Informācijas sistēmu drošība

Informācijas sistēma definīcijas

- Iekārtu, procedūru un personāla kopums, kas ir izveidots, strādā un tiek uzturēts, lai vāktu, uzkrātu, apstrādātu, uzglabātu un izmantotu informāciju.

Informācijas sistēma

Informācijas aprite — informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, lietošana un iznīcināšana;

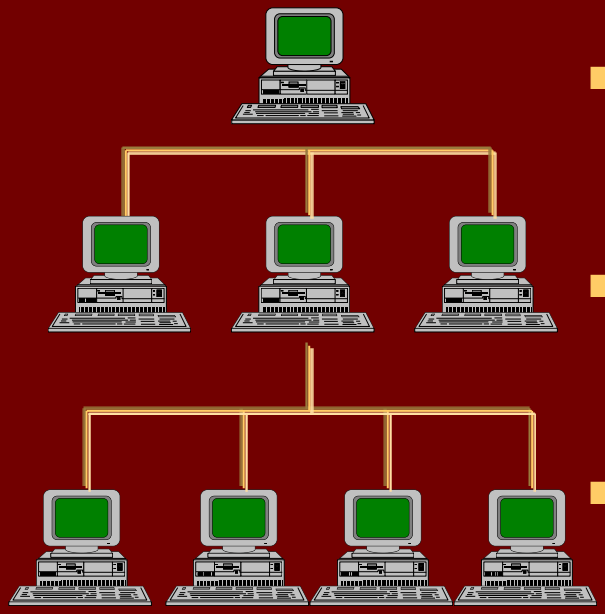
PUBLISKA PIEEJAMĪBA

NAV

ĪPAŠU PRASĪBU

Iegūst vai nosūta informāciju

globālajā tīmeklī



IEROBEŽOTA PIEEJAMĪBA

- informācijas **konfidencialitāte** - informācijas aizsardzība pret neautorizētu piekļuvi tai;
- informācijas **pieejamība** - autorizēta piekļuve informācijai nepieciešamajā laikā un vietā;
- informācijas **integritāte** - informācijas satura un struktūras nemainīguma saglabāšana.

Informācijas aprites kritiskās funkcijas

Vīrusi

- Vīrusi:
  - Sākumsektora inficētāji;
  - Datņu inficētāji;
  - Makrosu vīrusi;
  - Tārpi;
  - Trojas zirgi;
- Robottīkli;
- BIOS vīrusi;
- Utt..

Aizsardzība pret vīrusiem

- Atcerieties, ka vīrusi datorā nerodas paši no sevis - tie tiek iegūti no inficētām datnēm vai diskiem, vai lejupielādēti no interneta.

- Lai savu datoru aizsargātu no vīrusiem:
  - Lietojiet labas un uzticamas antivīrusu programmas;
  - Apmāciet lietotāju ikdienā veikt datu nesēju un datora skenēšanu;
  - Apmāciet personālu apmeklēt tikai uzticamas vietnes;

Informācijas sistēma definīcijas

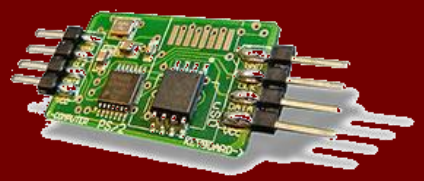
- Virtuālā mašīna

  virtuāla sistēma, kas šķietami nodota katra atsevišķa lietotāja rīcībā, bet kuras darbība tiek nodrošināta, virtuālo mašīnu lietotājiem kopīgi izmantojot reālās informācijas sistēmas resursus;

