človek hľadajúci →*zraniteľnosti* systémov s cieľom využiť ich na prienik do systémov. Hacker sa neusiluje ani o zisk, ani o poškodenie systémov.

hardvér [hardware] technická časť počítačového systému.

havária [emergency] bezpečnostná udalosť, ktorá spôsobila, že zdroje alebo procesy v organizácii nefungujú tak ako by mali, ich dostupnosť sa nedá obnoviť v požadovanom časovom rámci a vyžaduje si špeciálny zásah. Havária vážne narušuje činnosť organizácie.

heslo [password] tajný reťazec znakov známy len určitej →*entite* (a overovateľovi →*identity*), ktorý sa používa na →*autentifikáciu* danej →*entity*.

hrozba [threat] objektívne existujúca potenciálna možnosť priamo alebo nepriamo narušiť systém, informáciách, ktoré sa v ňom spracovávajú alebo iné aktíva organizácie.

hrozba, kybernetická [cyber threat] hrozba voči →*aktívam* →*kybernetického priestoru* alebo hrozba realizovateľná kybernetickými prostriedkami (prostriedkami kybernetického priestoru).

I

identifikácia [identification] deklarácia →*identity* nejakej →*entity* (v praxi napr. prihlásenie sa do systému menom).

identifikačné kritériá kybernetických bezpečnostných incidentov [cybersecurity incidents identification criteria] kritériá na identifikovanie závažných kybernetických bezpečnostných incidentov a ich zaradenie do jednej z troch tried podľa závažnosti dopadu.

identifikátor [identifier] informačný alebo materiálny objekt na základe ktorého je možné jednoznačne určiť buď →*identitu entity*, alebo samotnú →*entitu*

identita [identity] množina →*atribútov* nejakej entity, ktorá ju jednoznačne odlišuje od iných entít podobného druhu v nejakej →*oblasti aplikovateľnosti identity*. Identita je meno, osobné údaje nejakého človeka, identifikátor, preukaz, rodné číslo a pod.

incident [incident] udalosť alebo situácia, ktorá spôsobí alebo môže spôsobiť nežiadúce prerušenie činnosti, stratu, núdzový stav alebo krízu v nejakej organizácii, alebo v systéme.

informácia [information] základný pojem s rozličnou interpretáciou v rôznych oblastiach. V informatike informácia predstavuje opis nejakej skutočnosti (reálnej alebo fiktívnej) zaznamenaný v podobe →*údajov*. Informácia predstavuje obsah údajov a údaje sú formou zápisu informácie.

informácia, klasifikácia [information classification] pozri →*klasifikácia údajov*.

informačná a komunikačná infraštruktúra [information and communication infrastructure] pozri →*infraštruktúra, informačná*.

informačná bezpečnosť [information security] pozri →*bezpečnosť, informačná*.

informačné a komunikačné technológie, IKT [information and communication technology, ICT] 1. metódy, prostriedky a zariadenia na záznam, prenos, uchovávanie a spracovanie informácie; 2. →*digitálne informačné a komunikačné technológie*.

informačné prostredie [information environment] informačné prostredie subjektu pozostáva z: informácií, ktoré subjekt používa/spracováva, entít[33], ktoré sa na spracovaní informácie podieľajú, komunikačných kanálov a informačných tokov, pravidiel upravujúcich spracovanie informácií.

informačný systém [information system] aplikácia, služba, technické zariadenie alebo iný prvok, ktorý spracováva informáciu.

informačný systém verejnej správy [public administration information system] informačný systém v pôsobnosti povinnej osoby ako správcu informačného systému verejnej správy podporujúci služby verejnej správy, služby vo verejnom záujme a verejné služby.

infraštruktúra [infrastructure] z hľadiska organizácie je infraštruktúrou všetko to, čo sa priamo nepodieľa na plnení poslania organizácie, vrátane toho, čo organizácia nevlastní, ale čo pre plnenie svojho poslania nevyhnutne potrebuje.

infraštruktúra, kritická [critical infrastructure] →*infraštruktúra*, ktorej narušenie, zneprístupnenie alebo znefunkčnenie môže spôsobiť stratu schopnosti organizácie[34] plniť svoje poslanie, spôsobiť jej finančnú stratu, ktorú nedokáže kompenzovať alebo spôsobí ohrozenie zdravia a života ľudí.

infraštruktúra, informačná [information infrastructure] →*infraštruktúra*, ktorá slúži na získavanie, prenos, spracovávanie a uchovávanie informácií.

infraštruktúra informačná, kritická [critical information infrastructure] informačná →*infraštruktúra*, ktorej narušenie by ohrozilo fungovanie organizácie

integrita [integrity] 1. základná →*bezpečnostná požiadavka* na údaje, ktorej naplnenie znamená, že údaje nie je možné zmeniť bez toho, aby to ich vlastník alebo adresát nemohol zistiť; 2. v širšom zmysle je integrita bezpečnostná požiadavka na vylúčenie neoprávnených zmien v systémoch; t.j. zmien hardvéru, programového vybavenia alebo údajov.

ISO/IEC 27000 — Information security management system -- Overview and vocabulary úvodná norma k sérii medzinárodných noriem manažmentu informačnej bezpečnosti, obsahujúca prehľad existujúcich noriem série a terminologický slovník.

ISO/IEC 27001 — Information security management systems — Requirements. Toto je stručná norma obsahujúca požiadavky, ktoré musia spĺňať systémy manažmentu IB (ak majú získať certifikáciu podľa ISO/IEC 27001). Tieto požiadavky sú podrobnejšie rozpracované v norme *ISO/IEC 27002*.

ISO/IEC 27002 — Code of practice for information security management. Táto norma obsahuje 114 opatrení, ktoré je potrebné zaviesť na naplnenie požiadaviek stanovených v norme ISO/IEC 27001. Norma je základom pre záväzné bezpečnostné štandardy ISVS.

ISO/IEC 27005 — Information security risk management. Norma, ktorá popisuje správu rizík, vrátane podrobného postupu pri analýze rizík.

[33] Entitami sú ľudia, organizačné jednotky, IKT systémy a pod.

[34] Organizáciou môže byť súkromná spoločnosť, orgán verejnej moci alebo správy, príp. aj štát.

ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems - norma stanovujúca požiadavky na orgány vykonávajúce audit a certifikáciu ISMS.

ISO/IEC 27007 — Guidelines for information security management systems auditing (focused on auditing the management system) návod na audit ISMS.

ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (focused on auditing the information security controls) návod na audit bezpečnostných opatrení.

ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity norma popisujúca vytvorenie a fungovanie systému manažmentu kontinuity činnosti.

ISO/IEC 27032:2012 — Information technology — Security techniques — Guidelines for cybersecurity norma venovaná kybernetickej bezpečnosti.

J

jednotný informačný systém kybernetickej bezpečnosti, JISKB [cybersecurity integrated information system] špeciálny informačný systém, ktorý má od roku 2019 prevádzkovať a spravovať NBÚ. JISKB má slúžiť na zber a spracovanie informácií o kybernetických bezpečnostných incidentoch v SR, ako bezpečný komunikačný kanál, analytický nástroj, informačný zdroj a centrálny systém včasného varovania.

K

kanál, komunikačný [communication channel] 1. fyzické médium (kovový vodič, optické vlákno, priestor pre šírenie signálov a pod.) ktoré je schopné sprostredkovať šírenie signálov, prenášajúcich informáciu; 2. logické spojenie medzi účastníkmi komunikácie, ktoré môže byť vytvorené *ad hoc* len pre konkrétnu komunikáciu a môže využívať rôzne druhy fyzických médií.

kanál, skrytý [covert channel] metóda prenosu →*informácie* pomocou vedľajšieho (skrytého) efektu nejakej udalosti alebo činnosti nejakého mechanizmu pôvodne určeného na iný účel.

kategórie závažných kybernetických bezpečnostných incidentov [serious cybersecurity incident categories] tri kategórie →*závažných kybernetických bezpečnostných incidentov* odstupňované podľa rozsahu dopadu; najmenej závažné sú incidenty prvej a najzávažnejšie sú incidenty tretej kategórie.

kategorizácia informačných systémov a sietí [information systems and networks categorization] rozdelenie informačných systémov a sietí do nejakých tried/kategórií podľa klasifikačných kritérií. ZoKB neuvádza explicitnú klasifikačnú schému, ale implicitne rozdeľuje informačné systémy a siete na dve kategórie – tie, na ktoré sa vzťahuje a ostatné.

klasifikácia údajov [data classification] (bezp.) kategorizácia, posúdenie potrieb ochrany údajov z hľadiska →*dostupnosti,* →*dôvernosti,* →*integrity,* →*autentickosti* a i. a ich následné

zaradenie do klasifikačnej kategórie (triedy) zodpovedajúcej týmto potrebám.

klasifikačná schéma [classification scheme] zvyčajne systém hierarchicky usporiadaných tried, spolu s pravidlami, umožňujúcimi zaradiť údaje do práve jednej z tried a →*bezpečnostnými požiadavkami* pre jednotlivé triedy.

klasifikovaná informácia [classified information] 1. (všeob.) informácia zaradená do niektorej z klasifikačných tried; 2. (SR) informácia patriaca medzi utajované skutočnosti.

kód [code] 1. množina kódových slov; 2. program; 3. text programu.

kóder [encoder] systém alebo zariadenie na kódovanie údajov.

kódovanie [encoding] transformácia údajov (informácie) na postupnosť kódových slov nejakého kódu.

kompromitácia [compromise] strata dôvery, ohrozenie, vystavenie podozreniu. Napr. kompromitácia tajného kľúča znamená odôvodnené podozrenie, že k tajnému kľúču sa dostala neoprávnená osoba (a teda sa viac nedá používať na šifrovanie správ).

komunikačný kanál [communication channel] pozri →*kanál, komunikačný*.

Koncepcia kybernetickej bezpečnosti Dokument vypracovaný NBÚ, schválený Vládou SR (17. júna 2015), ktorý popisuje východiská a stanovuje ciele SR v oblasti kybernetickej bezpečnosti na roky 2015-2020.

konfigurácia systému [system configuration] 1. špecifikácia systému, jeho prvkov, vzťahov medzi nimi, procesov, stavov, okolia systému; 2. nastavenie parametrov systému.

kontaktná osoba [contact person] 1. osoba, ktorá zberá informácie o bezpečnostných incidentoch, eviduje ich a informuje o nich NBÚ; 2. poverená osoba, ktorá v organizácii prijíma informácie o bezpečnostne relevantných udalostiach v organizácii, v prípade podozrenia na bezpečnostný incident aktivuje procedúru riešenia bezpečnostných incidentov, komunikuje so subjektami, ktoré je organizácia povinná o bezpečnostnom incidente informovať (postihnuté subjekty, subjekty podieľajúce sa na riešení bezpečnostného incidentu, NBÚ, ÚOOÚ a pod.), s médiami a verejnosťou.

kontaktný bod [contact point] v organizácii osoba, alebo organizačná zložka, prostredníctvom ktorej v istej vecnej oblasti (napr. informačnej bezpečnosti) prebieha komunikácia s externými subjektami (ich kontaktnými bodmi). Kontaktný bod pôsobí aj vo vnútri organizácie, zberá relevantné informácie a distribuuje ich (podobne informácie od externých subjektov) zainteresovaným osobám a organizačným zložkám (napr. varovania).

kontaktný bod, národný, NKP [national contact point, NCP] organizácia štátu A zabezpečujúca v istej vecnej oblasti komunikáciu subjektov štátu A so subjektami štátu B prostredníctvom národného kontaktného bodu štátu B. Ak existuje centrálna autorita (na európskej úrovni), národný kontaktný bod zabezpečuje aj komunikáciu s touto centrálnou autoritou. Národný kontaktný bod tvorí rozhranie voči domácim organizáciám (ich systémom) a ostatným NKP a umožňuje komunikáciu domácich organizácií so zahraničnými bez nutnosti zosúlaďovať nastavenie ich systémov. V oblasti kybernetickej bezpečnosti plní úlohu národného kontaktného bodu SR Národný bezpečnostný úrad.

kontinuita činnosti [business continuity] kroky, ktoré organizácia podniká na to, aby zabezpečila nepretržitú dostupnosť svojich kľúčových funkcií (služieb, zdrojov) pre ich oprávnených používateľov.

kritériá pre klasifikáciu kybernetických bezpečnostných incidentov [cybersecurity incident classification criteria] kritériá pre určenie závažných kybernetických bezpečnostných incidentov a ich zaradenie do jednej z kategórií podľa miery dopadu:

