

# ***OPEN SOURCE informācijas riski uzņēmumos un iestādēs***



Mārtiņš Akermanis  
Toms Atteka



***LAI INFORMĀCIJAS APRITE BŪTU DROŠA, NEPIECIEŠAMS:***

- *Apzināties informācijas noplūdes riskus;*
- *Patstāvīgi pieņemt lēmumu par informācijas ierobežošanu;*
- *Salāgot to ar organizācijas vai iestādes politiku.*

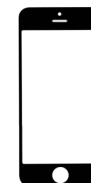
**NEAPSTRĀDĀTI  
DATI**



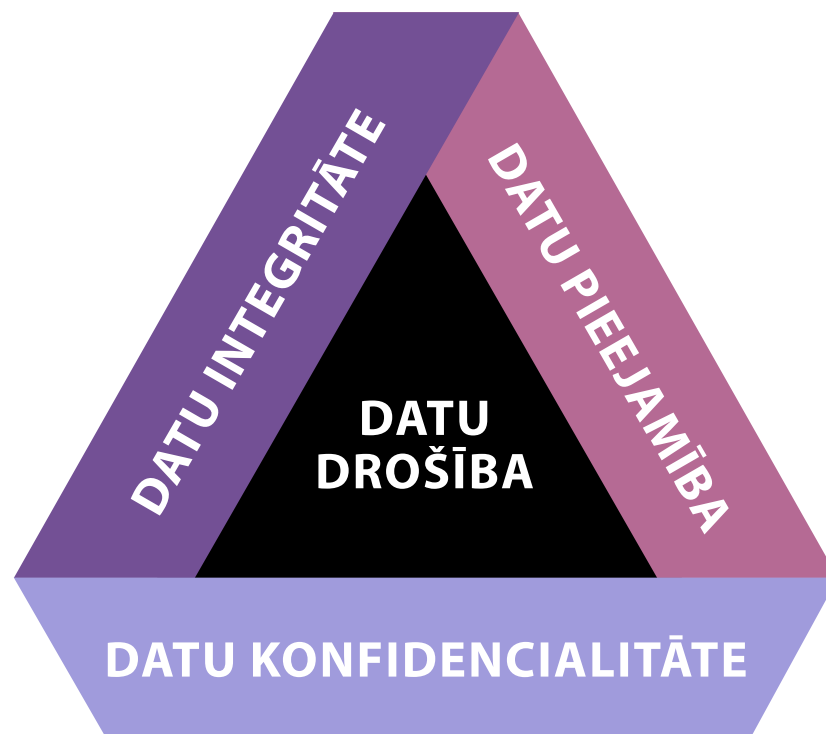
**APSTRĀDĀTI  
UN PIEEJAMI DATI**



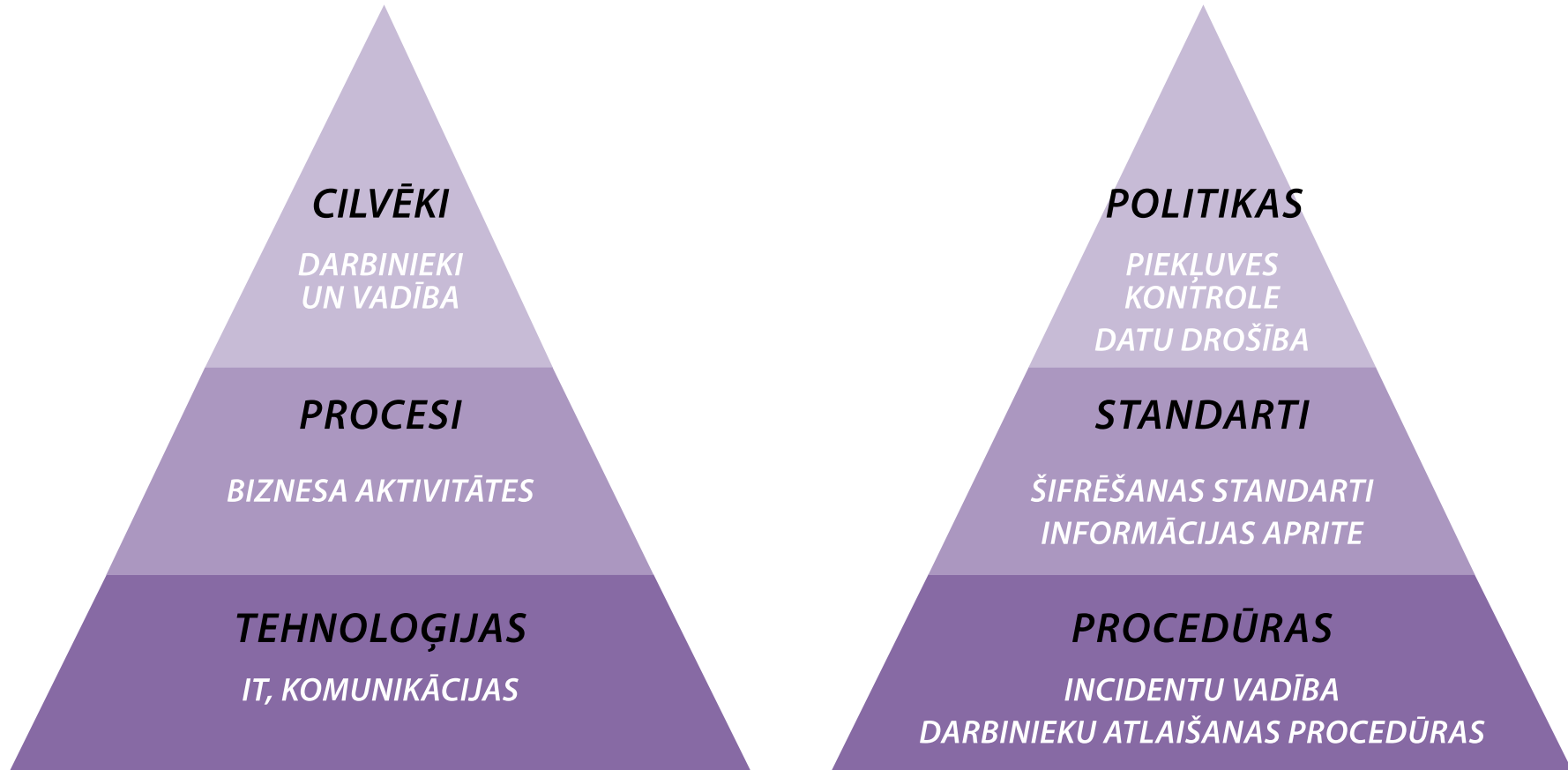
**PERSONISKIE  
UN NEPIEEJAMIE  
DATI**



# ***INFORMĀCIJAS DROŠĪBAS ELEMENTI***



# ***DROŠĪBAS