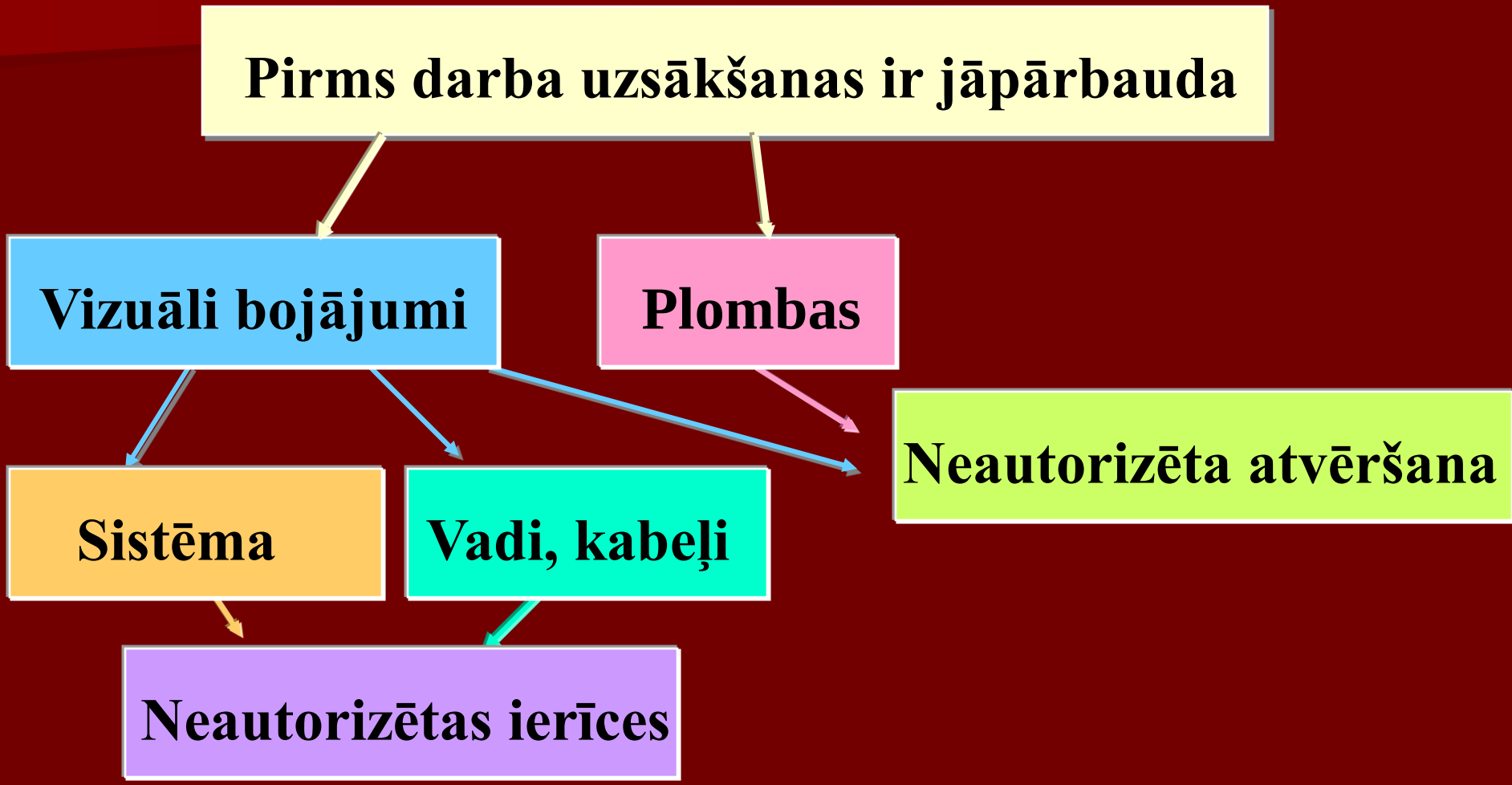
Sistēmas komponentes

Drošības pasākumi pirms darba uzsākšanas

Vizuālā pārbaude tiek veikta ar nolūku novērst informācijas noplūdes iespējas, jo tieši sistēmas komponentes ir vājās vietas, kurām var pieslēgt neautorizētas iekārtas.



Drošības pasākumi pirms darba uzsākšanas



Sistēmas komponentes

Pamanot jebkādas pazīmes, kuras liecina par korpusa atvēršanu, aprīkojuma bojājumu vai tā neesamību, par notikušo nekavējoties jāinformē informācijas sistēmas drošības amatpersonas.

IS drošība

- Pirms informācijas sistēmas nodošanas lietotājiem darba stacijām ierobežo iespēju pievienot pārnēsājamos datu nesējus.

