Informačná bezpečnosť(2)

Spoločnosť, informácia, informačné technológie, informačná bezpečnosť

Obsah prednášky

- význam informácie pre rozvoj ľudskej spoločnosti
- Vývoj informačných potrieb a informačných technológií
- Informačná bezpečnosť v klasickej ére
- Moderná éra: automatizácia spracovania informácií
- Informačné a komunikačné technológie
- Informatizácia spoločnosti
- Význam informačnej bezpečnosti pre informačnú spoločnosť
- História informačnej bezpečnosti
- Zdroje ohrozenia IKT
- Prehľad základných pojmov informačnej bezpečnosti
-
-

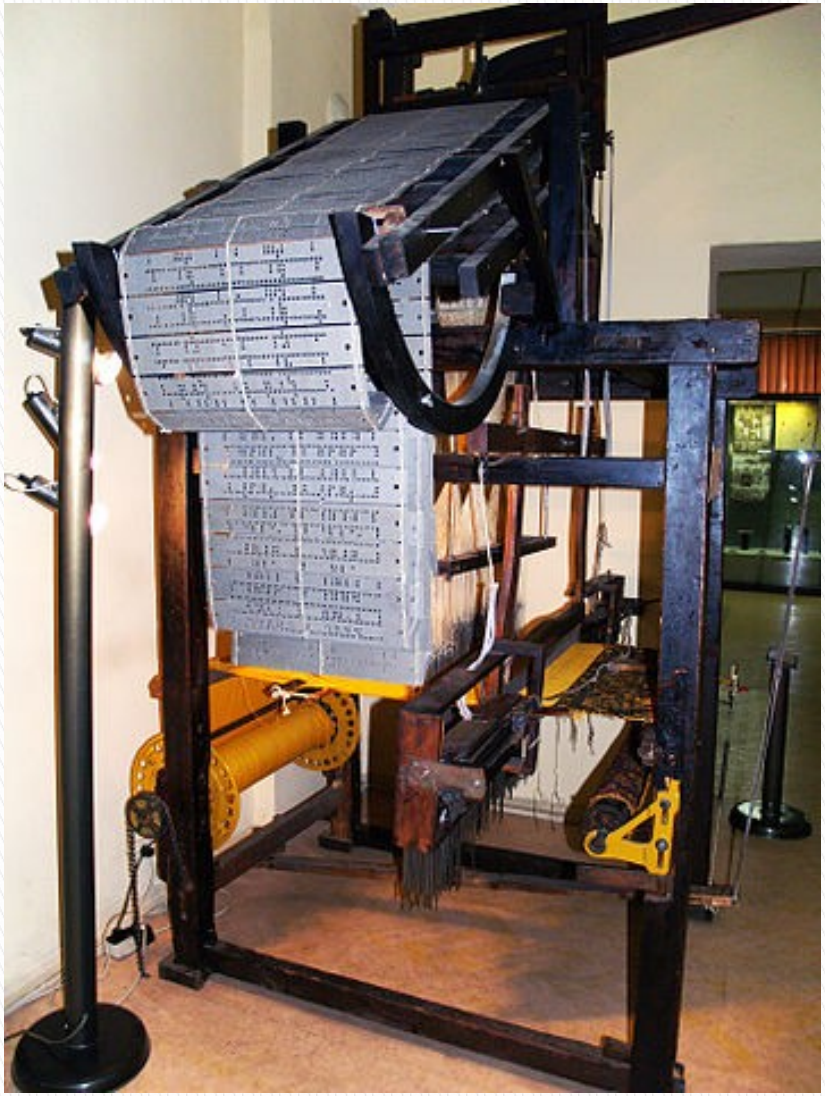
Význam informácie pre rozvoj ľudskej spoločnosti

