Úvod kybernetickej a informačnej bezpečnosti

UIB-2

Daniel Olejár

Univerzita Komenského

Február 2023

Agenda

- význam informačných technológií pre spoločnosť
- digitálne IKT
- čo je informačná bezpečnosť?
- základné pojmy
- kybernetická bezpečnosť

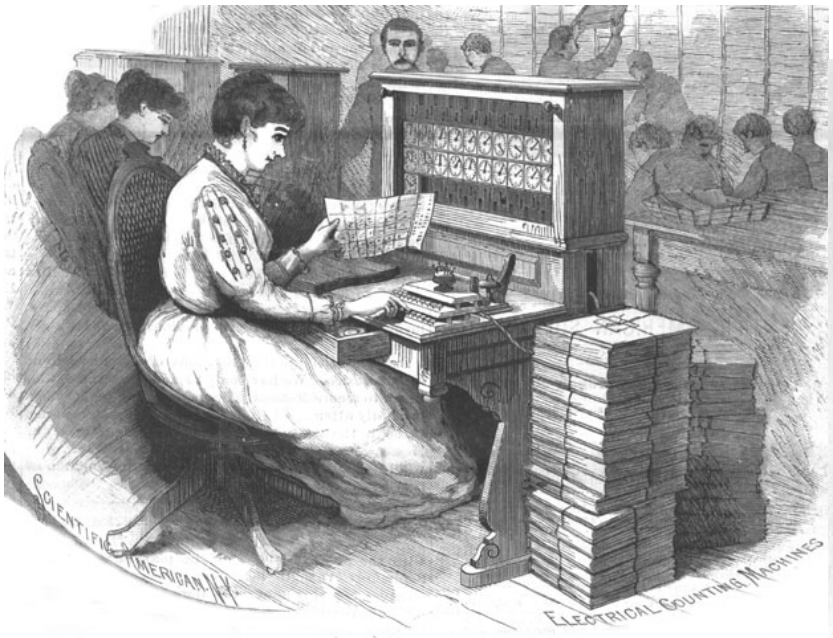
Zdroje

- https://en.wikipedia.org/wiki/1890_United_States_census#/media/File:1890_Census_Hollerith_Electrical_Counting_Machines_Sci_Amer.jpg
- http://ed-thelen.org/comp-hist/hollerith-pantagraph-punch.jpg
- https://upload.wikimedia.org/wikipedia/commons/2/2c/Fingerprintforcriminologystubs2.png

Informačné a komunikačné technológie, IKT

- na začiatok trocha širší kontext
- Komunikácia a učenie – základný predpoklad existencie a rozvoja ľudskej spoločnosti
- Informačné a komunikačné technológie – nie sú vynálezom 20. storočia
- Ale 20. storočie, resp. koniec 19 storočia- nový problém: spoločnosť potrebovala na svoju existenciu viac informácií, ako stihla spracovať manuálne
- USA, census v roku 1890 – diernoštítkové stroje
- Telegraf, rozhlas, televízia
- 2. svetová vojna, počítače (riadenie protilietadlovej paľby, kryptoanalýza, vylodenie v Normandii)
- Koniec 20. storočia – syntéza: masovokomunikačné prostriedky + telekomunikačné siete + počítače = digitálne IKT