ELEMENTI***



# ***DROŠĪBAS LĪMEŅI***

***FIZISKĀ DROŠĪBA***

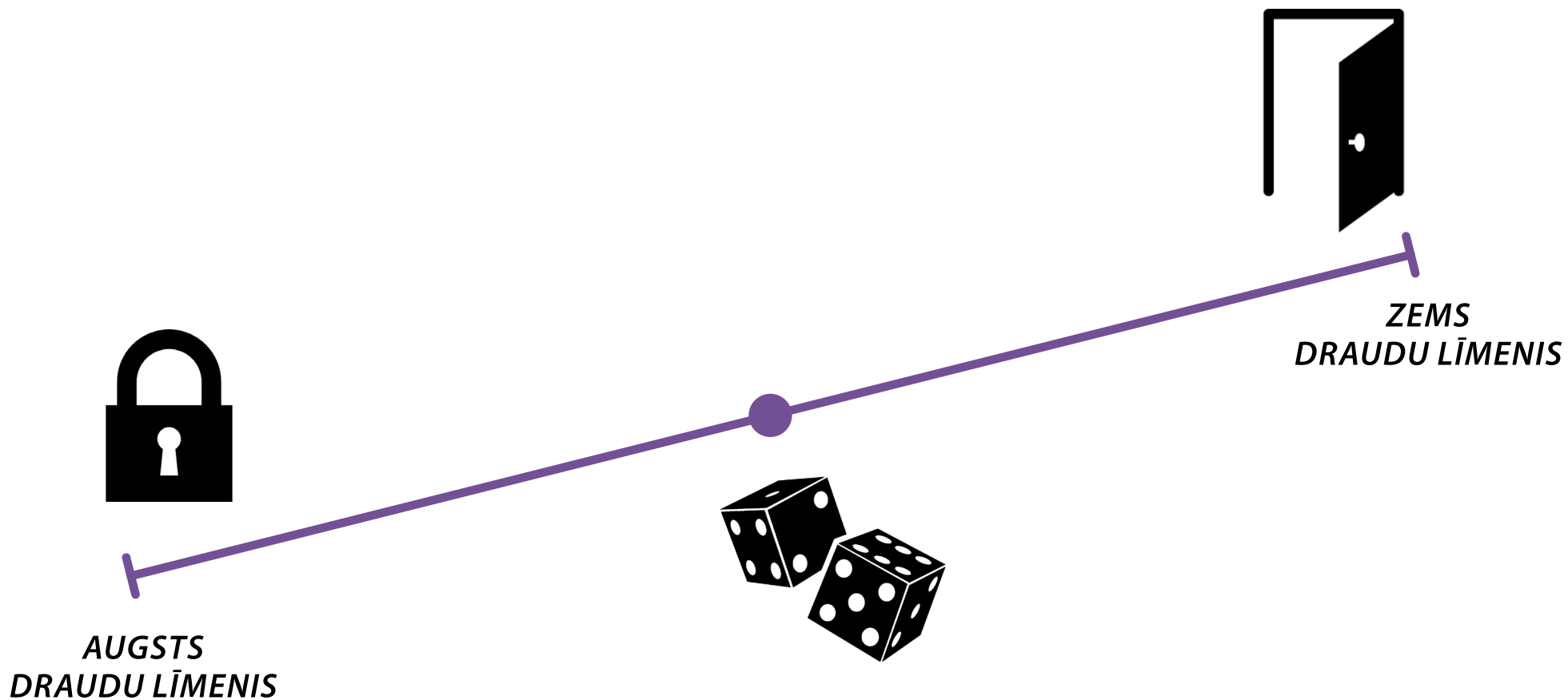
***UZGLABĀŠANAS DROŠĪBA***

***PIEEJAS KONTROLE***

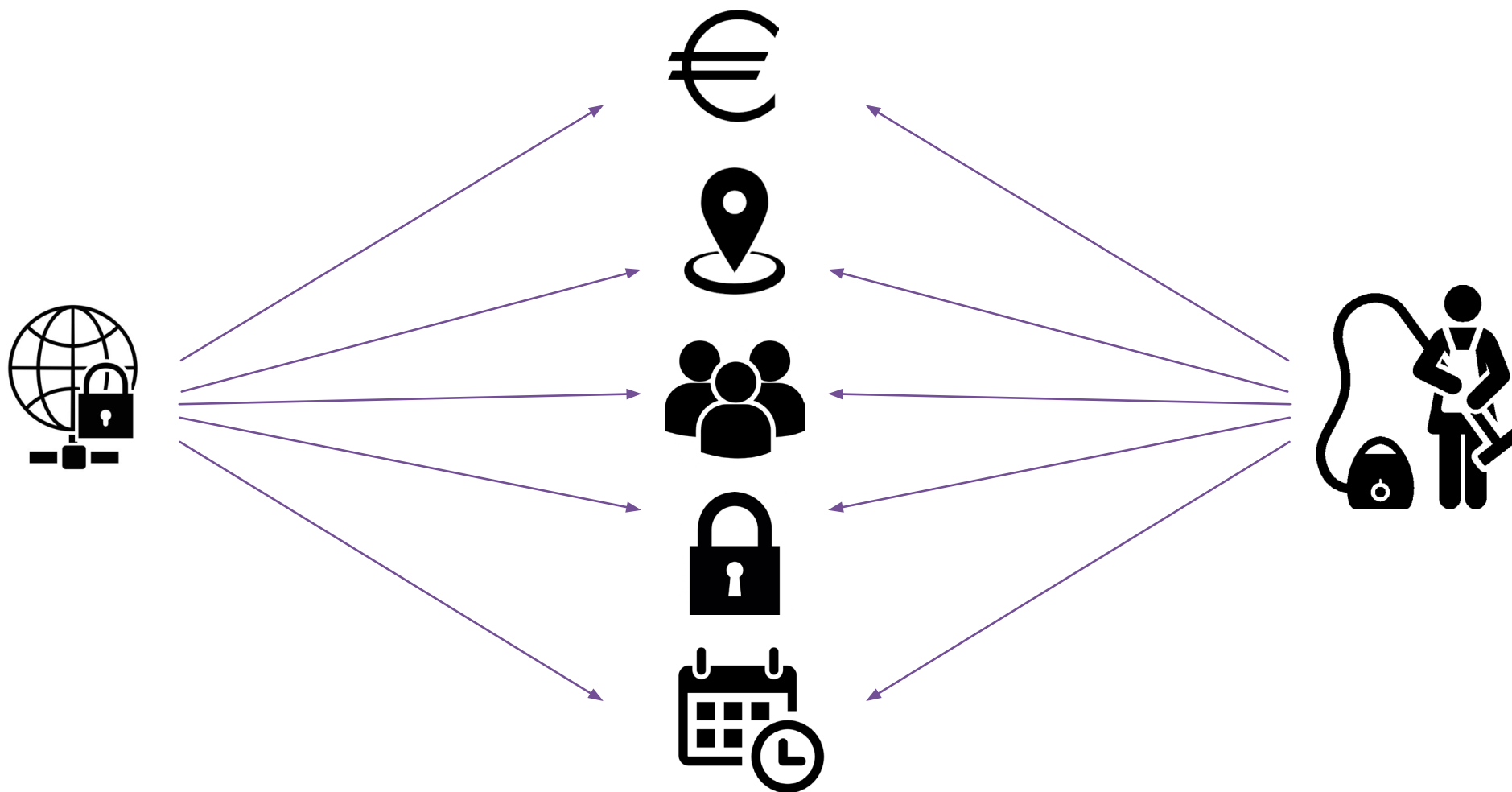