- Existencia systému (organizmus, organizácia, spoločnosť, technický systém) v prostredí – monitorovanie podmienok, predvídanie zmien a reakcie na ne
- Schopnosť spracovávať a využívať informácie = podmienka prežitia
- Komunikácia – základ pre spoluprácu (signály, jazyk)
- Individuálna skúsenosť a kumulované poznanie (učenie)
- Písmo (presnosť, trvácnosť, nie je potrebný sprostredkovateľ, rozsah, rýchlosť spracovania)
- Klasické informačné a komunikačné technológie (IKT) – kľúčový prvok = človek
-

Vývoj IKT (1)

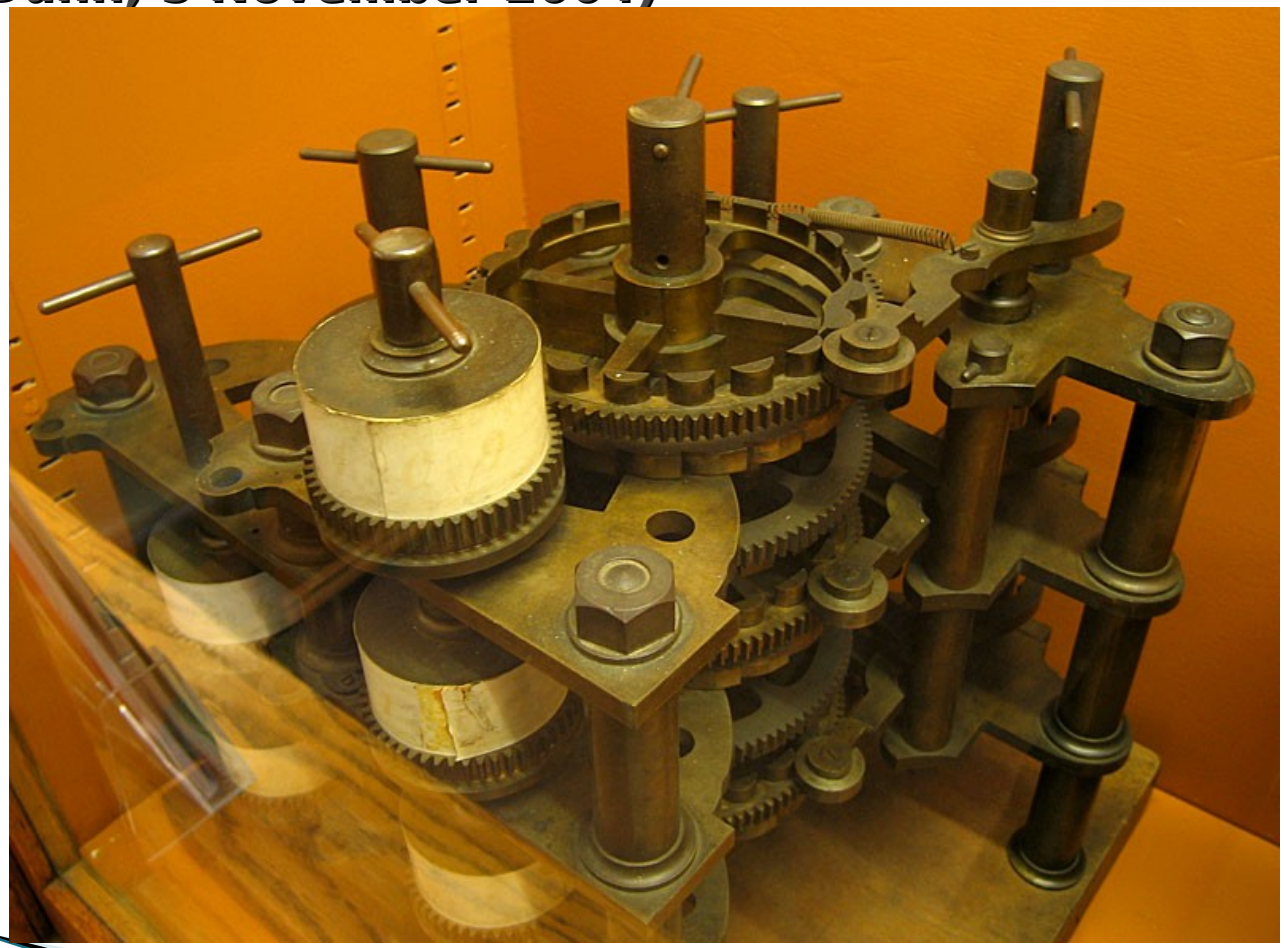
- Kníhtlač – zvýšenie dostupnosti informačných zdrojov
- Mechanické počítadlá – nerozšírili sa
- Komunikácia pomocou optických a zvukových signálov optický telegraf (Napoleon)
- Narastajúce potreby: množstvo informácií, presnosť, rýchlosť prenosu, dostupnosť
- Prvé pokusy o mechanizáciu spracovania informácie
  - Jacquardove krosná
  - Babbageov diferenčný a analytický stroj
- Telegraf, telefón, podmorské káble
- USA – sčítanie ľudu v roku 1890 – Hollerithove diernoštítkové stroje
- Rádiové vysielanie
-
  -
  -
-
-
-