- počet používateľov základnej služby alebo digitálnej služby zasiahnutých kybernetickým bezpečnostným incidentom,
- dĺžka trvania kybernetického bezpečnostného incidentu,
- geografické rozšírenie kybernetického bezpečnostného incidentu,
- stupeň narušenia fungovania základnej služby alebo digitálnej služby,
- rozsah vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu.

kritická infraštruktúra [critical infrastructure] pozri →*infraštruktúra, kritická.*

kritická informačná infraštruktúra [critical information infrastructure] pozri

→*infraštruktúra informačná, kritická.*

kritický prvok [critical element] 1. prvok systému, ktorý je pre jeho existenciu a fungovanie nenahraditeľný; 2. prvok kritickej infraštruktúry.

kryptoanalýza [cryptanalysis] 1. vedná disciplína zaoberajúca sa vývojom metód lúštenia (rozbíjania) →*šifier*; 2. →*lúštenie (rozbíjanie) šifry*

kryptografia [cryptography] vedná disciplína zaoberajúca sa návrhom →*kryptosystémov (šifier)*.

kryptografická transformácia [cryptographic transformation] →*šifrovacia* alebo →*dešifrovacia transformácia*.

kryptografický kľúč [cryptographic key] parameter →*kryptografických transformácií*. Môže byť utajovaný, ale aj verejne známy (v prípade →*asymetrických kryptosystémov*).

kryptológia [cryptology] vedná disciplína

zaoberajúca sa štúdiom →*kryptosystémov (šifier)*. Pozostáva z →*kryptografie a* →*kryptoanalýzy*.

kryptosystém [cryptosystem] dvojica →*kryptografických transformácií* (E, D), kde E je →*šifrovacia* a *D* →*dešifrovacia transformácia*.

kryptosystém s verejným kľúčom [public key cryptosystem] →*asymetrická šifra*, pre ktorú má každý jej používateľ dvojicu kryptografických kľúčov: súkromný a verejný. →*Súkromný kľúč* je utajený a →*verejný kľúč* je zverejnený napr. pomocou →*certifikátu verejného kľúča*. Na →*šifrovanie* správy odosielateľ používa →*verejný kľúč* adresáta, adresát šifrovú správu →*dešifruje* pomocou svojho →*súkromného kľúča*.

kultúra riadenia rizika [risk management culture] neznámy pojem, pravdepodobne →*kultúra rizika* postavená na systematickej správe rizík. Pozri →*ISO/IEC 27005*.

kultúra rizika [risk culture] formálne definované normy upravujúce spôsoby ako zohľadňovať riziká pri činnosti organizácie a postoje zamestnancov k dodržiavaniu týchto noriem a ich uplatňovanie v ich vlastnej činnosti.

kybernetická bezpečnosť [cybersecurity] pozri *bezpečnosť, kybernetická*.

kybernetická obrana [cyberdefense] systém koordinovaných činností zameraných na identifikáciu potenciálnych útočníkov, odradenie potenciálneho útočníka od útoku na systém, sieť alebo kybernetické priestor, zastavenie prebiehajúceho útoku, minimalizáciu jeho dopadov, analýzu priebehu útoku a prijatie opatrení na zamedzenie podobných útokov v budúcnosti. Súčasťou kybernetickej obrany sú aj činnosti zamerané na zníženie útočného potenciálu potenciálnych útočníkov.

kybernetické ohrozenie [cyber threat] 1. hrozba/y voči prvkom, subsystémom, podpriestoru alebo celému kybernetického priestoru 2. hrozba útoku kybernetickými (hardvérovými, softvérovými) prostriedkami

kybernetický bezpečnostný incident [cybersecurity incident] bezpečnostný incident, ktorý má negatívny dopad na kybernetický priestor, jeho časť, alebo prvok.

kybernetický bezpečnostný incident, závažný [serious cybersecurity incident] kybernetický bezpečnostný incident s veľkým spoločenským dopadom. Pozri →*kritériá pre kasifikáciu kybernetických bezpečnostných incidentov*.

kybernetický priestor [cyberspace] pôvodne metaforické označenie prostredia v ktorom prebieha prenos a spracovanie digitálne zaznamenanej informácie. V súčasnosti označuje →*informačnú a komunikačnú infraštruktúru* organizácie, štátu alebo globálnu informačnú a komunikačnú infraštruktúru.

kybernetický terorizmus [cyberterrorism] teroristické aktivity vyvíjané v kybernetickom priestore alebo vykonávané prostredníctvom (digitálnych) informačných a komunikačných technológií. Ide najmä o zastrašovanie, vyhrážanie sa štátnym inštitúciám,

organizáciám, osobám s cieľom presadiť politické alebo sociálne ciele prostredníctvom kybernetických útokov na systémy, siete alebo informácie, ktoré sa obsahujú.

kybernetický zločin [cybercrime] – protiprávna činnosť, ktorá (a) je zameraná na informačné a komunikačné systémy, alebo (b) ich využíva na nekalé ciele.

L

lokalizácia bezpečnostného incidentu [security incident localization] zamedzenie šírenia bezpečnostného incidentu.

M

manažment certifikátov [certificate management] vydávanie, distribúcia, uchovávanie, overovanie platnosti, používanie a rušenie →*certifikátov*.

manažment informačno-bezpečnostných incidentov [information security incident management] procesy odhaľovania, nahlasovania, vyhodnocovania →*informačno-bezpečnostných incidentov*, reakcií na ne, ich riešenia a poučenia sa z nich.

manažment kľúčov [key management] →*generovanie*, distribúcia, používanie, uchovávanie, aktualizácia a ničenie →*kryptografických kľúčov*.

manažment kontinuity činnosti [business continuity management] systematická činnosť zameraná na zabezpečenie dostupnosti kľúčových zdrojov organizácie a služieb/činností, pomocou alebo prostredníctvom ktorých organizácia napĺňa svoje poslanie. Organizácia identifikuje svoje kritické aktíva, scenáre naplnenia hrozieb, prijme opatrenia na minimalizáciu rizík, vytvorí kapacity na riešenie bezpečnostných incidentov, vypracuje a nacvičí postup v prípade krízovej situácie, zabezpečí náhradné zdroje na fungovanie v provizórnych podmienkach, plány obnovy, zdroje a postupy na ich realizáciu.

modulátor [modulator] systém/technické zariadenie upravujúce signál takým spôsobom, aby upravený niesol požadovanú informáciu.

monitorovanie [monitoring] sledovanie systému, komunikácie, činnosti používateľov alebo vybraných parametrov systému alebo siete a pod. v dlhšom časovom úseku za účelom odhaľovania odchýlok od štandardných hodnôt, ktoré by mohli byť príznakom bezpečnostného incidentu.

