2014 FIRST Symposium

October 14-16, 2014

Tbilisi

CERT-UA practice in ensuring the country's cybersecurity

Vizniak Roman
vrb@cert.gov.ua

CERT-UA

FIRST™
Improving Security Together

What will be discussed?

- CERT-UA. Who we are and what we do?
- Incident Response. The main goal – to prevent the incident.
- Problem of coordination. Our solutions.

Who fight against cyber threats of GOV organizations in Ukraine?

Security Service of Ukraine

LE

Department of Counterintelligence Protection of State's Interests in the Sphere of Information Security

State Service of Special Communication and Information protection of Ukraine

State Center of Protection of Information and Telecommunication Systems

Ministry of Internal Affairs of Ukraine

LE

Department on Combating Cybercrimes

State Center is responsible for:

- **N**ational **S**ystem of **C**onfidential **C**ommunication
- **S**ystem of **P**rotected **I**nternet **A**ccess
- **C**omputer **E**mergency **R**esponse **T**eam of Ukraine (**CERT-UA**)

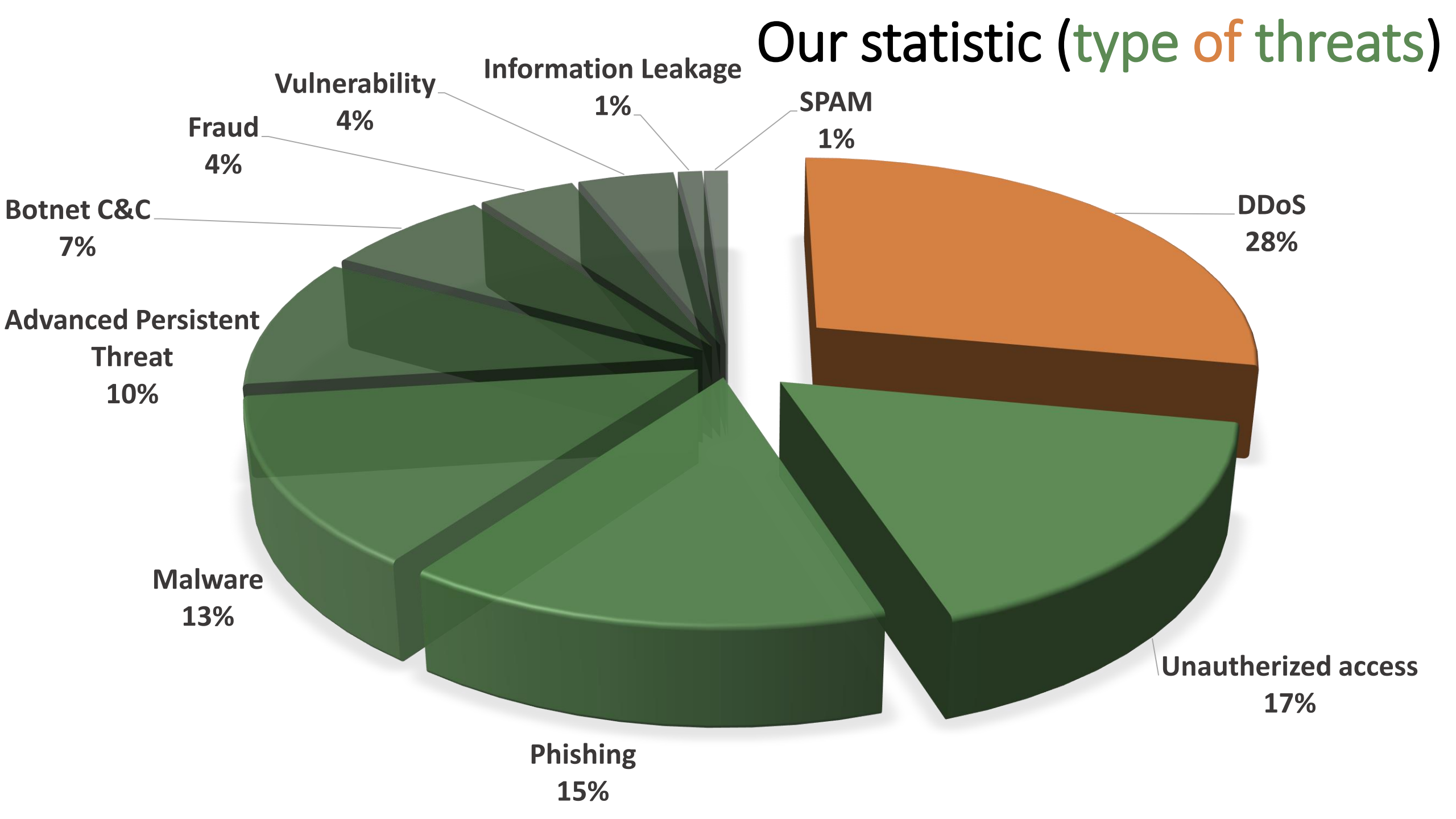
CERT-UA. Our mission

- to protect government information resources
- to provide security of Ukrainian segment of the Internet

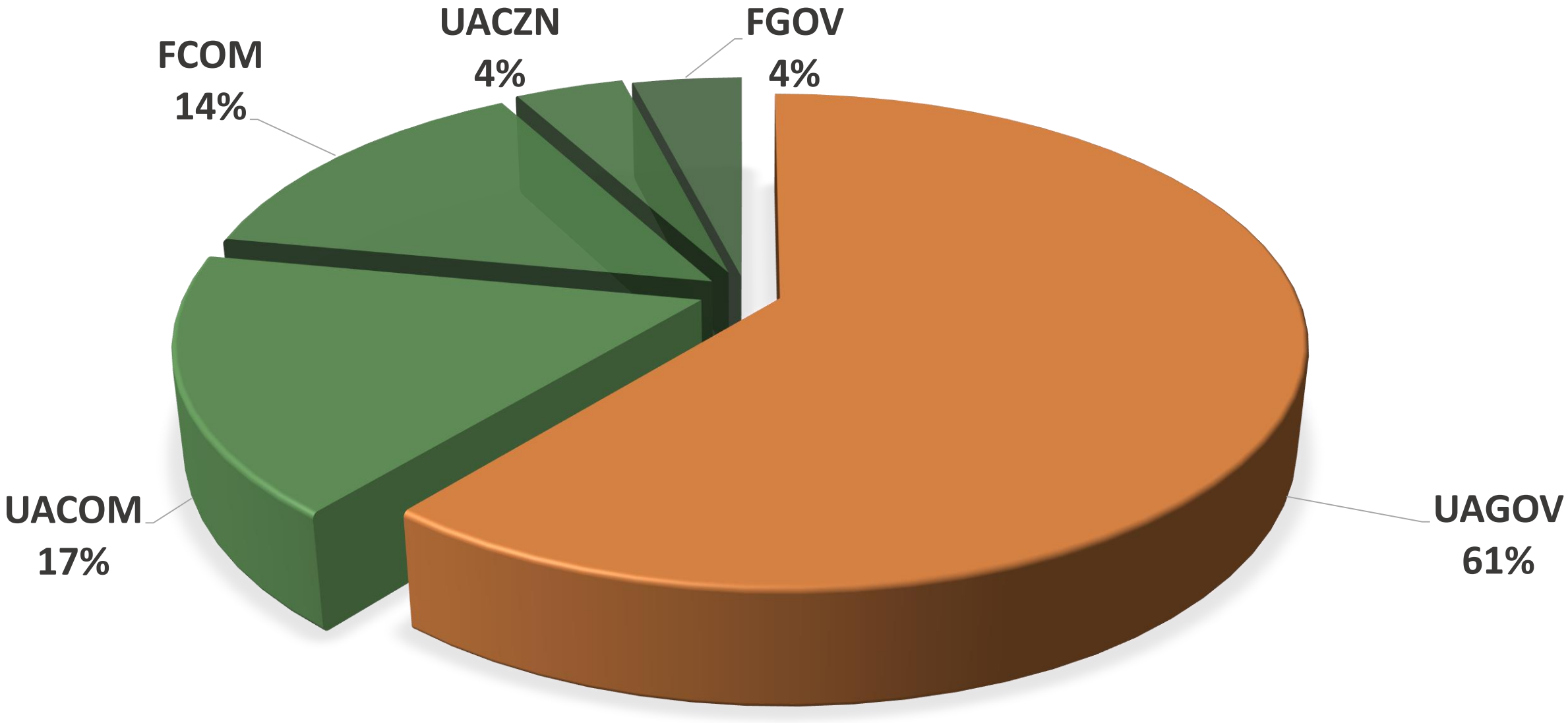
CERT-UA works in 5 sectors:

UAGOV
UACTZ
UACOM
FGOV
FCOM

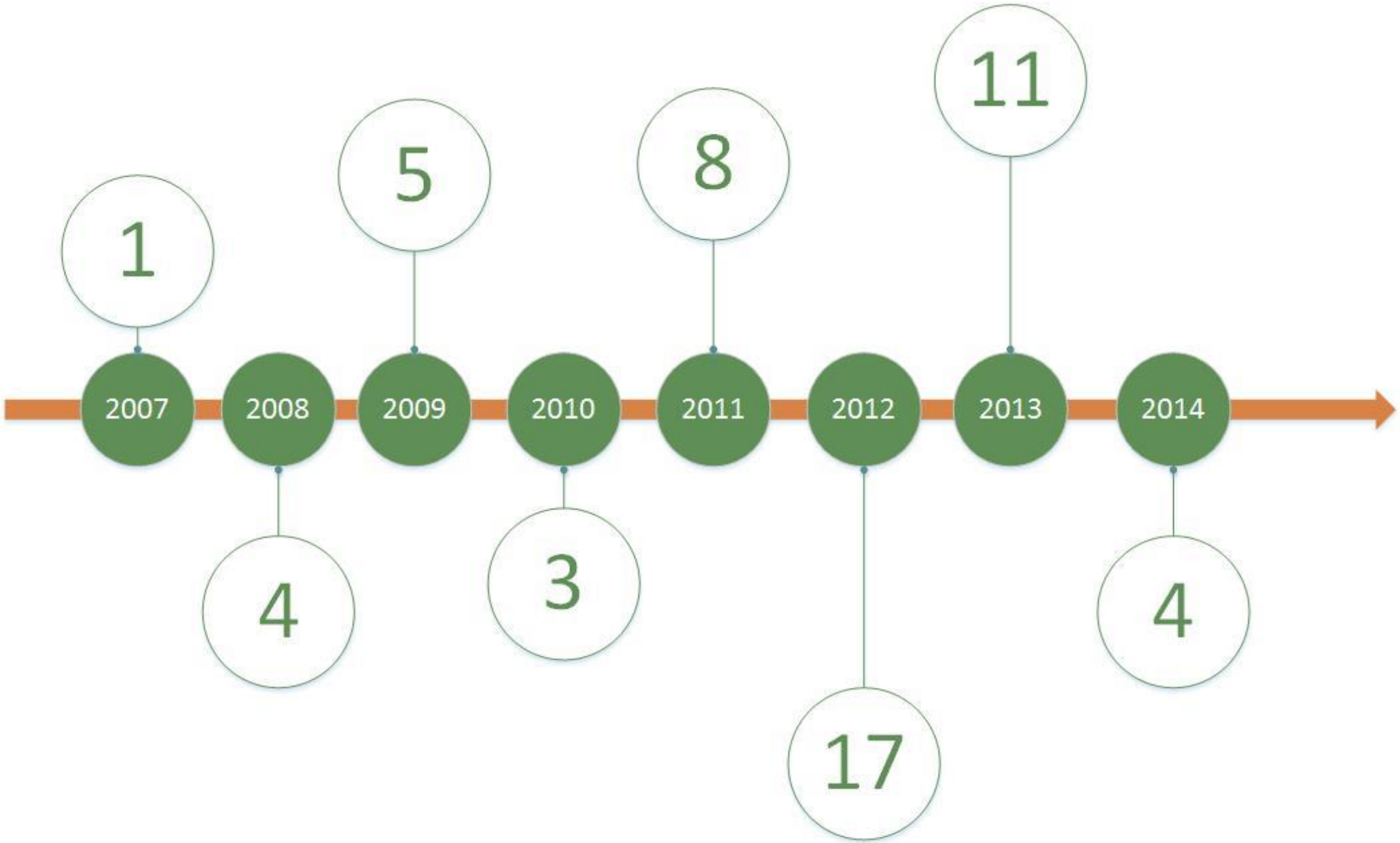
Our statistic (type of threats)