Jacquardove krosná



- Austrian hand-driven Jacquard loom, end of 19th century, now in the National Museum of Textile Industry, Sliven, Bulgaria

Part of Charles Babbage's Difference Engine (Photograph © Andrew Dunn, 5 November 2004)



This is a file from the Wikimedia Commons

Vývoj IKT (2)

- Rozhlas, televízia
- Počítače (riadenie protilietadlovej paľby, lúštenie šifier, neskôr vedecké a ekonomické výpočty)
- Masovokomunikačné prostriedky
- Počítačové siete
- Koncom 80-tych rokov konvergencia počítačov, masovokomunikačných prostriedkov a masmédií = moderné IKT
- Narastajú informačné potreby spoločnosti
- IKT:
  - digitálny zápis informácie
  - Spoločné prenosové médiá
  - Využitie počítačov pri spracovaní informácie
-

Vývoj IKT (3)

- Klesajúca cena, rastúca výkonnosť
- Programové vybavenie umožňuje, aby ich používali laici
- Narastajúci počet aplikácií
- Mobilné zariadenia
- IKT (pôvodne nástroj) ovplyvňujú spoločnosť (kde všade by sa IKT dali použiť)
- Informatizácia spoločnosti – redesign tradičných procesov, aby sa dali využívať IKT
- Dôvod: rýchlejšie, lacnejšie, pohodlnejšie, ale najmä – súčasné informačné potreby spoločnosti sa nedajú zabezpečiť pomocou tradičných (ručných) metód spracovania informácie
- Dôsledok: spoločnosť je závislá od fungovania svojich IKT

Prečo potrebujeme informačnú bezpečnosť?

- Spoločnosť je závislá od fungovania svojich IKT; IKT sú súčasťou jej kritickej infraštruktúry
- Keby došlo k narušeniu IKT, nemôžeme sa z kapacitných dôvodov vrátiť k ručnému spracovaniu informácie
- Narušenie IKT môže spôsobiť viacero faktorov:
  - Technická porucha (sú zložité, je ich veľa, majú veľký rozsah)
  - Chyba programového vybavenia
  - Neúmyselná ľudská chyba (omylný, nekvalifikovaný a unavený personál)
  - Prírodná katastrofa (využívajú rozsiahlu fyzickú infraštruktúru)
  - Úmyselný útok (ekonomický prospech, pomsta, terorizmus, špionáž, kybernetická vojna)
- Majú globálny charakter (dominový efekt)
- Riadia technologické systémy bežiace v reálnom čase

Informačná bezpečnosť(IB)