IS apdraudējumi lietojot ārējos datu nesējus

Konfidencialitātes zaudēšana

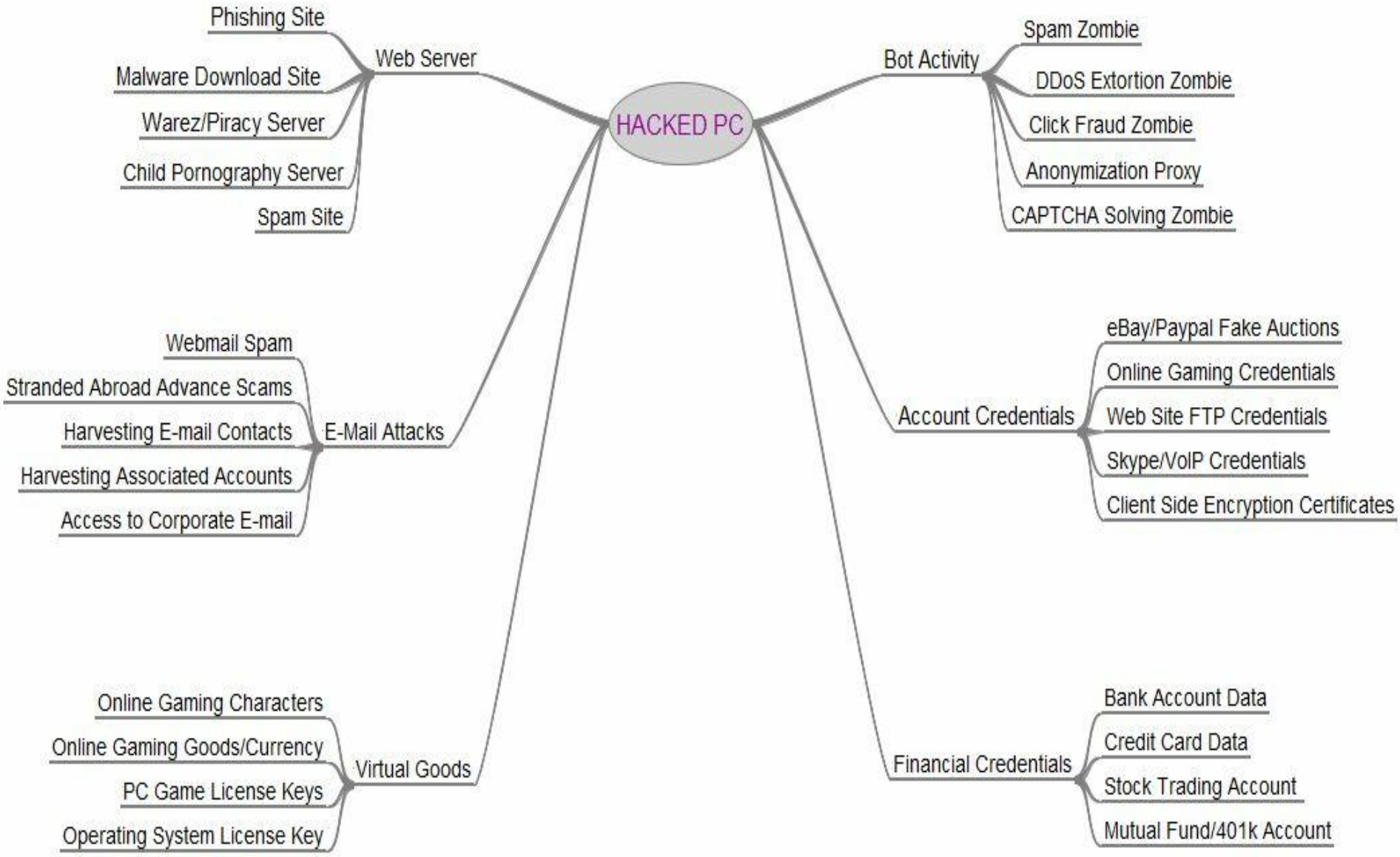
- Ārējo datu nesēju nepareiza izmantošana var nopludināt informāciju, apejot visus IS aizsardzības pasākumus

Integritātes zaudēšana

- Ar inficētu ārējo datu nesēju var panākt datu sagrozīšanu, dzēšanu, kopēšanu (virusi un ielaušanās programmas)

Pieejamības zaudēšana

- Inficēts ārējo datu nesējs var radīt pārslodzes tīklā, bloķēt pieeju pie datiem vai tos izdzēst


HACKED PC
Web Server
Phishing Site
Malware Download Site
Warez/Piracy Server
Child Pornography Server
Spam Site
Bot Activity
Spam Zombie
DDoS Extortion Zombie
Click Fraud Zombie
Anonymization Proxy
CAPTCHA Solving Zombie
E-Mail Attacks
Webmail Spam
Stranded Abroad Advance Scams
Harvesting E-mail Contacts
Harvesting Associated Accounts
Access to Corporate E-mail
Account Credentials
eBay/Paypal Fake Auctions
Online Gaming Credentials
Web Site FTP Credentials
Skype/VoIP Credentials
Client Side Encryption Certificates
Virtual Goods
Online Gaming Characters
Online Gaming Goods/Currency
PC Game License Keys
Operating System License Key
Financial Credentials
Bank Account Data
Credit Card Data
Stock Trading Account
Mutual Fund/401k Account