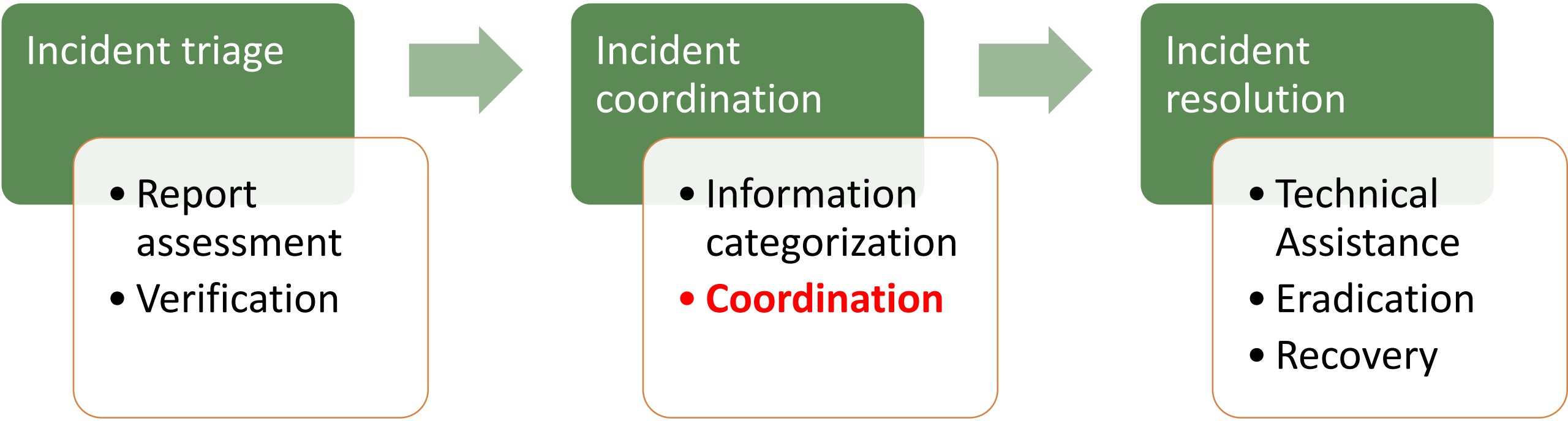
Our statistic (attacked zones)



Our statistic (information security audits)



Incident Response. Main steps (RFC 2350)



Coordination problem

We have to:

- try to get some basic info about incident from alternative(trusted) sources
- have much contact information of our ISPs, banks and other organizations (not GOV only)
- try to decentralize monitoring of theirs security status.

Our solutions

- Threat Monitoring System (passive mode)
- IP Guard (interactive system which called to create some kind of dialog between CERT-UA and subjects of information security)

Threat Monitoring System (passive mode)

DB contains info about IPs of compromised devices in UA Internet

Visualization works for UA GOV entities

GOV IPs gathering process:

- **3 official** inquiries on behalf of Prime-Minister of Ukraine
- **5 mount** for answers and data processing