***TĪKLU DROŠĪBA***

***IEKŠĒJĀ DROŠĪBA***

# *DRAUDU NOVĒRTĒŠANA*



# VAI PASTĀV INFORMĀCIJA BEZ VĒRTĪBAS?





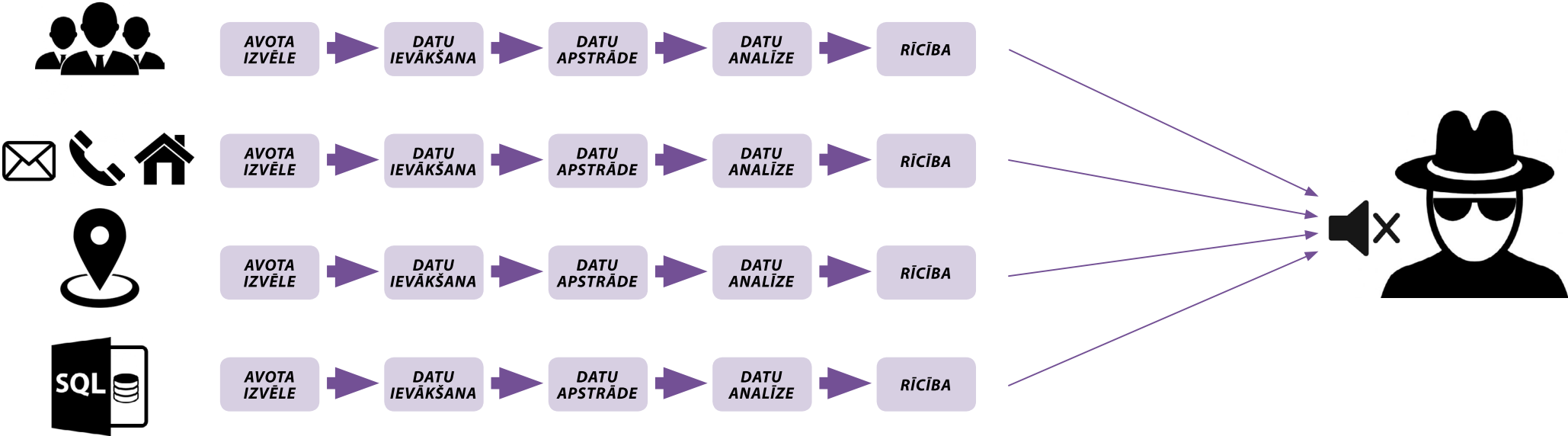
# *UPURA IZVĚLE*



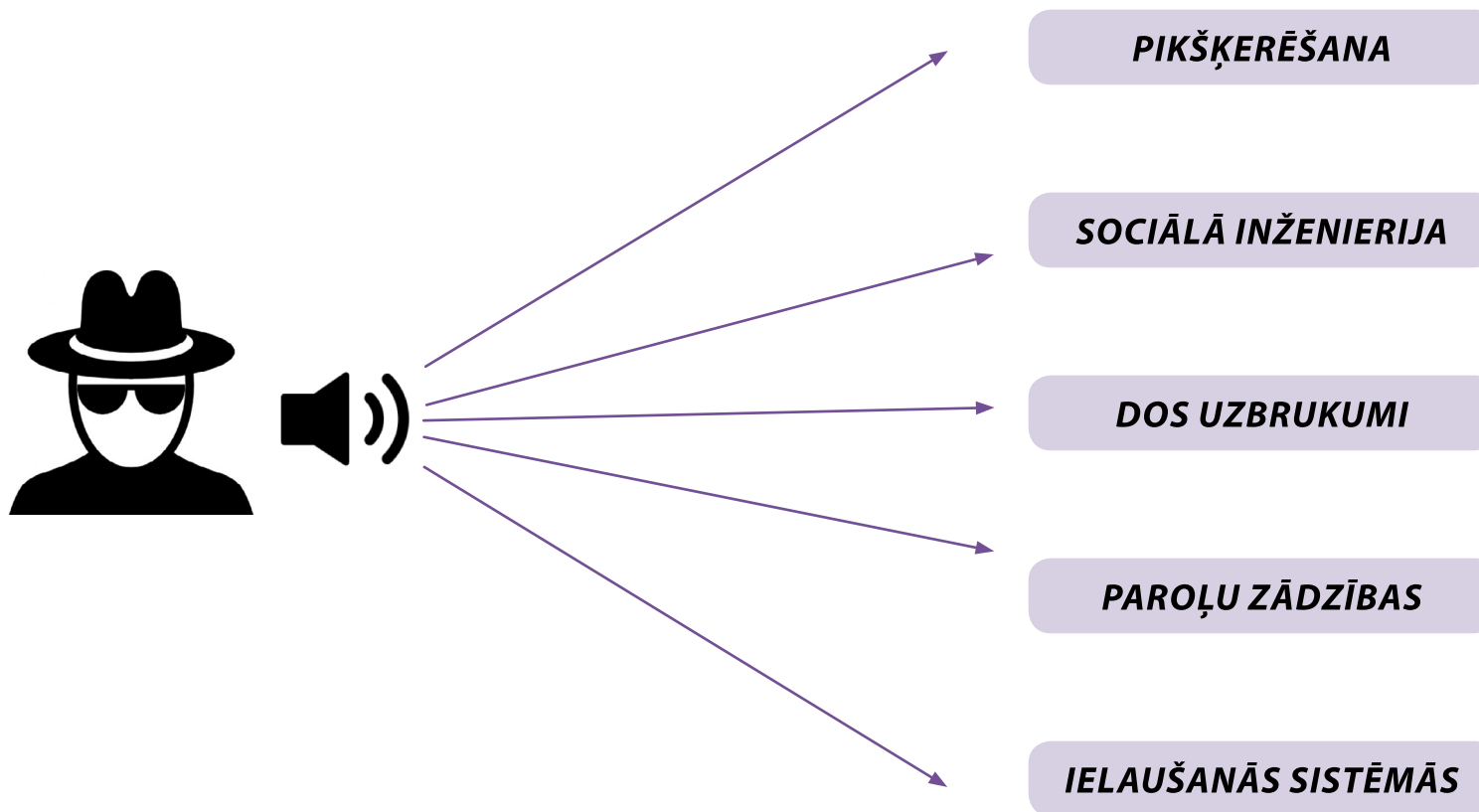