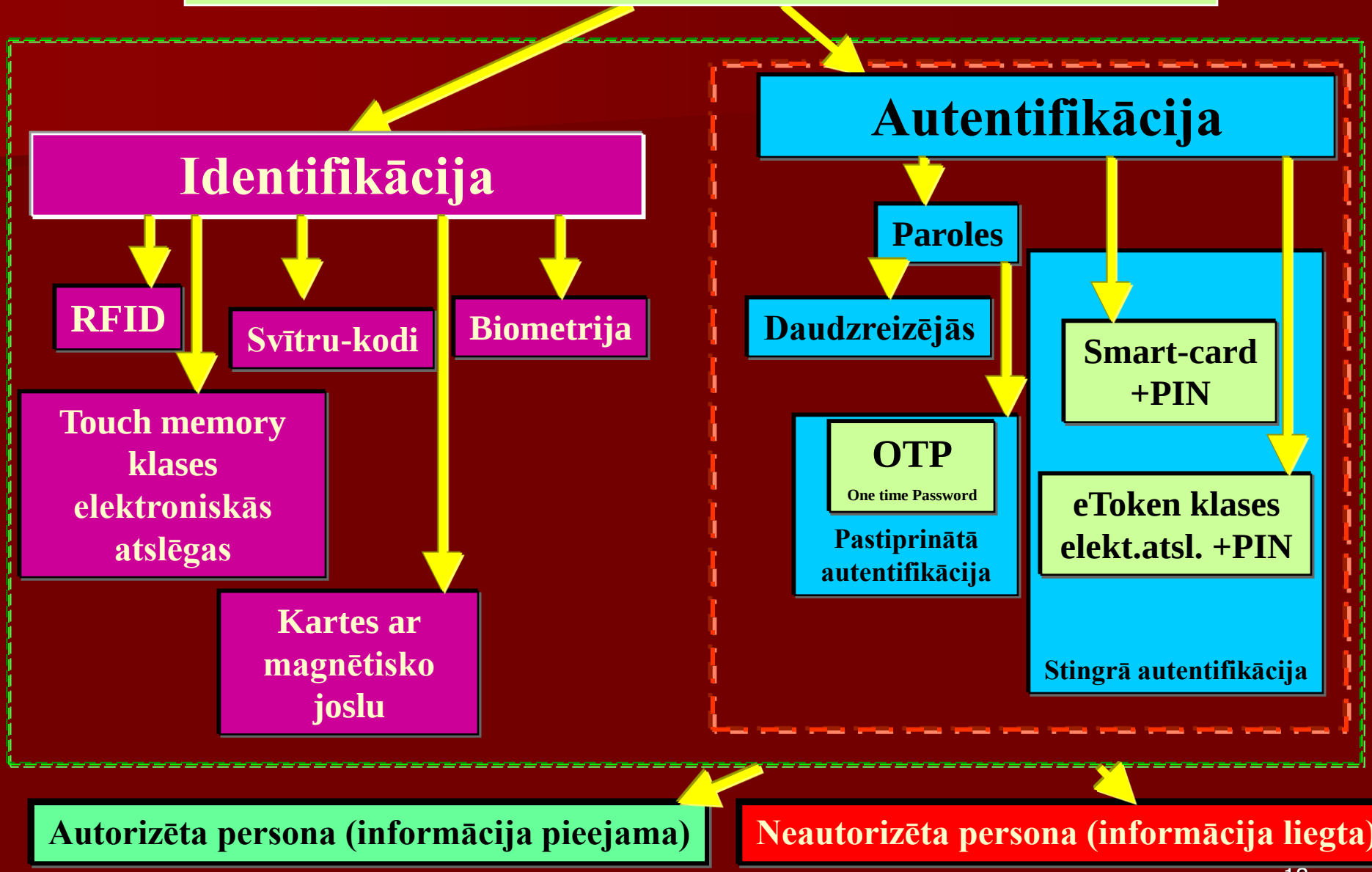
Izgūstāmā informācija

Item	Advertised Price (in US Dollars)
United States-based credit card with card verification value	$1–$6
United Kingdom-based credit card with card verification value	$2–$12
An identity (including US bank account, credit card, date of birth, and government issued identification number)	$14–$18
List of 29,000 emails	$5
Online banking account with a $9,900 balance	$300
Yahoo Mail cookie exploit—advertised to facilitate full access when successful	$3
Valid Yahoo and Hotmail email cookies	$3
Compromised computer	$6–$20
Phishing Web site hosting—per site	$3–5
Verified PayPal account with balance (balance varies)	$50–$500
Unverified PayPal account with balance (balance varies)	$10–$50
Skype account	$12
World of Warcraft account—one month duration	$10