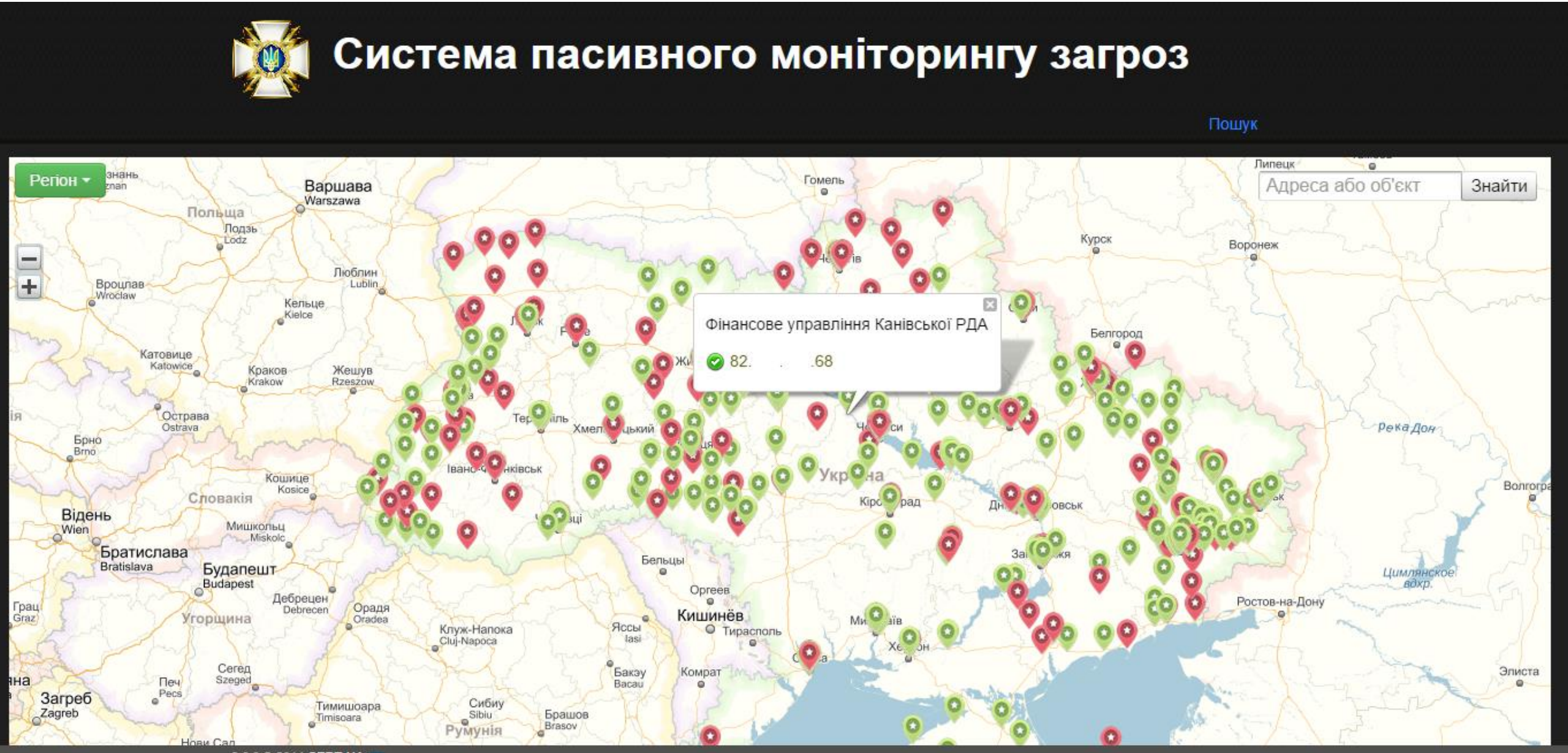
Finally:

Number of	Quantity
Organizations	1523
IP-addresses	3045
Compromised Org	605
Compromised IPs	586