N

národné kontaktné miesto pozri →*kontaktný bod, národný*.

narušenie bezpečnosti [security violation] akt alebo udalosť, ktorá nie je v súlade s →*bezpečnostnou politikou* systému alebo organizácie.

nepopretie [repudiation] schopnosť dokázať, že nastala nejaká udalosť, alebo bola vykonaná nejaká činnosť a čo /kto bol/o jej pôvodcom/vykonávateľom.

nepopretie pôvodu [non repudiation of origin] →*bezpečnostná požiadavka* na dokument, ktorej naplnenie znamená, že tvorca (odosielateľ) dokumentu nebude môcť poprieť, že dokument vytvoril (poslal).

nepopretie prijatia [non repudiation of receipt] →*bezpečnostná požiadavka* na dokument/správu, (resp. na systém doručovania dokumentov) ktorej naplnenie znamená, že adresát nemôže poprieť, že dokument prijal.

nesúlad [non-conformity] nesplnenie požiadavky.

O

obmedzenie následkov kybernetického bezpečnostného incidentu [cybersecurity incident impact reduction] opatrenia vedúce k minimalizácii dopadov na aktíva organizácie; medzi ne patria preventívne opatrenia pokrývajúce zraniteľnosti aktív organizácie a znižujúce pravdepodobnosť naplnenia hrozieb, včasná detekcia bezpečnostného incidentu, rýchla lokalizácia (zamedzenie

ďalšieho šírenia bezpečnostného incidentu), rýchle spustenie náhradnej prevádzky a následne obnova systému (a ošetrenia zraniteľnosti, ktorú hrozba využila); v prípade ohrozenia ľudí (požiar, havária) ochrana zdravia a života ľudí.

obnova činnosti [business recovery] kroky, ktoré organizácia musí podniknúť na to, aby po →*bezpečnostnom incidente*, havárii alebo katastrofe čo najrýchlejšie obnovila →*informačnú a komunikačnú infraštruktúru* podporujúcu jej kritické činnosti (disaster recovery).

odhaľovanie kybernetického bezpečnostného incidentu [cybersecurity incident detection] získavanie a vyhodnocovanie informácií o stave a činnosti systému; zohľadnenie výstrah, varovaní a ďalších informácií z externých zdrojov na nájdenie príznakov začínajúceho/prebiehajúceho útoku, zlyhávania systému alebo iného typu kybernetického bezpečnostného incidentu.

odolnosť [resilience] schopnosť systému odolávať pokusom o naplnenie →*hrozieb*; minimalizovať dopady naplnených hrozieb a obnoviť pôvodnú funkcionalitu po →*incidente*.

odolnosť, kybernetická [cyber resilience] →*odolnosť* systému voči →*kybernetickým hrozbám*.

odopretie služby [denial of service, DoS] výsledok akcie, alebo niekoľkých akcií, ktorý znemožňuje systému a/alebo aplikácii (najčastejšie z dôvodu preťaženia) správne fungovať a poskytovať požadované služby

odpočúvanie [eavesdropping] monitorovanie komunikácie prebehajúcej po →*prenosovom kanáli* s cieľom získať kópiu prenášaných údajov.

ohraničenie incidentu pozri →*lokalizácia bezpečnostného incidentu*.

ochrana kybernetického priestoru [cyberspace protection] opatrenia a činnosti zamerané na dosiahnutie a udržanie dostatočnej úrovne odolnosti →*aktív* (časti →*kybernetického priestoru*, ktorý je predmetom ochrany; t.j. na zníženie hodnoty→*rizík* vyplývajúcich z →*hrozieb* voči týmto aktívam, efektívnu reakciu a minimalizáciu dopadu v prípade →*bezpečnostného incidentu*, rýchle obnovenie postihnutých aktív a kvalifikovanú analýzu pôvodu a priebehu bezpečnostného incidentu.

ochrana prístupu, fyzická [physical access control] opatrenia fyzickej povahy (ploty, steny, dvere, mreže, strážna služba, kamerový systém, umiestnenie systémov a komponentov siete v chránených priestoroch, trezory, zamykateľné skrine a pod.), zamedzujúce alebo sťažujúce prístup nepovolaných osôb k aktívam organizácie.

ochrana prístupu, logická [logical acces control] riadenie prístupu k systémom a zdrojom organizácie na základe identifikácie, autentifikácie, autorizácie a auditu.

opatrenie [measure] pozri →*bezpečnostné opatrenie*.

opatrenie, kryptografické [cryptographic control] opatrenie využívajúce kryptografické prostriedky, napríklad šifrovanie na ochranu dôvernosti informácie, digitálne odtlačky na ochrany integrity, digitálne podpisy na ochranu autentickosti, časové pečiatky na dokumentovanie času, kedy k udalosti došlo a pod.

opatrenie, ochranné [protective control] bezpečnostné opatrenie preventívneho charakteru, ktorého cieľom je zamedziť naplneniu hrozby voči aktívu, alebo aspoň znížiť hodnotu rizika, naplnenia hrozby.

opatrenie, reaktívne [reactive control] bezpečnostné opatrenie, ktorého cieľom je zamedziť rozširovaniu pôsobenia hrozby na ďalšie aktíva (lokalizácia bezpečnostného incidentu), zastaviť pôsobenie hrozby na aktíva, odstrániť následky pôsobenia hrozby na aktíva (obnova).

operačný systém [operating system] programové vybavenie počítača, ktoré spravuje zdroje (pamäť, procesor, periférne

zariadenia, softvér) počítača a poskytuje služby iným programom počítača.

orgán posudzovania zhody [audit providing body] inštitúcia, ktorá má oprávnenie na vykonávanie auditu. Oprávnenie sa zakladá najmä na odbornej spôsobilosti a kapacitách dostatočných na vykonanie auditu na požadovanej úrovni. Požiadavky na organizáciu vykonávajúcu bezpečnostný audit (a certifikáciu) informačných systémov stanovuje norma ISO/IEC 27006.

osoba, neoprávnená [unauthorized person] osoba, ktorá nemá oprávnenie na využívanie niektorých zdrojov, výkon činností, prístup k informáciám systému/organizácie.

osoba, oprávnená [unauthorized person] osoba, ktorej boli pridelené prístupové práva do systému, oprávnenia na vykonávanie vybraných činností, využívanie zdrojov systému/organizácie. Činnosť v systéme sa zaznamenáva (záznam auditu, audit log) a vyhodnocuje. Aktivity presahujúce oprávnenia danej osoby sú bezpečnostne relevantnou udalosťou, alebo už bezpečnostným incidentom.

osobné informácie [personal information] informácie vzťahujúce sa na fyzickú osobu, ktorých kompromitácia by mohla danú fyzickú osobu nejako poškodiť.

osobné údaje [personal data] 1. údaje obsahujúce osobné informácie; 2. údaje týkajúce sa fyzických, fyziologických, psychických, mentálnych, ekonomických, kultúrnych a podobných atribútov určenej alebo určiteľnej osoby.

ošetrenie rizika [risk treatment] pozri →*riziko, ošetrenie*.