# *UZBRUKUMA FĀZES*



# UZBRUKUMA ANATOMIJA



# UZBRUKUMA ANATOMIJA

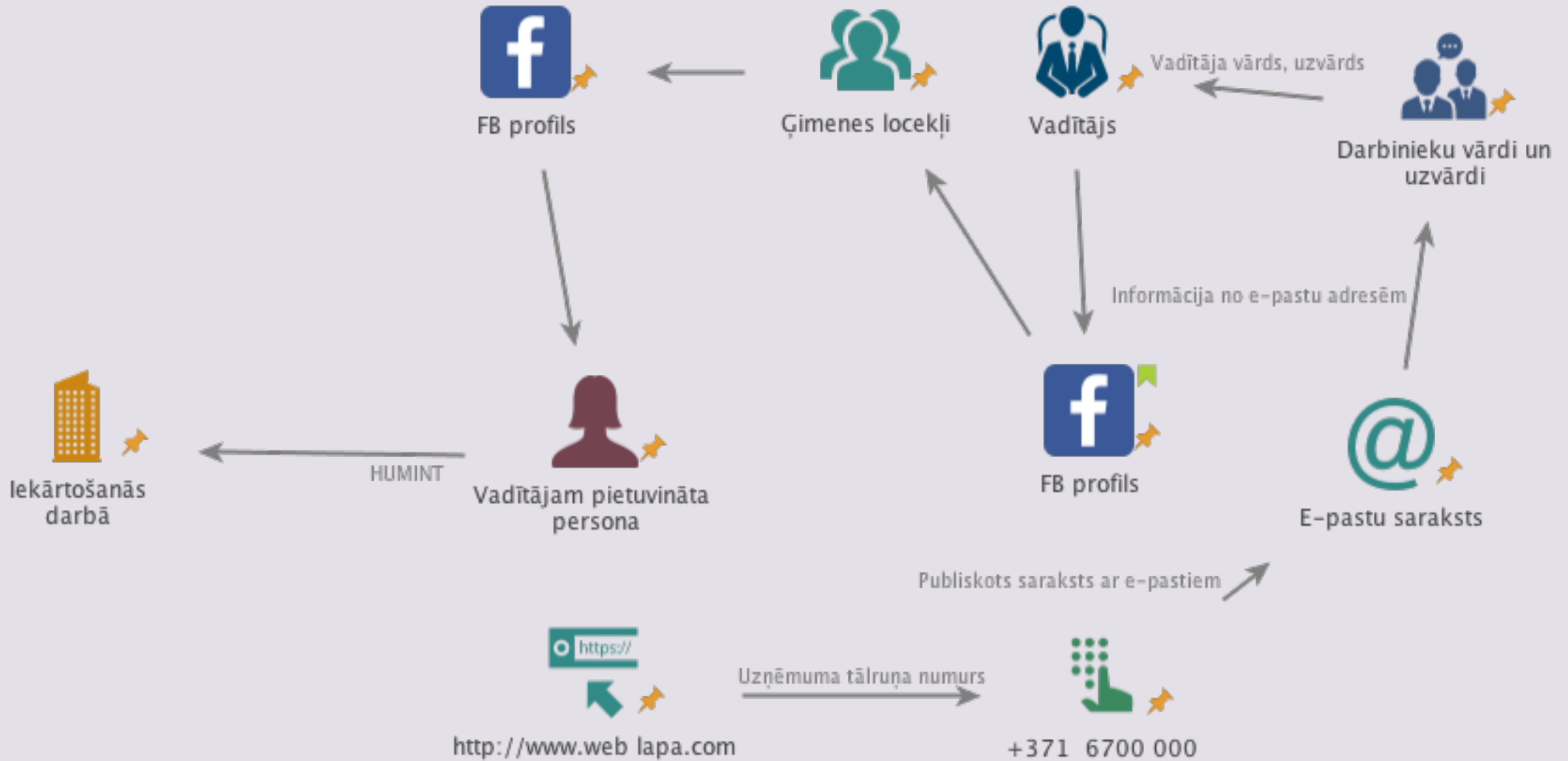


# ***PRAKTISKS PIEMĒRS***

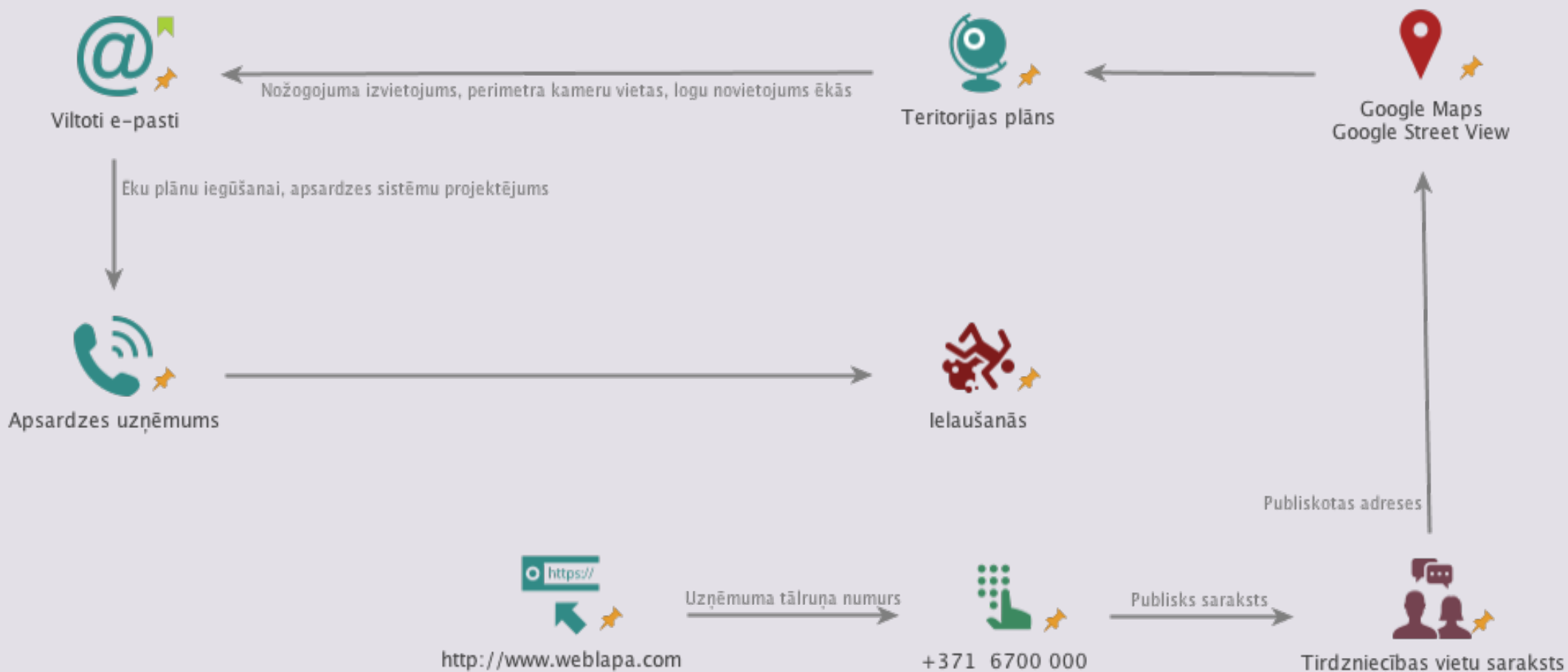
- *Nejaušs uzņēmums – zādzība, krāpšana, izspiešana, ...*
- *Konkurējošs uzņēmums – klientu saraksts, tehnoloģiskie risinājumi, sabotāža, ...*
- *Atriebība – nomelnošana, sabotāža, tiesvedība, ...*