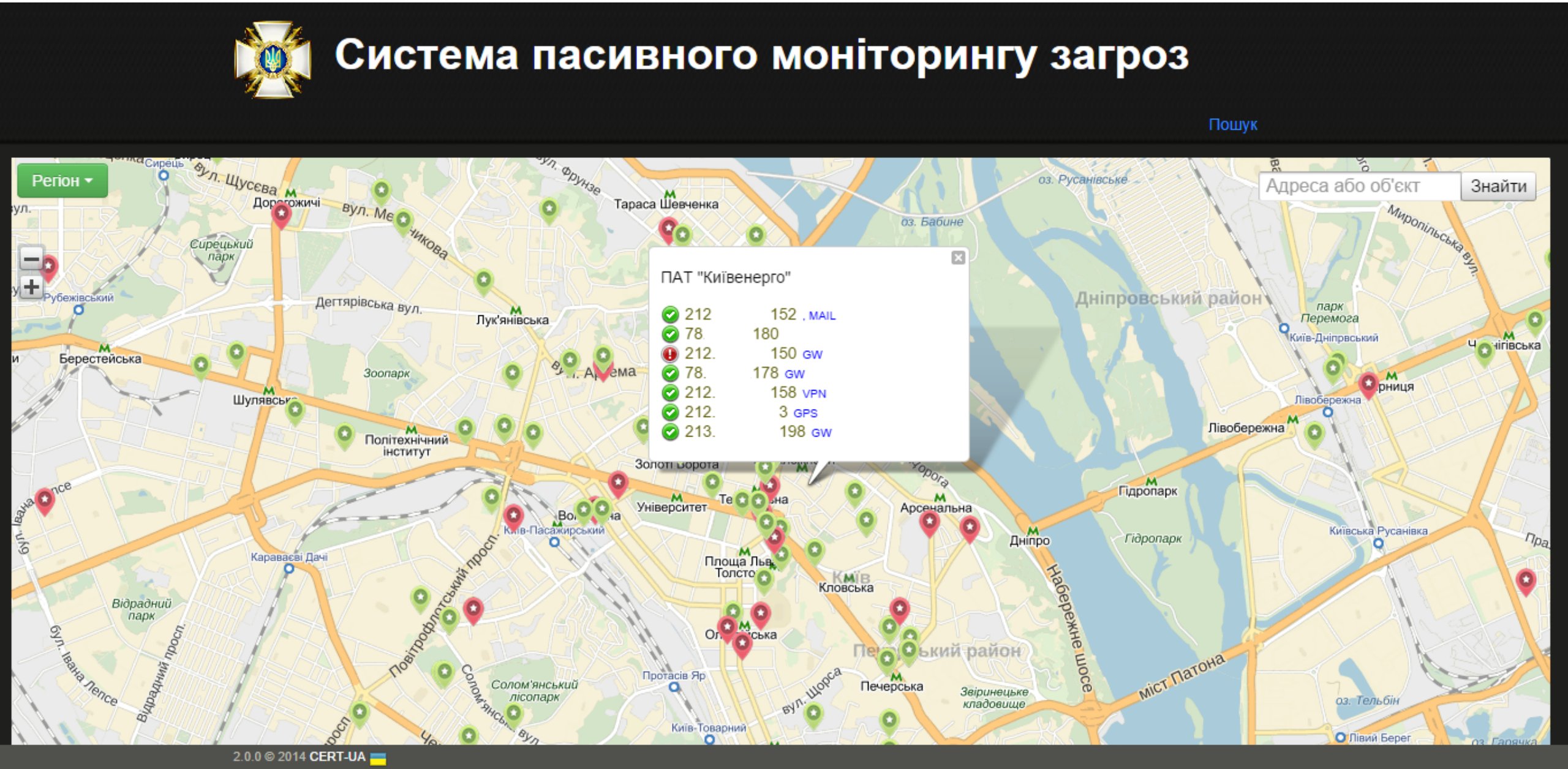
40%

ARE COMPROMISED

Threat Monitoring System (passive mode)



Threat Monitoring System (passive mode)



