



Drošība Internetā

10.08.2011. Ratniekos

Kirils Solovjovs

Saturs

- Teorija
- Apdraudējumi
- Lietojumi
- Risinājums

Svarīga atziņa (1)

Tas, ka kaut kas var notikt,
nenozīmē, ka tas tiešām notiks

Svarīga atziņa (2)

Pārlieku lielas rūpes par drošību radīs problēmas:

- draugi
- klienti
- saprāts

Svarīga atziņa (3)

Pārlieku mazas rūpes par drošību radīs problēmas:

- draugi
- klienti
- saprāts

Nedaudz teorijas

ID = integritāte + pieejamība + konfidencialitāte
+ (autentiskums + nenoliedzamība)

Integritāte

Informāciju nevar nemanāmi izmainīt

Pieejamība

Informācijai var piekļūt jebkurā brīdī

Konfidencialitāte

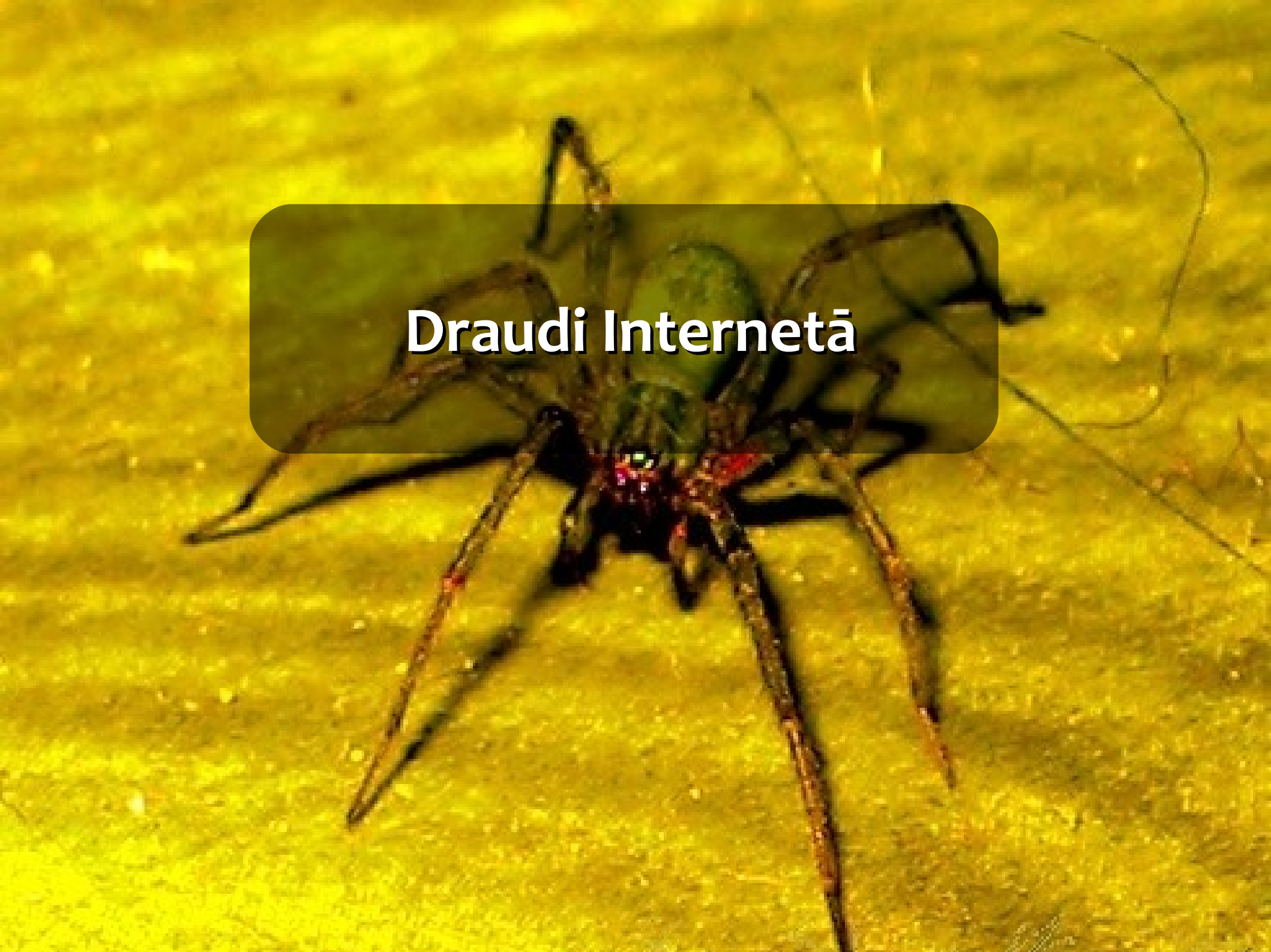
Informācijai var piekļūt tikai autorizētas personas

