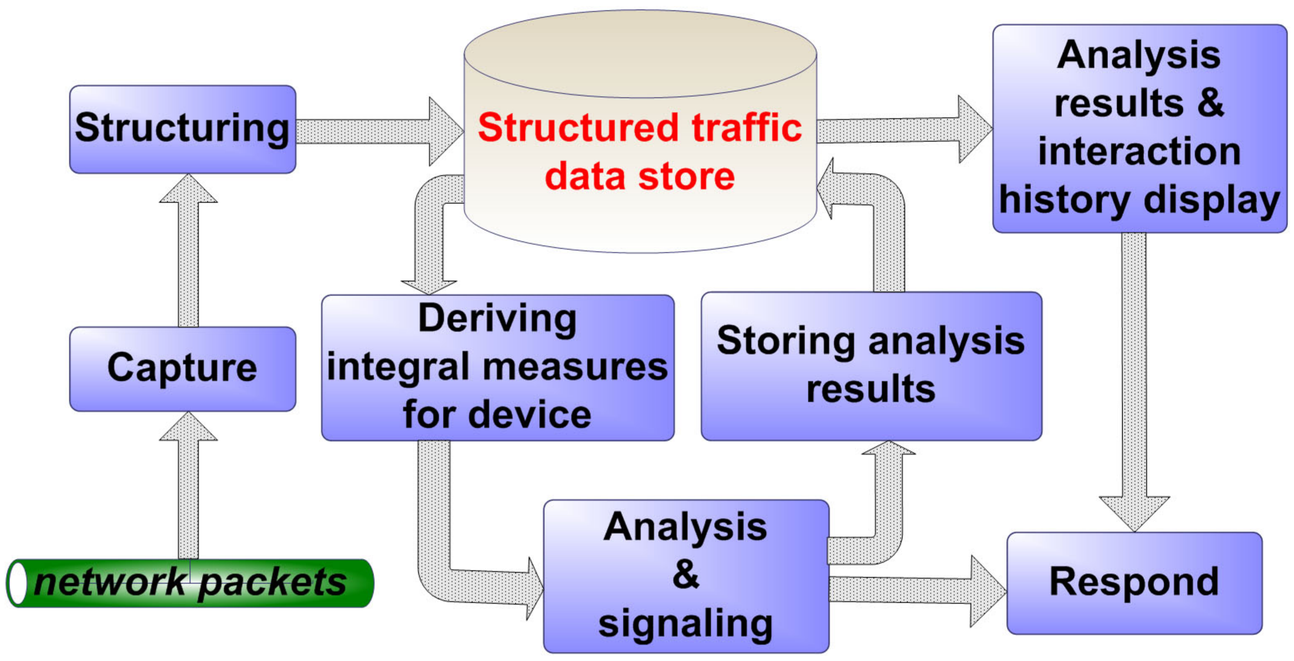
"SECURITY LOCATOR" - Network Monitoring and Anomaly Detection Tool