***NEJAUŠS UZŅĒMUMS -  
ZĀDZĪBA AR MĒRĶI  
IZSPIEST NAUDU  
PAR IEKĀRTU ATGŪŠANU***

# VEKTORS 1

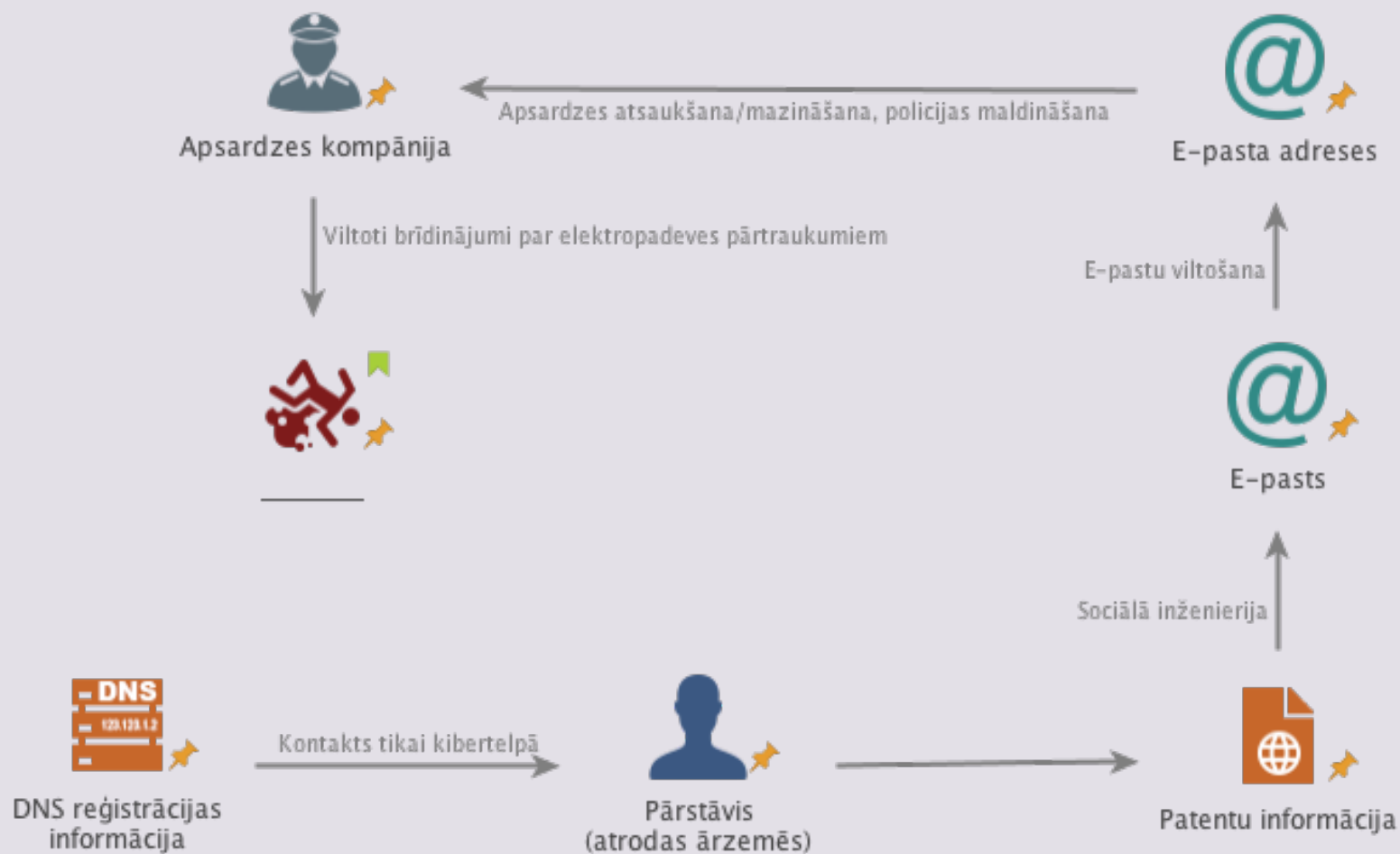


# VEKTORS 2





# VEKTORS 3



# ***RISINĀJUMI:***

## **1. PERSONĪGĀS INFORMĀCIJAS PUBLICĒŠANA**

Izvērtēt, cik daudz informācijas publicēt.

## **2. INFORMĀCIJAS APRITES POLITIKA**

Integrēt to uzņēmuma esošajā kultūrā.

## **3. DROŠĪBAS AUDITS**

Regulāri testēt drošības programmas efektivitāti.

## **4. BRĪDINĀJUMA SISTĒMAS**

Ļauj adekvāti reaģēt uz apdraudējumiem

## **5. PERSONĀLA IZGLĪTOŠANA**

Izmantot reālās dzīves piemērus.

***PALDIES  
PAR UZMANĪBU!***