Autentiskums

Informācija ir īsta, to radījušas pareizās personas

Nenoliedzamība

Autors nevar noliegt to, ka viņš ir piekritis datiem



Draudi Internetā

Sociālā inženierija

- Manipulēšana ar cilvēkiem komunicējot
- Parasti ar mērķi iegūt informāciju vai piespiest veikt kādu darbību

Vīrusi un tārpi

- Vīrusi – pagājušais gadsimts
- Tārpi – gan tīmeklī, gan pārējā Internetā
- Pielikumi
- Sociālā inženierija
- Teksta utml. dokumentus

Identitātes zādzība

- Izlikšanās sociālajos tīklos
- Uzdošanās, piemēram, veicot finanšu darījumus

Hakeri

- Profesionāļi un amatieri
- Mērķi ir
 - viegli pieejamas vietnes
 - vietnes ar svarīgu informāciju
 - vietnes ar interesantu informāciju

Zādzība

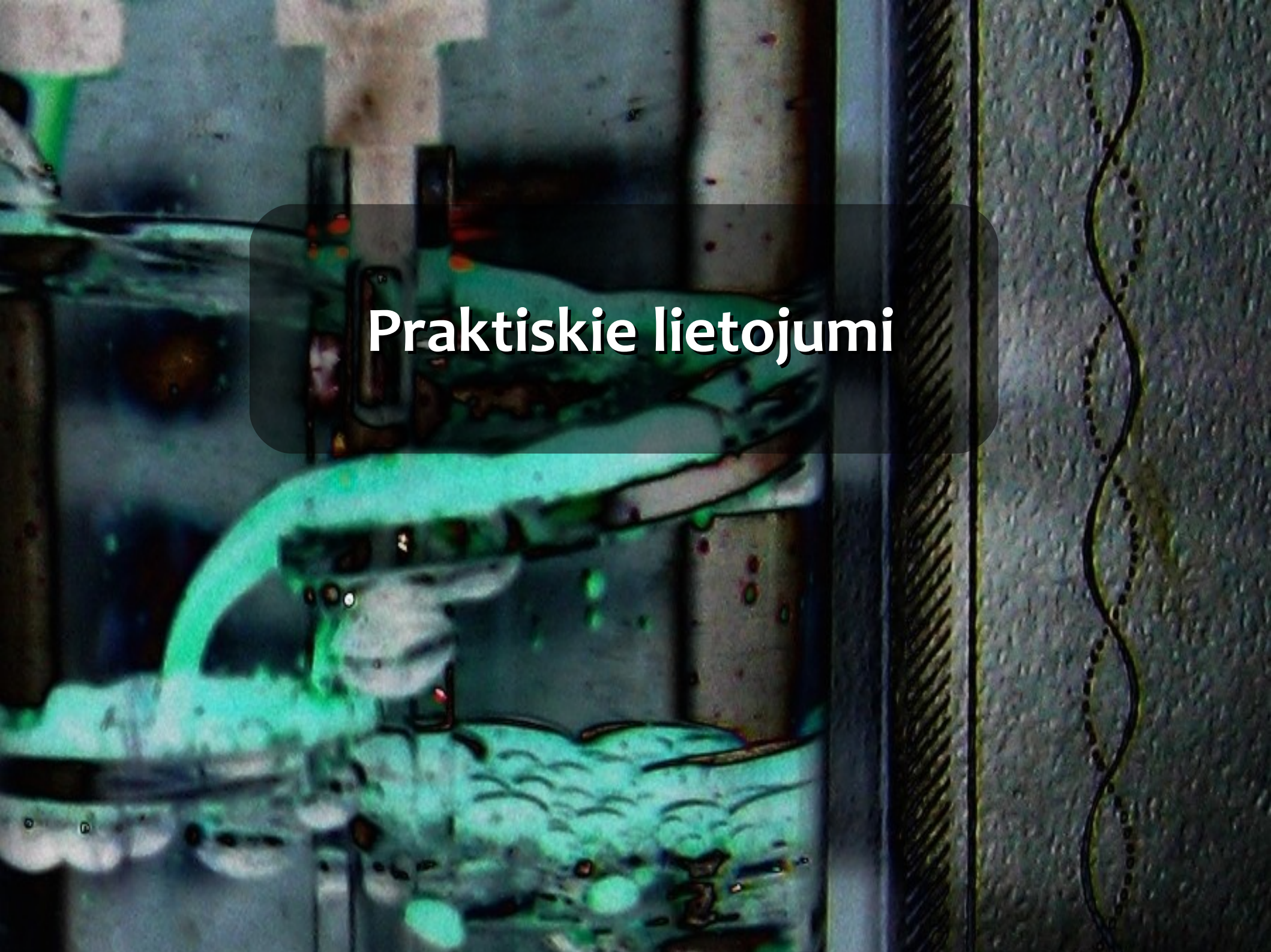
- Informācijas noplūde
- Autorizācijas noplūde

