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 kybernetická a informačná bezpečnosť je, rýchle sa rozvíjajúca multidisciplinárna oblasť ľudskej činnosti. Podobne ako v iných krajinách, tak aj na Slovensku je nedostatok odborníkov, ktorí by požiadavky zákonov na zaistenie kybernetickej a informačnej bezpečnosti v dotknutých organizáciách vedeli riešiť.

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*. Pre účely tohto dokumentu definujeme údaje ako *formu 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. 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,

c) informácia sa spracováva automatizovane, na základe programov.

Najvýstižnejšie 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, resp. spoločnosť sa dostala do závislosti od svojich digitálnych IKT. Digitálne IKT tvoria globálny systém (označuje sa aj pojmom digitálny ekosystém) 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.

Z praktického hľadiska je rozlišovanie kybernetickej a informačnej bezpečnosti nepodstatné. Organizácia 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[1] . 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 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.
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.

[1] 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.

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.

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[2], 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[3] 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.

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

[3] 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[4] 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

[4] 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.