P

personálna bezpečnosť [personnel security] opatrenia na zaistenie toho, aby sa minimalizovala pravdepodobnosť úmyselných útokov na systém a neúmyselných chýb interných pracovníkov pri práci so systémom. Opatrenia zahŕňajú výber, preverovanie, prípravu, monitorovanie personálu, procedúry pri zmene pracovného zaradenia a ukončení zamestnania v organizácii.

plán kontinuity činnosti [business continuity plan, BCP] výstup →*plánovania kontinuity činnosti*. Plán na zabezpečenie súvislej činnosti organizácie zahŕňajúci aj neinformatické aspekty, ako je zaistenie kľúčových ľudí, obnovu informačných zdrojov, zariadení, krízovú komunikáciu, ochranu dobrého mena. Plán kontinuity činnosti obsahuje aj preventívne, detekčné a korekčné opatrenia.

plán obnovy [disaster recovery plan, DRP] postupnosť krokov na čo najrýchlejšie odstránenie následkov havárie/katastrofy a obnovu kritickej →*informačnej infraštruktúry organizácie*.

plánovanie, havarijné [disaster recovery planning] plánovanie činnosti pre prípad havárií (preventívne opatrenia, detekcia havárií, opatrenia na zmiernenie následkov havárie, opatrenia na odstránenie následkov havárie →*plán obnovy*).

plánovanie kontinuity činnosti [business continuity planning] vytváranie, implementácia, testovanie a revízie plánov kontinuity činnosti.

počítačová kriminalita [computer crime] trestná činnosť zameraná proti počítačom, alebo využívajúca počítače. Ako synonymum sa používa pojem kybernetický zločin (cybercrime).

pokrytie rizika [risk treatment] ošetrenie rizika takým spôsobom, že jeho (zostatková) hodnota nepresahuje akceptovateľnú úroveň.

potvrdenie platnosti [validation] 1. potvrdenie správnosti alebo korektnosti príslušnej konštrukcie; 2. oficiálne potvrdenie zhody posudzovanej veci s príslušným štandardom.

používateľ systému [system user] osoba s minimálnymi privilégiami, ktoré má prístup k systému, vybraným zdrojom s ktorými môže vykonávať obmedzenú množinu operácií. Používateľ napríklad nemôže meniť

konfiguráciu systému, inštalovať na ňom vlastný softvér, nemusí mať prístup k niektorým súborom, resp. môže ich len čítať, ale nemôže ich meniť a pod.

povinné riadenie prístupu [mandatory access control] typ riadenia prístupu, v ktorom operačný systém obmedzuje schopnosť subjektu, alebo procesu vykonávať nejaké činnosti, alebo pristupovať k zdrojom systému.

preventívna činnosť [preventive action] činnosť zameraná na eliminovanie potenciálneho →*nesúladu* alebo inej potenciálnej nežiadúcej situácie.

prienik [penetration] úspešný, opakovateľný neoprávnený prístup k chránenému zdroju v systéme.

priestor, digitálny [digital space] globálnym digitálnym priestorom je súhrn (a) všetkých →*informačných a komunikačných technológií*, ich programového vybavenia a dokumentácie opisujúcej ich štruktúru, konfiguráciu a činnosť, (b) →*informácií*, ktoré sa prostredníctvom nich prenášajú, spracovávajú alebo uchovávajú, (c) procesov, ktoré v nich prebiehajú, (d) podpornej infraštruktúry zabezpečujúcej ich činnosť, (e) ľudí zabezpečujúcich ich činnosť, (f) vzťahov medzi entitami digitálneho priestoru a pravidiel upravujúcich tieto vzťahy.

priestor, kybernetický [cyberspace] globálny dynamický otvorený[35] systém, ktorý tvoria telekomunikačné a počítačové siete, informačné a komunikačné systémy, ich programové vybavenie a údaje, ktoré sa pomocou nich spracovávajú; elektronické subsystémy riadiacich, výrobných, bezpečnostných a iných systémov a zariadení; činnosti, ktoré v jednotlivých častiach tohto systému prebiehajú; vzťahy a interakcie medzi časťami, prvkami a subsystémami tohto systému.

princíp najmenšieho privilégia [least privilege principle] podstata princípu spočíva v tom, že každá →*entita* (človek, program, proces) v systéme má prístup len k tým zdrojom, ktoré potrebuje na plnenie svojho poslania.

princíp potreby poznať [need-to-know principle] iná verzia princípu najmenšieho privilégia: človek má prístup len k tým informáciám, ktoré potrebuje poznať na plnenie svojich pracovných povinností.

prístup [access] 1. možnosť a schopnosť →*entity* využívať zdroje systému; 2. interakcia →*entity* a systému.

prístupové práva [access rights] oprávnenia na →*prístup* k zdrojom systému a na vykonávanie vybraných operácií s nimi (napr. čítanie a zápis údajov, spúšťanie programov).

procedúra [procedure] špecifický spôsob, ako vykonať nejakú činnosť alebo proces.

proces [process] postupnosť navzájom súvisiacich činností, ktorá transformuje vstupy na výstupy.

programové vybavenie [software] súhrnné označenie programov inštalovaných na počítači. Súbor programov počítača obvykle tvoria systémové programy (operačný systém) slúžiace na zabezpečenie činnosti počítača, správu zdrojov, komunikáciu s periférnymi zariadeniami a aplikačné programy slúžiace na riešenie špecifických úloh používateľa.

prvok kritickej infraštruktúry [element of critical infrastructure] logicky, organizačne alebo fyzicky ucelená časť kritickej infraštruktúry (= systém), ktorého výpadok alebo narušenie obmedzí alebo znemožní plnenie niektorých funkcií štátu.

prvok kybernetického priestoru [cyberspace component] prvkami →*kybernetického priestoru* sú logicky, organizačne alebo fyzicky

[35] Globálny kybernetický priestor je otvorený, jeho časť môže byť izolovaná a uzavretá.

ucelené časti kybernetického priestoru, o ktorých štruktúre nie je potrebné na danej úrovni rozlíšenia (alebo popisu kybernetického priestoru) uvažovať.

prvok systému [system element] v závislosti od charakteru systému logicky, organizačne alebo fyzicky ucelená časť systému, o ktorého štruktúre nie je potrebné na danej úrovni rozlíšenia (alebo popisu systému) uvažovať.

pseudonymita [pseudonymity] bezpečnostná služba umožňujúca uchovať v tajnosti →*identitu* →*entity* pred neoprávnenými osobami tým, že sa namiesto mena používa pseudonym. Oprávnená osoba pozná meno osoby nahradené pseudonymom.