- Trojaký význam pojmu IB
  - Interdisciplinárna oblasť
  - Ideálny stav IKT a/alebo informačných a komunikačných systémov organizácie
  - Činnosť zameraná na dosiahnutie ideálneho stavu
- Budeme uvažovať všetky tri významy
- Pripomíname, že
  - IB nevznikla až s príchodom IKT
  - Má minimálne 4000 ročnú históriu (šifrovanie)
  - So vznikom IKT IB získava nový obsah
  - Ale – stále je potrebné chrániť informáciu
- Nová situácia - oslabenie väzby informácie/údajov na materiálny nosič – výhoda z hľadiska spracovania, nevýhoda z hľadiska bezpečnosti
-
-

História informačnej bezpečnosti (1)

- Prečo? Lebo budúcnosť je pokračovaním minulosti
- Samostatná kapitola informačnej bezpečnosti je kryptológia a komunikačná bezpečnosť
- Kahn D. The Codebreakers, Scribner, New York 1996
- 2. svetová vojna (Enigma, Purple)
- Po 2. svetovej vojne rozvoj telekomunikácií (nelegálne telefonovanie)
- Počítače a elektronické IKT
  - (obdobie 1950-1975) počítačové sály najmä fyzická a režimová bezpečnosť
  - Terminály, lokálne siete, fyzická ochrana nepostačuje
  - 80-te roky – prepojenie cez modemy a telefónne linky
  - Nové služby bulletin board service (BBS)
  - Koniec 80-tych rokov PC a Internet

História informačnej bezpečnosti (2)

- Prvý červ (Morris 1988)
  http://en.wikipedia.org/wiki/Morris_worm
- CERT http://www.cert.org/
- Hackeri
- Vírusy a iná háveď
- Nedávna minulosť a súčasnosť
  - Elektronický obchod
  - Profesionalizácia útočníkov
  - Ekonomické motívy
  - Kriminálne živly a teroristi
  - Špionáž
  - Vojna v cyberpace

História informačnej bezpečnosti (3)

Aktuálne problémy (BSI)

- Poruchy systémov a infraštruktúry
- Bezpečnostné diery
- Zlomyseľný softvér
- DoS útoky
- Nevyžiadaná pošta
- Bot-nets
- Phishing a krádeže identity
- Vlastní zamestnanci, chyby a nedbalosť
- Outsourcing

Dodávame

- Terorizmus
- Sociálne siete
- Špionáž a sabotáže
- Štátom organizované/podporované útoky
-

História informačnej bezpečnosti (4)

- Politický dosah
  - USA (podrobnejšie pri legislatíve a štandardoch)
  - EÚ – informatizácia spoločnosti (e-Europe, i-Initiative)
- Echelon a UKUSA
- Čo z toho vyplýva:
  - IKT = Kritická infraštruktúra spoločnosti
  - Ochrana digitálneho priestoru si vyžaduje komplexný a koordinovaný prístup
- Naviac spoločenské aspekty
  - Ochrana duševného vlastníctva
  - Ochrana súkromia
  - Právo na informácie
  - Sloboda prejavu
- Budúcnosť ???

Odvrátená tvár informačnej bezpečnosti - The Big Brother

November 1999, WASHINGTON (NWS) -- The U.S. Navy is supporting new speech recognition research for its potential benefits to Navy sonar. Biomedical engineers at the University of Southern California have created the world's first machine system that can recognize spoken words better than humanscan. In benchmark testing, USC's speech recognition system bested all existing computer systems and outperformed the keenest human ears. The system may eventually advance voice control of computers and other machines, help the deaf, aid air traffic controllers and others who must understand speech in noisy environments, and instantly produce clean transcripts of conversations, with each speaker correctly identified.

a ekonomika ...

- some examples of the misuse of economic information intercepted by global networks such as *ECHELON.*
  - We can actually quote the contract which was spirited away from France in January 1994. It involved an arms supply contract worth 30 million francs with Saudi Arabia. The contract ended up with McDonnell-Douglas, the rival of the Airbus consortium, because the former was privy to the financial terms offered by Airbus thanks to the electronic interception system.
  - that ECHELON has been used to benefit American companies involved in arms contracts and to strengthen Washington´s hand in major negotiations with Europe in the World Trade Organisation in relation to disputes with Japan concerning the export of motor vehicle spare parts.
  - the French electronics giant, Thomson, had lost a contract worth 1.4 million dollars for the supply of a surveillance system to Brazil because the Americans had intercepted details of the negotiations and passed them on to the US Raytheon Corporation, which subsequently won the contract.