US 1890 census a Hollerithov stroj



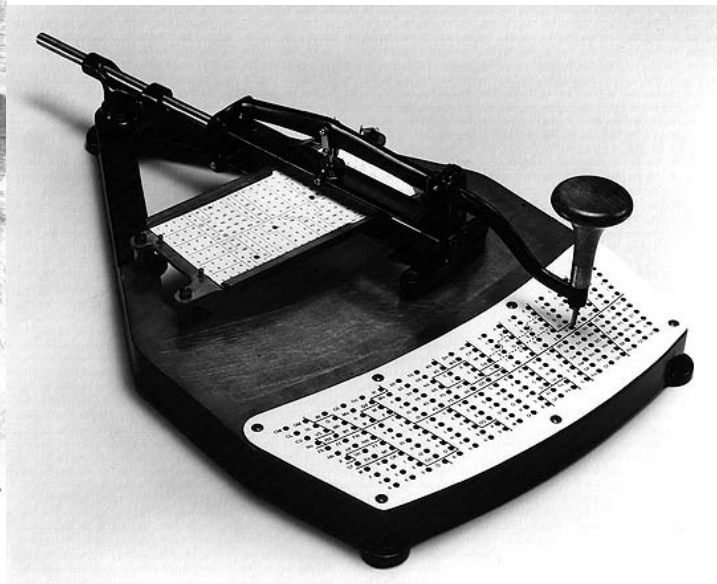


Figure: Hollerithov tabulátor

- Oproti klasickým IKT:
  - Digitálne kódovanie informácie
  - Tie isté prenosové kanály
  - Automatizované spracovanie informácie
- Internet, web (DARPA, CERN)
- Rozvoj informačnej spoločnosti
  - Masové rozšírenie počítačov a ich prepojenie do sietí,
  - zabudované špecializované počítače do elektronických zariadení
  - Informačný obsah na Internete
  - Najrôznejšie aplikácie
  - Sociálne siete
  - Virtuálna/virtualizovaná realita
- `https://en.wikipedia.org/wiki/Zettabyte`

Prečo potrebujeme informačnú bezpečnosť?

- Každá organizácia má nejaký zmysel existencie (poslanie)
- Na jeho naplnenie vyvíja nejakú činnosť
- Na túto činnosť potrebuje zdroje
- Informácie sú kľúčovým zdrojom
- Aby sa dalo spracovávať potrebné množstvo informácií, používajú sa IKT
- Narušenie IKT a informácií môže organizácii spôsobiť problémy
- Bez IKT sa informácie v požadovanom množstve a čase nedajú spracovávať
- IKT a informácie potrebujeme chrániť - dostatočná úroveň IB je nutnou podmienkou fungovania organizácie

Čo je informačná bezpečnosť (IB)?

- Často sa vyskytujúci dôležitý pojem, ale nie je poriadne definovaný a používa sa v rozličných významoch (=zdroj nedorozumení) [*presne vieme, čo znamená, až kým sa nás na to niekto neopýta.* sv. Augustín]
  - Želaný stav IKT (všetko funguje v súlade s požiadavkami a potrebami organizácie) [úroveň IB v organizácii]
  - Činnosť smerujúca k dosiahnutiu ideálneho stavu [Systém manažmentu informačnej bezpečnosti]
  - Medziodborová vedná disciplína zaoberajúca sa vývojom metód ochrany informácie a IKT
- Pojem IB budeme používať vo všetkých troch významoch, najmä však v druhom

Ciele informačnej bezpečnosti

- Všeobecný cieľ je jasný (mať vždy včas k dispozícii informácie, na ktoré sa môžeme spoľahnúť), ale treba ho konkretizovať, aby bolo možné na jeho dosiahnutie niečo spraviť
- Informácie sú zaznamenané v podobe údajov (údaj = forma, informácia = obsah), ak to nebude podstatné, budeme pojmy údaj a informácia chápať ako synonymá
- Informácie spracovávanie - spracovanie informácií znamená vytváranie, získavanie, prenos, uchovávanie, vlastné spracovávanie, využívanie, archivovanie, ničenie informácií
- Čo potrebujeme chrániť: informáciu od vytvorenia až po zničenie;
- chrániť = zaistiť dôvernosť, integritu, dostupnosť údajov

- **Dôvernosť údajov (confidentiality)** – k informácii, ktorú údaje obsahujú nemajú prístup nepovolané osoby
- **Integrita údajov (data integrity)** – údaje nemôžu byť modifikované bez toho, aby si to oprávnená osoba všimla
- **Dostupnosť údajov (data availability)** – oprávnená osoba má údaje k dispozícii kedykoľvek, keď o to požiada
- CIA = základné bezpečnostné atribúty údajov/informácie alebo základné bezpečnostné požiadavky na ochranu údajov

Poznámky

- Okrem CIA existujú aj iné bezpečnostné požiadavky na ochranu údajov
- Rozdiel medzi prístupom k údajom a prístupom k ich obsahu
- Spôsob zabezpečenia dôvernosti (ochrana prístupu a šifrovanie)
- Dôvernosť – všeobecný pojem a dôverné = druhý stupeň klasifikačnej schémy utajovaných skutočností
- Integrita: absolútna požiadavka – nemennosť údajov – je nerealistická Zaistenie integrity – ochrana prístupu, logy a kryptografické prostriedky
- Dostupnosť – prípustné omeškanie, alebo max. % nedostupnosti

Čo chrániť?