Table 3. Advertised prices of items traded on underground economy servers
Source: Symantec Corporation

Identifikācija, autentifikācija un autorizācija

Identifikācija un Autentifikācija



Identifikācija

Lietotāja identifikācija

Lietotāja atpazīšana pēc biometrijas un/vai dažādu veidu ID kartēm vai elektroniskajām atslēgām. Šo darbību veic, lai lietotājus atšķirtu vienu no otra.

Autentifikācija

Lietotāja autentifikācija

Lietotāja atpazīšanas process, kura gaitā noskaidro, vai lietotājs atbilst uzrādītajam identifikatoram (legāls vai nelegāls).

Autorizācija

Autorizācija

Procedūra, ar kuru datorsistēma lietotajam piešķir noteiktas pilnvaras un resursus šajā sistēmā. Atšķirībā no autentifikācijas, kura nosaka legālos un nelegālos lietotājus, autorizācija nodarbojas tikai ar legālajiem lietotājiem, kuri izgājuši autentifikācijas procedūru.

Lietotāja parole

Parole

Rakstzīmju (parasti burtu un ciparu) virkne, ko izmanto, lai autentificētu lietotāju, kuram ir tiesības izmantot datoru tīkla resursus un pakalpojumus. Dažkārt parole precizē resursu un pakalpojumu izmantošanas tiesību robežas, piemēram, nosaka, vai lietotājs drīkst tikai lasīt informāciju vai arī to kopēt.

Parole

Informācijas sistēmas paroles veido šādi:

Izvērtējot sistēmā izmantoto programmatūru, pielietotos lietotāju autentifikācijas mehānismus un veikto risku analīzi;

- Izmanto lielos un mazos burtus;
- Izmanto ciparus;
- Izmanto speciālās zīmes.

Piemērs parolei: ***q%5kjA#9a!***

Parole

Paroli nepieciešams mainīt ne retāk kā ik pēc iestādē noteiktā laika, vai ikreiz, kad tā šķiet nedroša (piemēram, ja uzskatāt, ka kāds ir redzējis jūs ievadām paroli).

Darbinieku prombūtnes laikā vai amata pienākumu pārstrukturēšanas gadījumos paroles un citus ID parametrus citam darbiniekam nenodod.

Parole

Paroles *ir daļa no personas identifikācijas procesa, un nododot vai dodot iespēju kādam lietot Jūsu paroli, Jūs uzreiz apdraudat visu drošību un tā persona pilnīgi droši darbosies Jūsu vārdā, un par visiem nodarītajiem kaitējumiem nāksies atbildēt Jums.*

Sociālie tīkli

- Sargāt profilus ar uzticamu paroli;
- Nepublicēt aizsargājamu informāciju, attēlus ar tehniku, telpām, utt;
- Rūpīgi izvēlēties informāciju, kuru publicējam par sevi;
- Akceptējam tikai labi zināmus cilvēkus;

E-pasts

- Nevērt vaļā vēstules no nezināmiem adresātiem;
- Nevērt vaļā SPAM vēstuļu pielikumus;
- Nevērt vaļā vēstuļu pielikumus pirms tam tos nepārbaudot ar antivīrusa programmatūru;
- Droši glabāt paroli;
- SPAM filtri;

Interneta lietošana

- Apmeklēt tikai uzticamas tīmekļa vietnes;
- Pievērst uzmanību pēkšņlodziņiem (popup);
- Vienmēr pārbaudīt ievadītās adreses;
- Aizdomīgu e-pasta saturā esošās adreses neaktivizēt, bet izmantot iepriekš sagatavotas grāmatzīmes, vai ievadīt pašrocīgi;

Marķēšana

Vairākkārtēji izmantojamos datu nesējus klasificē atbilstoši to izmantošanas laikā tajos plānotās uzglabājamās informācijas augstākajai klasifikācijas pakāpei.