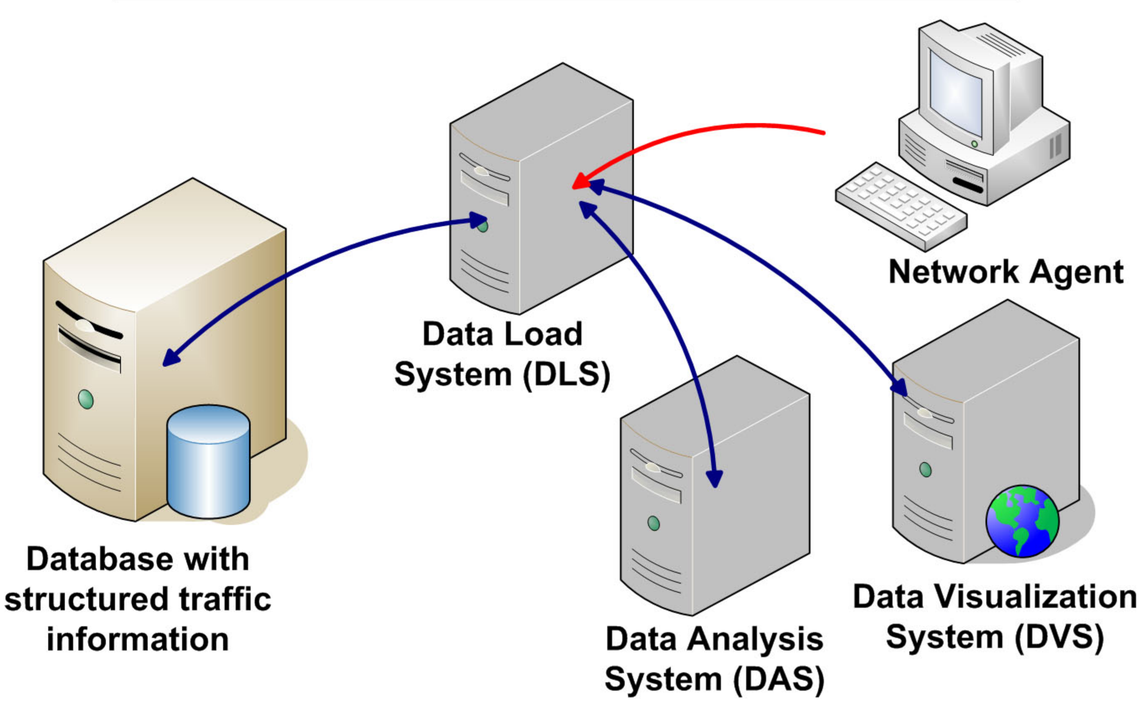
M. Zhdanova, E. Druzhinin
LLC "Laboratory of Network Technologies", Moscow, Russia
http://www.eyeadmin.com

The research is focused on developing computer-based system "SECURITY LOCATOR", that provides continuous monitoring of network devices functioning states and automated detection of network anomalies. An anomaly is understood as any deviation from the normal behavior pattern, that describe the standard functioning process of a network device. The main data source considered is structured information on network traffic. This work is financed by Foundation for Assistance to Small Innovative Enterprises (FASIE).

TRAFFIC PROCESSING SCHEME



"LOCATOR" COMPONENTS



ANOMALY DETECTION

1. Network traffic structuring

TIME_STEP	KEY	CNT1	CNT2	...	CNTm	N/A

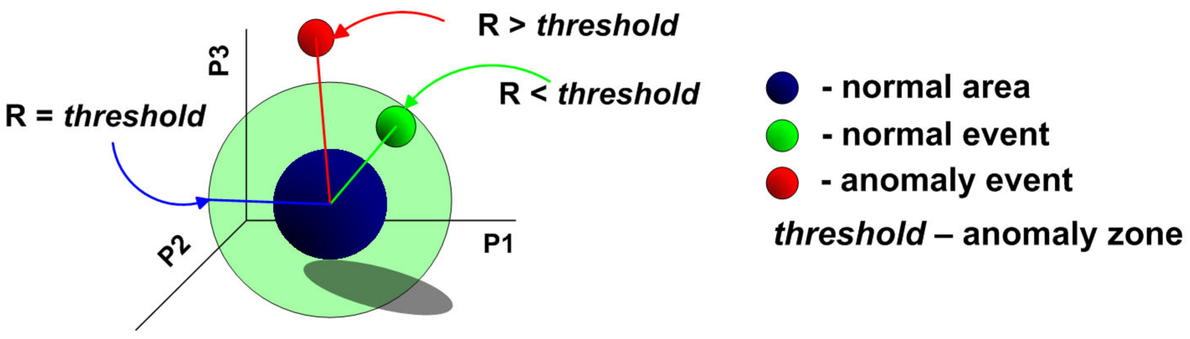
- event

TIME_STEP – structuring step (fixed period of time), determines granularity of data representation

CNTi – simple / conditional counter on packet header field, grouped by KEY (for example, packets number, traffic volume, etc.)