- Informácia počas celého životného cyklu – rôzne formy, v rozličných systémoch, prístup k nej majú rozliční ľudia,
- Rôzne informácie môžu mať rôzne požiadavky na ochranu
- Miera podrobnosti pri špecifikácii informácie/údajov/systémov (väčšia podrobnosť, presnejšie požiadavky, väčšia zložitosť)
- Vnesieme do ochrany informácií systém/poriadok:
- **Aktívum (asset)** – čokoľvek, čo má pre organizáciu hodnotu a vyžaduje si ochranu (príklady: pracovné procesy, činnosti a služby organizácie, dobré meno, informácie, hw, sw, sieť, personál, sídlo, organizačná štruktúra,...)

- **Hrozba** - objektívne existujúca možnosť, ktorej naplnenie môže poškodiť niektoré aktívum (prírodné javy, technické poruchy, chyby, omyly, ľudia)
- Hrozba má **nositeľa** (hrozba záplavy, nositeľ rieka, kanalizačné potrubie)
- **Zraniteľnosť** : chyba, nedostatok, spôsob použitia aktíva, ktoré spôsobujú, že sa hrozba voči aktívu môže uplatniť (príklad: hrozba krádeže, zraniteľnosť – umiestnenie počítača v nezabezpečenej miestnosti)

Základné pojmy IB (2)

- Existujú rozsiahle katalógy hrozieb aj zraniteľností
- Naplnenie hrozby, v širšom zmysle akákoľvek odchýlka od stanovených pravidiel, ktorá môže viesť k narušeniu bezpečnosti – bezpečnostný incident
- **Útok** – cieľavedomý pokus o narušenie informačnej bezpečnosti
- Pôvodca útoku: **útočník**
- **Útočný potenciál**:
  - Motivácia
  - Znalosti
  - Príležitosť
- Príklad: krádež PC a krádež údajov z databázy organizácie

Základné pojmy IB (3)

- **Dopad** – negatívne dôsledky toho, že sa naplnila hrozba voči aktívu (ukradnutý počítač, prezradené heslo)
- samotný dopad nie je dobré kritérium - príklad - pád meteoritu - nepravdepodobný
- **Riziko** = veličina umožňujúca merať prakticky závažnosť hrozieb, zohľadňuje dopad aj pravdepodobnosť udalosti
- **hodnota rizika** stredná hodnota dopadu hrozby (dopad x pravdepodobnosť toho, že hrozba nastane)
- Príklad: organizácia má 100 PC, pravdepodobnosť poruchy 15%, cena opravy 200 Euro, riziko poruchy je 100 x 0.15 x 200 = 3000 Euro

Základné pojmy IB (4)

- **opatrenie**: riešenie (technické, organizačné, personálne, právne, iné), ktoré znižuje riziko (pravdepodobnosť naplnenia a/alebo dopad hrozby)
- **Analýza rizík** – stanovenie a vyhodnotenie rizík vyplývajúcich z hrozieb relevantných vo vzťahu k aktívam organizácie
- **Hranica akceptovateľného rizika** – úroveň rizika, ktorú sa organizácia rozhodla znášať (napr. preto, lebo znižovanie rizika pod akceptovateľnú úroveň nie je z ekonomického hľadiska efektívne)

Základné pojmy IB (5)

- **Informačné a komunikačné technológie** (IKT, anglicky ICT) pojem sa používa na označenie digitálnych IKT
- **Informačný systém** – ucelený systém, ktorý slúži na spracovanie informácie (A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. NIST SP 800-53)
- Zaujímajú nás IS postavené na digitálnych IKT
- Systém a jeho okolie (hranica systému)
- Bezpečnostné prostredie/okolie systému – všetko, čo má vplyv na bezpečnosť systému

Základné pojmy IB (6)

- spory o to, čo potrebujeme/sme povinní chrániť (MH, MIRRI, NBÚ SR)
- logika veci je jasná - všetko, čoho znefunkčnenie alebo narušenie by mohlo znemožniť organizácii (štátu) plniť poslanie
- potrebujeme uchopiť celok ale tak, aby sa dal rozložiť na časti
- nezvyklý, ale výstižný pojem **digitálny ekosystém**
- A digital ecosystem is a distributed, adaptive, open socio-technical system with properties of self-organisation, scalability and sustainability inspired from natural ecosystems. `https://en.wikipedia.org/wiki/Digital_ecosystem`

Vo virtuálnom priestore absentuje fyzický kontakt

Figure: His master voice, (Ilustračný obr. Wikimedia Commons)

Ako zistiť s kým komunikujeme, alebo ako zistiť, kto je kto vo virtuálnom priestore?