R

riadenie kontinuity pozri →*manažment kontinuity činnosti*.

riadenie prístupu [access control] opatrenia na zaistenie toho, aby →*prístup* ku zdrojom (→*aktívam*) mali len oprávnené →*entity* a len v súlade s ich →*prístupovými právami*.

riadenie rizík pozri →*správa rizík*.

riziko [risk] veličina závisiaca od závažnosti (možného dopadu) →*hrozby* a pravdepodobnosti, že sa hrozba naplní.

riziko, analýza [risk analysis] pozri →*analýza rizík*.

riziko, akceptovateľné [acceptable risk] úroveň →*zvyškového rizika*, ktorú je organizácia schopná/ochotná tolerovať.

riziko, eliminácia [risk elimination] prijatie riešení, ktoré znížia pravdepodobnosť naplnenia hrozby alebo jej dopad na aktíva organizácie na nulu. Môže ísť o prijatie opatrenia, ktoré odstráni zraniteľnosť prostredníctvom ktorej sa hrozba uplatnila, alebo môže ísť o vyhnutie sa riziku prijatím iného riešenia, pri ktorom sa daná hrozba nemôže uplatniť, alebo prenesenie rizika na tretiu stranu (poistenie, outsourcing).

riziko, identifikácia [risk identification] proces vyhľadávania, rozpoznávania a popísania →*rizík*.

riziko, kritériá [risk criteria] referenčné hodnoty, oproti ktorým sa vyhodnocuje významnosť →*rizika*.

riziko, ošetrenie [risk treatment] riešenie konkrétneho ohodnoteného rizika, ktorého hodnota bola posúdená vzhľadom na kritériá vyhodnotenia rizík. Riziko možno ošetriť 1. zavedením alebo úpravou opatrení, ktoré znížia pravdepodobnosť naplnenia príslušnej hrozby, alebo jej dopad na aktívum; 2. akceptovať riziko (ak je jeho hodnota nižšia ako hranica prijateľného rizika); 3. vyhnutím sa riziku (prijatím riešenia, pri ktorom sa daná hrozba nemôže uplatniť); 4. zdieľaním rizika (poistenie, externý monitoring).

riziko, stanovenie [risk assesment] celkový proces →*identifikácie rizika*, →*analýzy rizík* a →*vyhodnotenia rizika*.

riziko, vyhodnotenie [risk evaluation] proces porovnávania výsledkov →*analýzy rizík* s →*kritériami rizika*, ktorého cieľom je rozhodnutie, či je riziko a/alebo jeho hodnota akceptovateľná alebo tolerovateľná.

riziko, zvyškové [residual risk] →*riziko*, ktoré ostalo po prijatí →*opatrení*.

robotická sieť [botnet] množina počítačov infiltrovaných →*zlomyseľným softvérom*, umožňujúcim ich ovládanie zo vzdialeného riadiaceho centra. Takéto siete sa využívajú na šírenie →*spamu* a na →*útoky* na vybrané ciele na Internete.

robustnosť [resilience] schopnosť systému odolávať negatívnym vplyvom a cieleným pokusom o narušenie.

rola [role] trieda používateľov s ekvivalentnými oprávneniami na prístup k systémom, resp. úlohami v informačnej bezpečnosti. Príkladmi rôl sú používateľ, správca systému, operátor, audítor, bezpečnostný manažér a i.

rootkit [rootkit] súbor nástrojov, pomocou ktorých môže útočník získať oprávnenia na úrovni správcu systému.

rozsah auditu [audit scope] špecifikácia toho, čo sa pri audite bude posudzovať a voči čomu

S

sieť [network] 1. systém zložený z uzlov poprepájaných linkami; 2. počítačová sieť – sieť, ktorej uzlami sú počítače, prepínače, smerovače a ďalšie zariadenia slúžiace na riadenie prenosu informácie a linkami komunikačné kanály; 3. → *sieť, elektronická komunikačná*.

sieť, elektronická komunikačná [electronic communication network] systém zložený z komunikačných liniek a zariadení na prepájanie alebo smerovanie signálov, umožňujúci prenos informácie pomocou elektromagnetických signálov.

sieťová bezpečnosť [network security] ochrana sietí a sieťových služieb pred neoprávnenou modifikáciou, zničením alebo únikom údajov, zneprístupnením služieb, a tiež zaistenie záruk, že sieť správne funguje a nevznikajú žiadne škodlivé vedľajšie efekty.

signál [signal] fyzikálna veličina nadobúdajúca aspoň dve rôzne hodnoty, ktorá sa dá použiť na prenos informácie.

silná autentifikácia [strong autentication] →*autentifikácia* založená na dvoch alebo viacerých nezávislých metódach na →*overenie* →*identity* →*entity*.

skrytý kanál pozri →*kanál, skrytý*.

služba [service] služba je činnosť, ktorú jedna →*entita* (poskytovateľ služby) vykonáva za vopred dohodnutých/stanovených podmienok na požiadanie/podnet druhej entity (klient). Službou je aj jednorazové poskytnutie alebo opakované poskytnutie zdrojov jednej entity poskytovateľa služby klientovi na požiadanie klienta.