Terorizmus (1)

Cyberterrorism is defined as “The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives.” (Kevin G. Coleman of the Technolytics Institute.)

Terorizmus (2)

- Potenciál veľký, hrozba zatiaľ reálne nenaplnená (výnimka Estónsko, možno NIMDA)
- Aktraktívny
  - Anonymita
  - Potenciál spôsobiť veľké škody
  - Psychologický dopad
  - Príťažlivá téma pre médiá
- Cyberterrorism spája dve obavy
  - Možnosť stať sa náhodnou obeťou
  - Strach z počítačových technológií
- Médiá preháňajú (Dan Brown Digital Fortress)
- Kritické informačné systémy sú chránené (aj air gap), ale nie dostatočne Stuxnet – SCADA (2010)

Estónsko

- V apríli 2007 chceli v Talline premiestniť sochu a hrob neznámeho vojaka
- Protesty ruskej minority
- Denial od service attack na vládne systémy, banky, noviny, telekomunikačných operátorov
- Na webe premiéra Andrusa Ansipa – zverejnený falošný ospravedlňujúci list
- Predpoklad – Rusi, sa nedokázal
- Pôvodca nebol odhalený, v januári obvinili jediného človeka (Dmitri Galushkevich) za účasť na útoku, dostal pokutu asi 1600 USD
- http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
- Estonia has urged its allies in the European Union and NATO to take firm action against a new mode of warfare

ACTA, TRIPS, IPR a ľudské pr a

- V digitálnom priestore sa podniká
- Nedajú sa doň mechanicky preniesť pravidlá z fyzického sveta
- Vzťahy vo virtuálnom svete sa len vyvíjajú a ťažko sa regulujú
- Zločinci objavili možnosť podnikať v digitálnom priestore (krádeže identity, pirátstvo, krádeže údajov, špionáž a pod.)
- Pokusy zaviesť pravidlá na postihnutie zločincov sa stále objavujú, ale
  - Sú jednostranné (preferujú záujmy držiteľov IPR)
  - zasahujú neprimerane do práv obyčajných ľudí
  - a sú neúčinné
- O ACTA, TRIPS, EU direktívach na ochranu intelektuálneho vlastníctva budeme hovoriť

Aktuálne

"Whereas intellectual property is important to society and must be protected, it should not be placed above individuals' fundamental rights to privacy and data protection [and other rights such as presumption of innocence, effective judicial protection and freedom of expression]. A right balance ... should be ensured."

European Data Protection Supervisor, Peter Hustinx

(Press release of 22 February 2010, accompanying the EDPS Opinion on the then available text of ACTA.

The words in square brackets have been added; they are taken from para. 83 of the Opinion)

- ACTA vzbudila nebývalú pozornosťverejnosti aj politikov

Ale aké je riešenie?

Prehľad základných pojmov

- Skôr, ako budeme pokračovať, pripomenieme aspoň stručne základné pojmy informačnej bezpečnosti
  - IKT systém, jeho aktíva, bezpečnostné okolie, hrozba, zraniteľnosť, riziko, nositeľ hrozby, útok
  - Údaje a informácia
  - Bezpečnostné aspekty informácie (dôvernosť, integrita, dostupnosť, autentickosť a i.)
  - Analýza rizík, ohodnotenie rizík, návrh a implementácia opatrení, zvyškové riziko, správa rizík
  - Kontinuita činnosti, zotavenie po katastrofách
  - Bezpečnostná politika, systém riadenia informačnej bezpečnosti
- K týmto pojmom sa ešte vrátime a rozoberieme ich detailnejšie