KEYs used: *{IP_source, IP_dest, Port_source, Port_dest}; {IP_source, IP_dest,Type, Code}; {IP}* **- device**; *{Port}* **- service**

2. Normal behavior pattern creation



3. Detection & classification

Currently the research is carried out in two directions: statistical approach and immune network theory

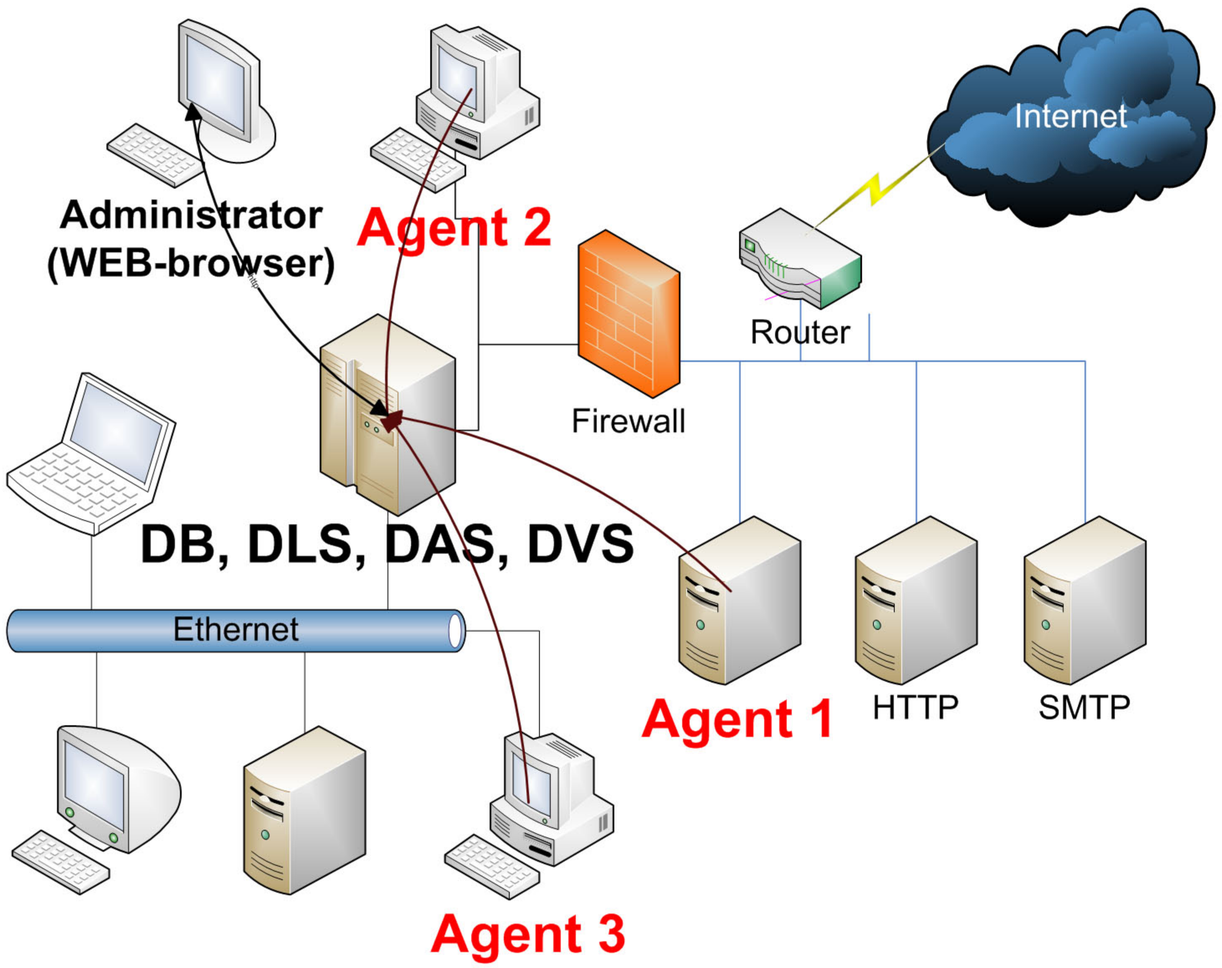
N – set of normal events, R < *threshold*
A – set of anomaly events, R > *threshold;*
A = A1+A2+…+An (Ai – specified intrusion)
D – detector set, rules that specify abnormal activity

event $\in$ **Ai if** $\exists$ **Di: R(e*vent*, Di)< thresholdDi**

Detector	Param1	Param2	...	Paramk	Intrusion

Parami - integral measure; packet header field value; calculated value

INTEGRATION SCHEME



ANALYSIS RESULTS