služba, digitálna [digital service] tri špecifické →*služby informačnej spoločnosti*, uvedené v →*smernici NIS;* online trhovisko, internetivý vyhľadávač a služba cloud-computingu

služba informačnej spoločnosti [Information Society service] →*služba*, ktorá sa bežne poskytuje za odplatu, na diaľku, elektronickým spôsobom a na základe individuálnej žiadosti príjemcu služieb

služba, základná [essential service] →*služba*, ktorá spĺňa nasledujúce tri podmienky: 1) je podstatná pre udržanie kritických spoločenských a/alebo ekonomických aktivít, 2) jej poskytovanie závisí od sietí a informačných systémov, 3) bezpečnostný incident zasahujúci sieť alebo systém, ktoré sa využívajú pri poskytovaní tejto služby, by mal významný negatívny dopad na poskytovanie služby**.**

smernica NIS [Directive NIS] Smernica Európskeho parlamentu a rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

sniffer [sniffer] program umožňujúci monitorovanie komunikácie prebiehajúcej prostredníctvom siete.

sociálne inžinierstvo [social engineering] netechnické metódy →*prieniku* do systémov založené na interakcii s inými ľuďmi, ktorých sa útočník snaží nejakým spôsobom oklamať a primäť k tomu, aby porušili normálne používané bezpečnostné postupy.

softvér [software] počítačový program alebo súbor počítačových programov.

softvérové pirátstvo [software piracy] neoprávnené kopírovanie, distribúcia a používanie počítačových programov, ktoré spadajú pod zákon na ochranu autorských práv.

spam [spam] nevyžiadaná elektronická pošta/komunikácia.

spoľahlivosť [reliability] schopnosť/vlastnosť entity správať sa konzistentne zamýšľaným spôsobom a dosahovať požadované výsledky.

spoof [spoof] pokus neoprávnenej osoby získať →*prístup* do systému vydávaním sa za inú (oprávnenú) osobu.

spracovanie informácie [information

processing] zber, prenos, uchovávanie (vlastné spracovávanie: triedenie, spájanie výber), používanie, archivácia a ničenie informácie.

správa aktív [asset management] systematický proces efektívnej starostlivosti o aktíva zahŕňajúci celý životný cyklus aktív (hmotných aj nehmotných) – vývoj/vznik/nadobúdanie, prevádzka, udržiavanie, upgrade, vyraďovanie.

správa rizík [risk management] identifikácia rizík, odhad rizík, vyhodnotenie rizík, prijatie opatrení a monitorovanie zostatkových rizík, prehodnocovanie rizík.

stanovenie rizika [risk assesment] pozri →*riziko, stanovenie*.

stav systému [system state] 1. teor. súbor všetkých informácií, ktoré charakterizujú systém v danom okamihu jeho existencie; 2. výsledok vyhodnotenia systému podľa nejakého kritéria (funkčnosť, bezpečnosť, výkon a i.)

subsystém [subsystem] systém, ktorý je časťou väčšieho systému.

súkromnosť [privacy] →*bezpečnostná požiadavka* na →*údaje*, ktorej naplnenie znamená, že osoba, ktorej sa údaje týkajú, má možnosť rozhodnúť, komu, aké a za akých podmienok sa údaje, ktoré sa jej týkajú, poskytnú, a skontrolovať, či sa jej rozhodnutia dodržujú.

súlad [conformity] splnenie príslušnej požiadavky.

systém [system] 1. všeobecný pojem označujúci entitu (reálnu alebo abstraktnú), ktorú možno popísať vymedzením jej prvkov, vzťahov medzi nimi, stavov, pravidiel pre zmenu stavov, okolia systému; 2.informačný a komunikačný systém slúžiaci na spracovanie informácie.

systém, dynamický [dynamic system] systém, ktorého stav sa mení, napríklad na základe podnetov okolia.

systém, globálny [global system] systém s celosvetovou pôsobnosťou.

systém, otvorený [open system] systém, ktorý komunikuje so svojím okolím. Opakom je uzavretý systém.

systém riadenia informačnej bezpečnosti [information security management system] systematický prístup k riešeniu →*informačnej bezpečnosti* v organizácii založený na súbore formálne zdokumentovaných a vzájomne koordinovaných bezpečnostných politík stanovujúcich ciele a úroveň informačnej bezpečnosti v organizácii, zodpovednosť za IB, organizačné zabezpečenie, upravujúcich požiadavky na personálnu bezpečnosť, vzťahy s externými partnermi, fyzickú bezpečnosť, prevádzkovú a komunikačnú bezpečnosť, ochranu prístupu a súlad s legislatívou.

Š

šifra [cipher] synonymum pojmu →*kryptosystém*.

šifra, asymetrická [asymmetric cipher] 1. →*šifra*, v ktorej sa na →*šifrovanie* používa iný →*kľúč* ako na →*dešifrovanie*, 2.→*kryptosystém s verejným kľúčom*.

šifra, symetrická [symmetric cipher] šifra, v ktorej sa na →*šifrovanie* a →*dešifrovanie* používa ten istý →*tajný kľúč*.

šifrovacia transformácia [encryption/enciphering transformation] pozri →*transformácia šifrovacia*.

šifrovanie [encryption, enciphering] transformácia →*otvoreného textu* na →*šifrový* pomocou →*šifrovacej transformácie* a →*šifrovacieho kľúča*.

šifrovanie od odosielateľa po príjemcu [end-to-end encryption] ochrana →*dôvernosti* prenášaných správ založená na tom, že odosielateľ správu →*zašifruje*, pošle ju v šifrovanej podobe príjemcovi, ktorý ju →*dešifruje*.

šifrový text [ciphertext] pozri →*text, šifrový*.

štandard informačnej bezpečnosti [information security standard] 1. medzinárodné normy, pozri sériu noriem

ISO/IEC 27000; 2. národné štandardy; 3. bezpečnostné štandardy výnosu Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov.

štandard kybernetickej bezpečnosti [cybersecurity standard] 1. norma ISO/IEC 27023; 2. štandardy, ktoré by na základe ZoKB mal vydať NBÚ.

štandard, znalostný [body of knowledge] 1. ucelený súbor znalostí a zručností potrebných na to, aby človek bol schopný plniť úlohy vyplývajúce zo zaradenia nejakej roly; 2. štandard, ktorý by na základe ZoKB mal vydať NBÚ.