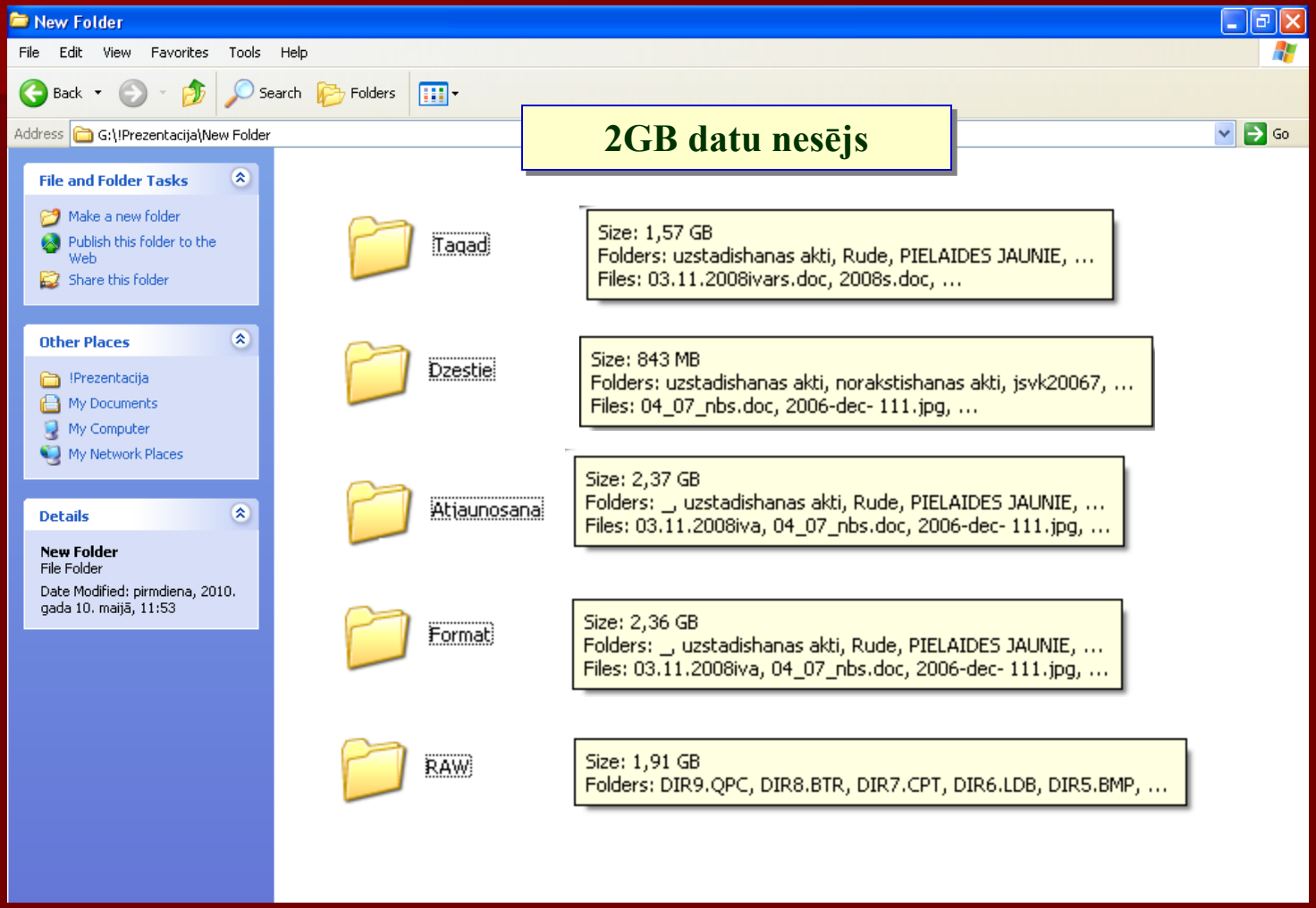
Elektroniskās informācijas un datu nesēju dzēšana

- Informācijas sistēmā izmanto drošus datu dzēšanas līdzekļus, kas izdzēš datus. Pirms datu dzēšanas līdzekļu uzstādīšanas informācijas sistēmā informācijas atbildīga amatpersona veic minēto līdzekļu pārbaudi.

Datu nesēju iznīcināšana

- 100% droša datu dzēšana tiek uzskatīta tad, kad tiek iznīcināts pats datu nesējs:
  - Cietie diski;
  - Zibatmiņas un CD/DVD;
  - Atmiņas kartes;
  - Drukas kasetnes;
  - Magnētiskās lentes;
  - Utt;

Iznīcināšana un atjaunošana



Kontaktinformācija

NBS Sakaru skola
Rīga, Ezermalas ielā – 8
LV - 1014