- potrebujeme overovať aj autentickosť dokumentov, správ a neživých/nehmotných objektov
- **Entita** (osoba vec, správa, myšlienka, ...) čokoľvek, čo je totožné len so samým sebou a dá sa odlíšiť od iných objektov (entít) toho istého typu
- **Atribúty entity** (vlastnosti, charakteristiky)
- **Identita** = množina atribútov postačujúca na odlíšenie entity od iných entít toho istého typu
- **Absolútna identita**
- Stačí aj podmnožina absolútnej identity
- **Oblasť použiteľnosti identity**
- **Identifikátor** = špecifická identita, môže pozostávať z jediného umelého atribútu, ktorý je entite priradený a ktorý je jedinečný (rodné číslo)

- **Identifikácia** = deklarácia identity (meno)
- **Autentizácia** = potvrdenie deklarovanej identity (heslo)
- Spôsoby autentizácie
  - To čo viem (heslo, PIN)
  - To čo mám (autentizačný token, napr. preukaz, pas)
  - To čo som (biometrické údaje)

Figure: Odtlačok prsta

Cyberspace a pod.

- V IB je veľa pojmov s predponou cyber-
- Nemá to logiku, lebo Kybernetika = veda o riadení v živých organizáciách a strojoch (Wiener, Ashby, Ampér)
- ale William Gibbson v románe Neuromancer 1984 zaviedol pojem

  Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.

Cyberspace

- pojem sa ujal a hoci nemá vnútornú logiku, široko sa používa
- William Gibson o cyberspace

  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.

JULIET
'Tis but thy name that is my enemy;
Thou art thyself, though not a Montague.
What's Montague? it is nor hand, nor foot,
Nor arm, nor face, nor any other part
Belonging to a man. O, be some other name!
What's in a name? that which we call a rose
By any other name would smell as sweet;
So Romeo would, were he not Romeo call'd,
Retain that dear perfection which he owes
Without that title. Romeo, doff thy name,
And for that name which is no part of thee
Take all myself.

Cyberspace

- nemá zmysel viesť terminologickú vojnu, ani hľadať logiku v rôznych pojmoch (pink of death, smurf attack)
- vyše 30 rôznych definícií cyberspace
- V súčasnosti cyberspace označuje informačnú a komunikačnú infraštruktúru alebo
- Sociálne vzťahy budované na základe a udržiavané prostredníctvom Internetu, sociálnych sietí a pod.
- Reálne to je nejaký podsystém digitálneho ekosystému (keď sa o ňom hovorí, treba identifikovať, ktorý to je)
- ďalšie cyber- pojmy sú už našťastie menej rozporné

- **Cybercrime**: kybernetický zločin
  - Trestné činy, pri ktorých sa počítače používajú ako nástroje
  - Trestné činy zamerané na IKT
- **cybersecurity** (kybernetická bezpečnosť) - podmnožina informačnej bezpečnosti, lebo sa zameriava na technickú časť digitálneho ekosystému a rieši cielené útoky naň, ale najrozumnejšie je stotožniť ju s informačnou bezpečnosťou (všetky 3 významy)
- nejde o slová, ale o podstatu - čo treba chrániť
- kompromis, ktorý sa ujal - Kybernetická a informačná bezpečnosť, KIB

- Ďalšie pojmy zavedieme v prednáškach
- V učebnici krátky výkladový slovník pojmov IB (250+ pojmov)
- Existuje veľký výkladový slovník (2000 pojmov)

Legislatíva a odborná terminológia

- spoločnosť sa riadi zákonmi
  - štátne orgány môžu robiť len to, čo im ukladá zákon
  - súkromné organizácie a jednotlivci môžu robiť to, čo im zákon nezakazuje
- zákony pomocou právnych nástrojov občas upravujú aj oblasti, kde platia objektívne zákony alebo pravidlá
- ak je zákon v súlade s objektívnou realitou - dobre, ale často je medzi nimi nesúlad, alebo rozpor
- nekompetentnosť autorov, alebo snaha o súlad s inými, staršími zákonmi, ktoré neuvažovali o špecifickej oblasti, ktorú upravuje novší zákon
- ak ste mali logiku, poznáte Godelove vety o úplnosti
- prirodzený jazyk je menej jednoznančný ako predikátový počet a určite sa v ňom dá popísať formálna aritmetika