T

text, otvorený [cleartext] text, ktorý nebol modifikovaný žiadnou →*kryptografickou transformáciou*.

text, šifrový [ciphertext] výsledok zašifrovania otvoreného textu pomocou →*šifrovacej transformácie* E (a šifrovacieho kľúča).

transformácia dešifrovacia [deciphering transformation] injektívne zobrazenie D, ktoré →*šifrovému textu* priradí →*otvorený text* m. Dešifrovacia transformácia máva okrem šifrového textu aj druhý parameter, k, dešifrovací kľúč. K dešifrovacej transformácii prislúcha opačná →*šifrovacia transformácia* E. Obe transformácie sú spojené vzťahom $\forall m \forall k\ D(E(m,k),k) = m$.

transformácia šifrovacia [enciphering transformation] spravidla injektívne zobrazenie E (encryption, enciphering), ktoré správe m (→*otvorenému textu*) priradí →*šifrový text* c. Šifrovacia transformácia má spravidla dva argumenty – →*šifrovací kľúč* k a správu m: $E(m,k) = c$. K šifrovacej transformácii prislúcha opačná, →*dešifrovacia transformácia D*. Obe transformácie sú spojené vzťahom $\forall m \forall k\ D(E(m,k),k) = m$.

U

účinnosť [effectivness] rozsah, v ktorom boli vykonané plánované činnosti a dosiahnuté plánované výsledky.

údaje [data] forma záznamu →*informácie* v →*informačných a komunikačných systémoch*.

udalosť [event] výskyt alebo zmena špecifickej množiny okolností.

udalosť relevantná pre informačnú bezpečnosť [information security event] identifikovaný výskyt stavu systému, služby alebo siete, ktorý indikuje možné porušenie bezpečnostnej politiky, alebo zlyhanie bezpečnostného opatrenia; alebo dovtedy neznáma situácia, ktorá môže mať význam z hľadiska informačnej bezpečnosti.

únik údajov [data leakage] náhodný tok citlivých údajov k neoprávnenej →*entite*.

úroveň rizika [level of risk] hodnota →*rizika*; v kvantitatívnom vyjadrení stredná hodnota →*dopadu* príslušnej →*hrozby* na dané →*aktívum;* pri kvalitatívnom vyjadrení hodnota zohľadňujúca dopad hrozby na aktívum a pravdepodobnosť jej naplnenia.

útočník [attacker] osoba, ktorá vykonáva →*útok* na →*systém*, alebo nejaké →*aktívum* systému/organizácie.

útočný potenciál [attack potential] znalosti, motivácia a príležitosť →*útočníka* uskutočniť úspešný →*útok*.

útok [attack] cieľavedomý pokus o využitie →*zraniteľnosti* systému/aktíva za účelom získania neoprávnených →*privilégií*, alebo poškodenia/zničenia daného aktíva, alebo niektorého z iných aktív systému/organizácie.

útok, kybernetický [cyber attack] →*útok* voči →*aktívam* →*kybernetického priestoru* alebo útok prostredníctvom kybernetických prostriedkov.

útok hrubou silou [brute force attack] kryptoanalytický útok založený na preberaní všetkých možností (napríklad možných dešifrovacích kľúčov, →*otvorených textov*).

útok úplným prehľadávaním [exhaustive attack] →*útok hrubou silou*.

útok typu denial of service [denial of service (DoS) attack] útok na systém/aplikáciu s cieľom dosiahnuť →*odmietnutie služby*

V

varovanie [warning] upozornenie na hrozbu, ktorá sa môže naplniť (potenciálna udalosť), na rozdiel od výstrahy, ktorá upozorňuje na bezpečnostný incident, t.j. udalosť, ku ktorej už došlo.

varovanie, včasné [early warning] varovanie, ktoré prichádza hneď po objavení sa hrozby, aby ohrozené subjekty mali čas prijať proti nej potrebné opatrenia.

vniknutie/prienik [intrusion] →*hrozba*, pri naplnení ktorej neoprávnená osoba získava prístup k →*citlivým údajom* tým, že obíde (úmyselne alebo neúmyselne) →*bezpečnostné opatrenia* systému.

voliteľné riadenie prístupu [discretionary access control] →*riadenie prístupu* založené na tom, že (a) oprávnenia na činnosť v systéme sú viazané na →*entity*, ktoré musia preukázať svoju →*identitu*, (b) entity sú vlastníkmi systémových zdrojov (napr. údajov), a môžu iným entitám prideliť alebo odňať →*prístupové práva* k týmto zdrojom.

vyhodnotenie rizík [risk assesment] analytická činnosť zameraná na systém alebo organizáciu, ktorej výsledkom je identifikácia →*aktív* systému (organizácie); relevantných →*hrozieb* voči aktívam organizácie; →*bezpečnostných požiadaviek* na organizáciu; →*zraniteľností* aktív; výpočet všetkých rizík vyplývajúcich z relevantných hrozieb voči aktívam organizácie.

výstraha [alarm/alert] informácia o bezpečnostnom incidente, ktorý už nastal a môže zasiahnuť aj systémy organizácie, ktorej bola výstraha určená.

využitie [exploit] explicitne definovaný spôsob, ako narušiť bezpečnosť systému využitím jeho →zraniteľnosti.

Z

zadné vrátka [trap door] skrytý softvérový alebo hardvérový mechanizmus, ktorý po aktivácii umožní obchádzať bezpečnostné mechanizmy systému.

zapisovač klávesnice [key logger] zlomyseľný program nepozorovane zaznamenávajúci stláčanie kláves na klávesnici, ktorý následne poskytuje túto informáciu inému subjektu, než je prihlásený používateľ.

základné bezpečnostné štandardy [security baselines] štandardy špecifikujúce minimálny (základný) súbor →*bezpečnostných opatrení,* ktoré sú za normálnych okolností vhodné pre väčšinu organizácií s podobným technickým a programovým vybavením a porovnateľnými bezpečnostnými potrebami.

záznam auditu [audit log] časovo usporiadaný zoznam zápisov o bezpečnostne relevantných udalostiach v systéme. Zápis o bezpečnostne relevantnej udalosti obsahuje minimálne čas, popis udalosti a →*identifikátor* entity, ktorá udalosť spôsobila.

zlomyseľný softvér [malicious software, malware] →*červy,* →*vírusy,* →*trójske kone* a iné programy vytvorené s cieľom získať pre svojho používateľa neoprávnené privilégiá na cudzom počítači, alebo jeho majiteľa poškodiť.

zneužitie identity [identity fraud] nezákonná zmena →*identity*.

zraniteľnosť [vulnerability] vlastnosť, spôsob použitia alebo okolnosť umožňujúce naplnenie nejakej špecifickej →*hrozby.* Napr. pripojenie nechráneného počítača k Internetu umožňuje hackerský útok, neaktuálna databáza vírusov je zraniteľnosťou umožňujúcou napadnutie počítača zlomyseľným softvér.