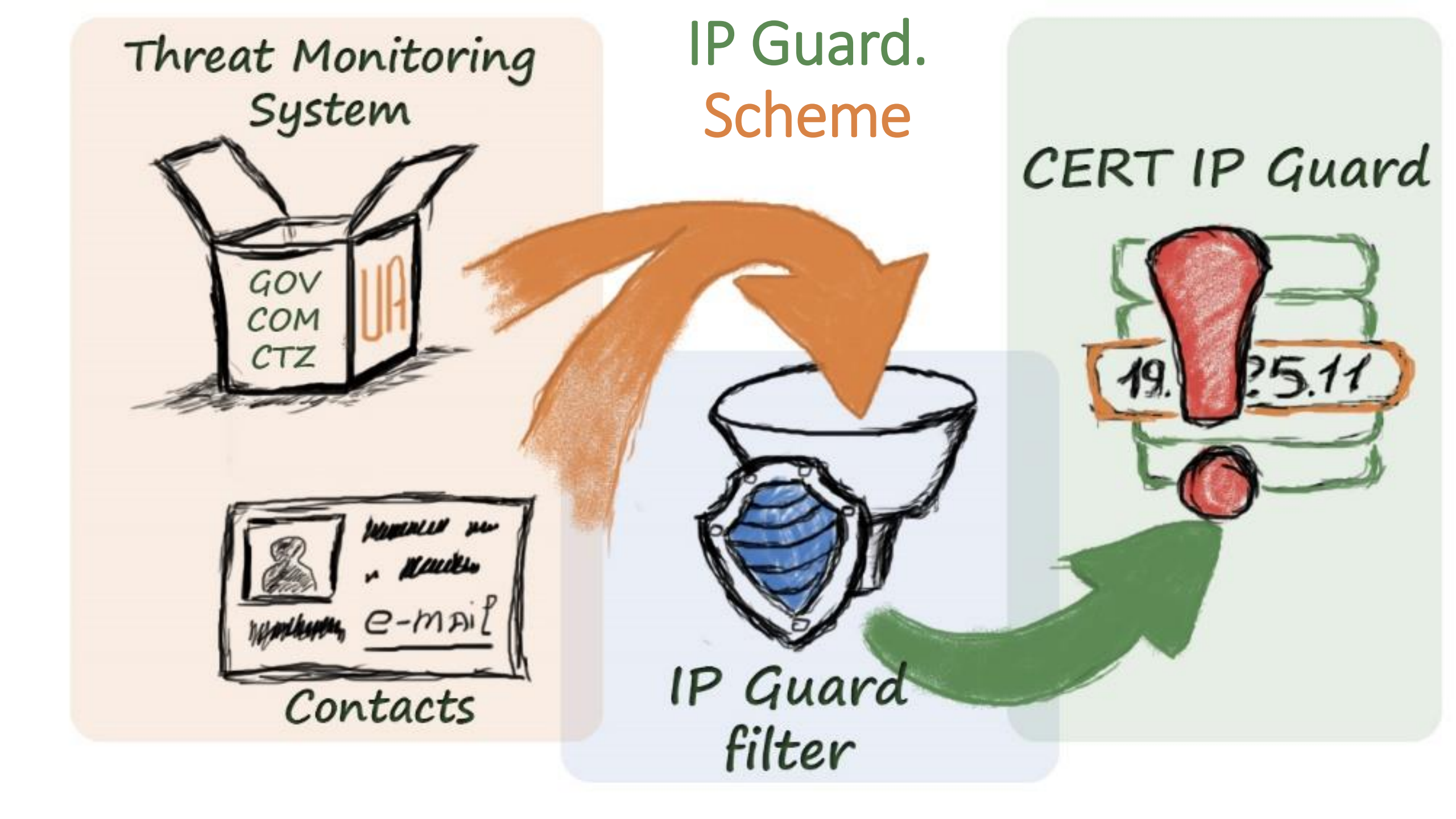
IP Guard. What we have…

Diagram of the system include:

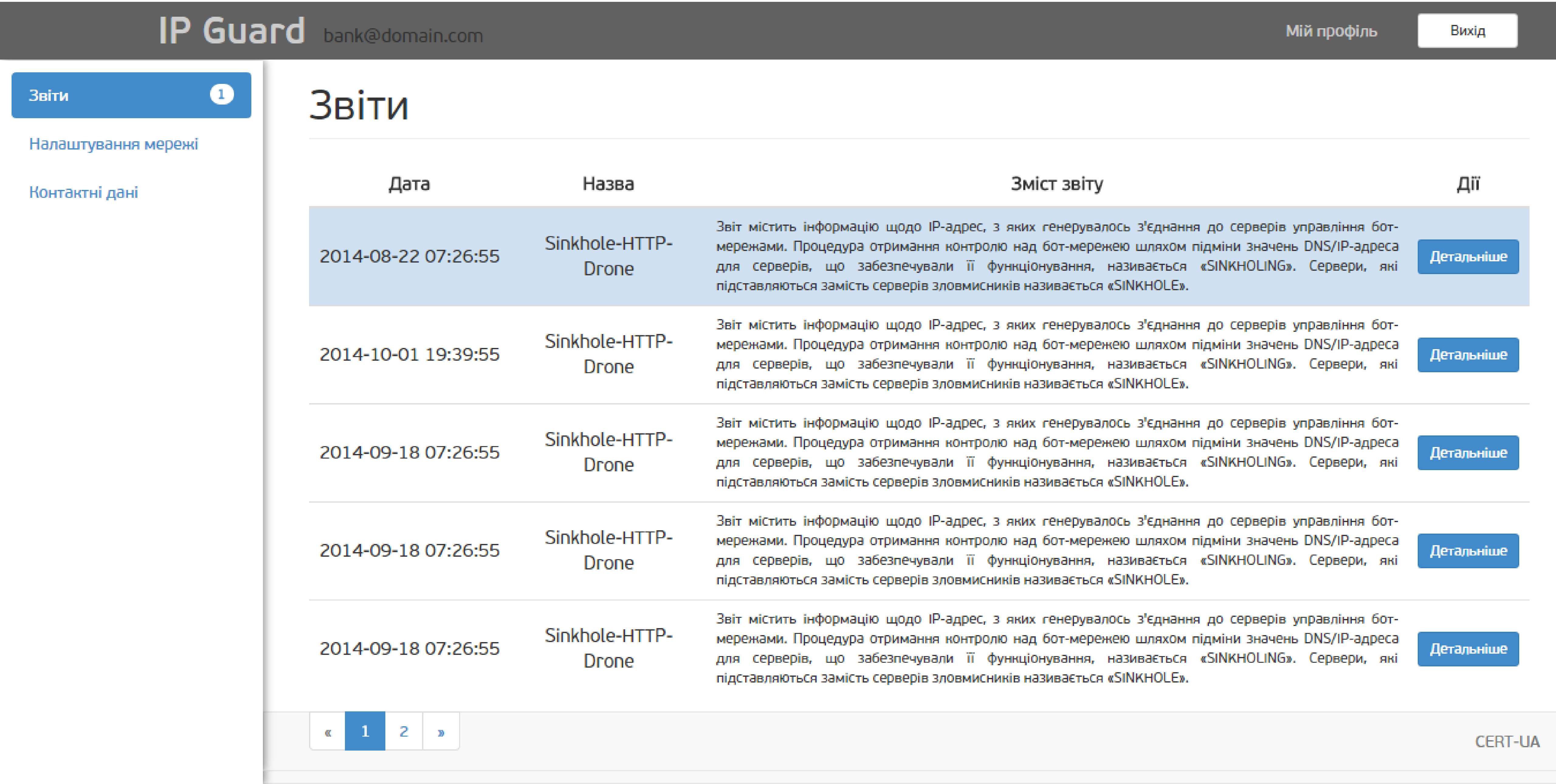
- Threat Monitoring System (include all UA sectors – UAGOV, UACOM, UACTZ)
- Information about user of IP Guard (basic info and contacts, which certainly will be checked by CERT-UA members)
- Information about users IPs or some range of IPs, which he interested in.

As a result.. you'll see **what we know** about requesting IPs

IP Guard. Scheme



IP Guard. Looks like this



What we are trying to achieve. Global

- **Raise coordination level**
- Raise awareness level in information security of each citizen of Ukraine.

What we are trying to achieve. Developing

- Add some visualization to IP Guard (some statistic)
- Bring some mobility to IP Guard
- Try to make our Internet safer

THANKS A LOT FOR YOUR ATTENTION

CERT-UA

Roman Vizniak
vrb@cert.gov.ua