Legislatíva a odborná terminológia

- ako občania musíme rátať s nedokonalosťou zákonov, ak sa nám naskytne možnosť tvoriť zákon, bude treba hľadať rozumný kompromis medzi odbornou exaktnosťou a zrozumiteľnosťou/vykonateľnosťou a tiež súlad s inými zákonmi
- špeciálna kapitola sú zákony EÚ, ktoré prekladáme do slovenčiny
- častokrát slovenský preklad nezodpovedá anglickému originálu (eIDAS)
- ale aj nejednoznačnosť jazyka (terminologický štandard ISO)
- mistake, error, failure, fault, fail; chyba, omyl, nedostatok, zlyhanie,kaz
- v KIB je dôležitá schopnosť rozumieť nejasným ale záväzným formuláciám(zákonov, nariadení, štandardov) a vedieť ich interpretovať tak, aby ste ostali v rámci predpisu a spravili to, čo treba

V poslednom čase bolo prijatých niekoľko právnych noriem relevantných z hľadiska informačnej bezpečnosti

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**) (Text with EEA relevance)
  `https://eur-lex.europa.eu/eli/reg/2016/679/oj`
- nadväzne na Nariadenie bol prijatý (a novelizovaný) Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov `https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/`

Aktuálna legislatíva

- Zákon 69/2018 Z. z. o kybernetickej bezpečnosti
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
- Vyhláška Národného bezpečnostného úradu, č. 362/2018 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

- nebudeme sa teraz zaoberať týmito právnymi predpismi pozrieme sa len na to, ako chápu základné pojmy
- Zákon o ochrane osobných údajov

  Osobnými údajmi sú údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje,) alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.

Terminológia Zákona 69/2018 Z. z. o kybernetickej bezpečnosti

- Zákon ide do väčších podrobností a definície sa pri novelizáciách občas menia
- "terminologický" § 3, konkrétne
- pôvodné znenie §3 písm. a) sieťou a informačným systémom elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov,
- aktuálne znenie §3 písm. a) sieťou elektronická komunikačná sieť podľa osobitného predpisu,8)
- odvoláva sa na § 2 ods. 1 zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov.

Zákon o kybernetickej bezpečnosti, § 3

- písm. c) kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi,
- písm. d) kontinuitou strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,
- písm. e) dôvernosťou záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,
- písm. f) dostupnosťou záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná,

Zákon o kybernetickej bezpečnosti, § 3

- písm. g) integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,
- písm. h) kybernetickou bezpečnosťou stav, v ktorom sú siete a informačné systémy schopné 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,
- písm. i) rizikom miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,
- písm. j) hrozbou každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,

Ďalšie informácie o zákone o kybernetickej bezpečnosti

- analyzovali sme Zákon o KB https://obchod.wolterskluwer.sk/sk/zakon-o-kybernetickej-bezpecnosti-komentar.p3976.html a
- https://uniba.sk/infosec/

Zákon o IT vo verejnej správe

- Zákon č. 95/2019 Z. z.Zákon o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
- lex specialis k Zákonu o kybernetickej bezpečnosti (lex generalis)
- nezavádza vlastné pojmy
- podrobne rozoberá povinnosti organizácií verejnej správy prevádzkujúcich informačné systémy
- špeciálne KIB
- veľmi podrobná vyhláška č. 179/2020 Z. z., ktorá kopíruje bezpečnostné opatrenia ISO/IEC normy 27002
- najprv musíme vedieť čo, prečo a ako sa v KIB robí, aby sme vedeli posúdiť ISO normu, resp. požiadavky zákonov a vyhlášok

Vybrané zákony EÚ

- hierarchia
  - Nariadenie
  - Smernica
  - Odporúčanie
- Nariadenie eIDAS – upravuje služby na zaistenie dôvery v digitálnom priestore
- Na Slovensku – Zákon o e-governmente
- GDPR – ochrana osobných údajov
- Zákon o ochrane osobných údajov

Vybrané zákony EÚ

- COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
- Zákon č. 45/2011 Z. z. o kritickej infraštruktúre
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
- Európska komisia dňa 16.12.2020 prijala návrh "novej smernice NIS" (tzv. Smernica NIS II), ktorá má prvú Smernicu NIS nahradiť.

Historický vývoj IB/KIB

- Stará záležitosť (šifrovanie)
- Kryptológia, steganografia
- Špionáž, kryptoanalýza
- Povojnová konferencia v Paríži
- Enigma, Purple
- Orange Book, NSA
- DES
- Rainbow series
- Common Criteria
- ISO/IEC JTC 1 SC 27

Zdroje

- NIST SP 800 https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-informati
- BSI Standards https://www.bsi.bund.de/EN/Home/home_node.html
- resp. špeciálne štandardy BSI https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
- https://www.ncsc.gov.uk/section/education-skills/cybok
- Učebnica v súboroch