Privātuma apdraudējums

- “Cepumu” datnes
- Lielo korporāciju veikta izsekošana
- Labticīga informācijas nodošana
- Spiegošanas programmatūra
- Nešifrēts savienojums
- Programmētāja kļūda

Sekas

- Kādas ir iespējamās sliktākās sekas?
 - Laupīšana, cietums, dzīvības un veselības apdraudējums, uzņēmuma likvidācija...
- Kādas ir ticamās sekas?
 - Sūdzības saņemšana, reputācijas zaudējums, soda nauda



Praktiskie lietojumi

E-pasta saziņa

- Publiskais e-pasts: gmail, inbox, u.c.
- Privātais e-pasts:
 - izglītības iestāžu
 - korporatīvais
 - individuālais

Sociālie tīkli

- Facebook
- Draugiem
- Twitter
- 4square

Tērzēšana un balss zvani

- Gtalk / jabber
- IRC
- Skype
- VoIP
- Sociālo tīklu čati

Anketas un aptaujas

- Visidati: Skaistumkopšanas nozīme
- Google: RTU studentu aptauja
- Doodle: Aptauja par sēdes laiku
- Individuāli izstrādāts: LF reģistrācijas anketa
- Dokumentu iesūtīšana, personiskā saziņa

Masu saziņa

- Mājaslapas
- Prese relīzes
- Vēstkopas



Privātuma apdraudējumu risinājums

Iepriekš

- Saziņa starp cilvēku iekārtām
 - Caur serveri
- Saturs kļūst zināms serverim
- Ir izņēmumi:
 - SILC
 - PGP

Rezultāts (1)

- Gala iekārtas šifrē ziņojumus
 - izmantojot kopīgu atslēgu
 - $(A \rightarrow S \rightarrow A)$
 - $(A \rightarrow S \rightarrow B_1, B_2, B_3, \dots B_n)$
 - izmantojot saņēmēja publisko atslēgu
 - $(A_1, A_2, A_3, \dots A_n \rightarrow S \rightarrow B)$

Rezultāts (2)

- Katram ierakstam tiek pievienots unikāls ID
- Serveris uztur saturu, bet algoritmiski nevar atšifrēt

Piemērs – RFC 5545 – iCalendar

```
BEGIN:VEVENT
CREATED:20110523T160718Z
LAST-MODIFIED:20110524T141724Z
DTSTAMP:20110608T134901Z
UID:29265a25-5696-487b-b3ea-d773d50534c6
SUMMARY:iesniegt Briseles saturisko atskaiti
PRIORITY:5
STATUS:CONFIRMED
DTSTART;TZID=Europe/Riga:20110524T170000
DTEND;TZID=Europe/Riga:20110524T174500
CLASS:PUBLIC
TRANSP:OPAQUE
SEQUENCE:3
END:VEVENT
```

Piemērs – RFC 5545 – iCalendar

```
BEGIN:VEVENT
CREATED:20110523T160718Z
LAST-MODIFIED:20110524T141724Z
DTSTAMP:20110608T134901Z
UID:29265a25-5696-487b-b3ea-d773d50534c6
ENCRYPTED:hQQOA8RlwneaJcgcEA//bOwVZ08dhJ879Ms5B5CR/R3NLgaWX6Me
Rb7KTNETILpCHM28HmCbX/t7
ENCRYPTED:Ykz96C7V7XwyF9yJaKZxweD4QidBwoiQD0u8ouqRF0Wy3NyCNdZp
HbUxKuwBXVjVZeZchWzLjs3K
ENCRYPTED:xR29tnHSpBrjxCDogSxzaF1kl2w4IMMKm53nSDZegqywn/nThlYWug
VLkz1bO7YZ/iosGrKuEPyf
.....
ENCRYPTED:yNWr3USjXaSILd//V/tDPiljlo8DyHpclMk5AQDxRL3qU+uK8rmaM4P7
D8tDbFaq6o0VR32Niwl
ENCRYPTED:zVPppILX0EXRMHRrGXySCStD5VY31v+I/bqWihdXrMIHyij4uWd3q6n
9FjwDUaWbpA==
END:VEVENT
```


Paldies par uzmanību!



Kirils Solovjovs, IT drošības eksperts, Mg. dat.

kirils.solovjovs@kirils.com

+371 26036916

@KirilsSolovjovs