Команда команда реагування на комп’ютерні надзвичайні події України

CERT-UA

Соколов Іван
sio@cert.gov.ua
cert.gov.ua
01/10/2015

Короткий зміст

- Хто забезпечує кібербезпеку на Україні?
- Приклад загрози. Цільова атака на мережу з подоланням повітряного бар'єру
- Рішення від CERT-UA #1: IPGuard FEEDs
- Рішення від CERT-UA's #2: IPGuard AMS 1.0

Національна система кібербезпеки

Рада національної безпеки і оборони України

Держспецзвязку

СБ України

МВС України

Міноборони України

Генеральний штаб ЗС України

СЗР України

Законодавча база (не вся)

- Закон України «Про Державну службу спеціального зв'язку та
- Закон України «Про інформацію»
- Закон України «Про захист інформації у інформаційно-телеком
- Закон України «Про захист персональних даних»
- Закон України «Про електронний цифровий підпис»

Under develop

- Проект Стратегії забезпечення кібербезпеки України (на по
- Проект Закону України «Про основні засади забезпечення к

Державна служба спеціального зв'язку та захисту інформ

Деякі принципи: *

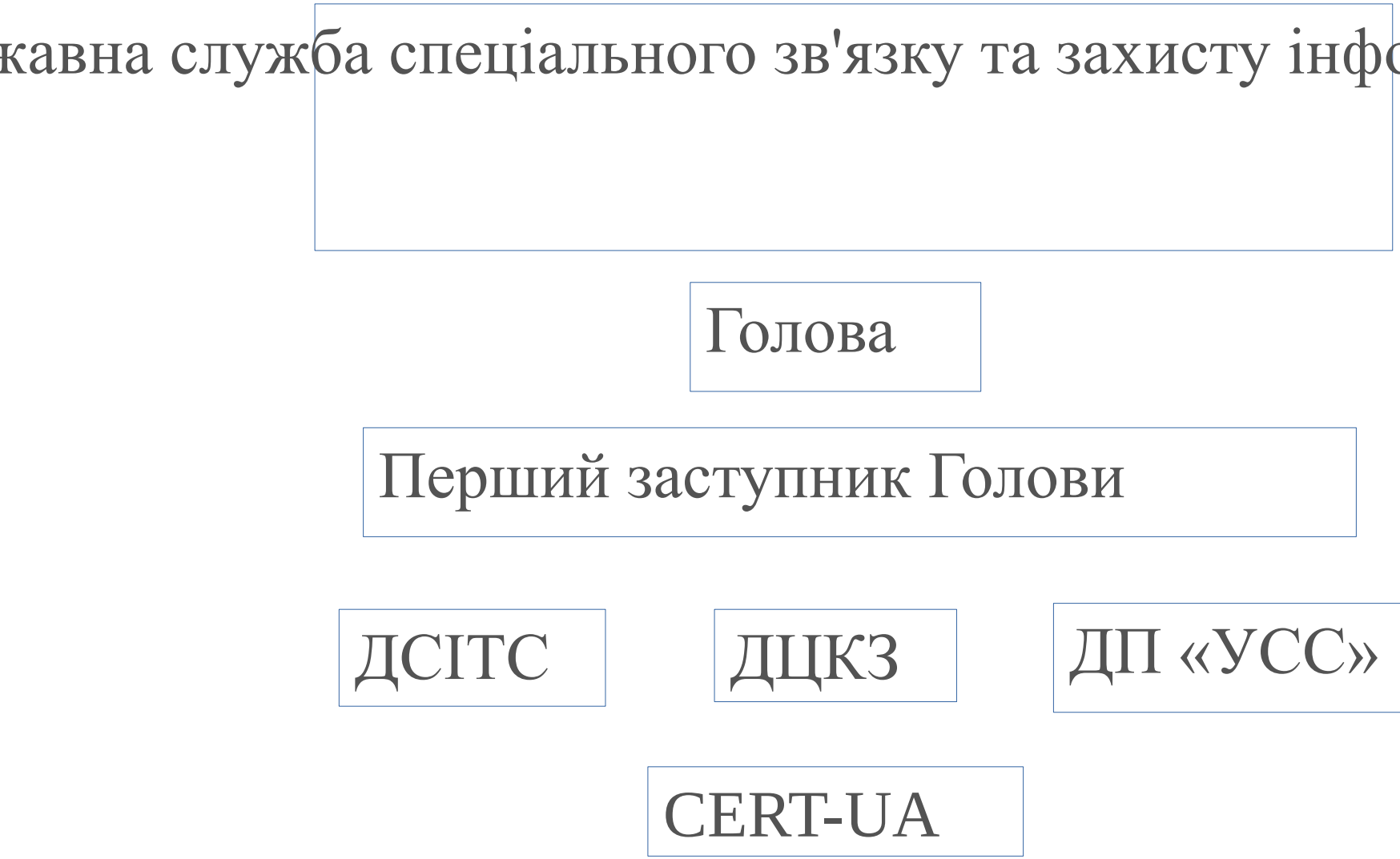
.Формує та реалізує публічні політики для захисту державних інформаі

.Координує державні органи, місцеві органи, військові формування створе

.Забезпечує функціонування Computer Emergency Response Team of Ukrain

** (Закон України "Про Державну службу спеціального зв'язку та захисту інформації України" 23 лютого 2006 № 3475-IV (у*

Структура Держспецзв'язку



Державний центр кіберзахисту та протидії кіберзагрозам

Державний центр — підрозділ Державної служби.

Його відповідальність:

- НСКЗ
- ЄТД
- CERT-UA

CERT-UA

дрозділ у складі Державного центру кіберзахисту та протидії

Ретроспектива CERT-UA:

- 2009 — акредитовано у FIRST
- 2012 — член ITU-IMPACT
- 2013 — член APWG
  — взято участь у DBIR 2014
- 2014 — член проекту The Honeynet
  — авторизовано для використання CERT-UA

Огляд загроз

У 2014 році

Направлені цільові атаки — 26 (більшість — miniduke, Ti

Розподілені атаки на відмову в обслуговуванні — 50 (біл

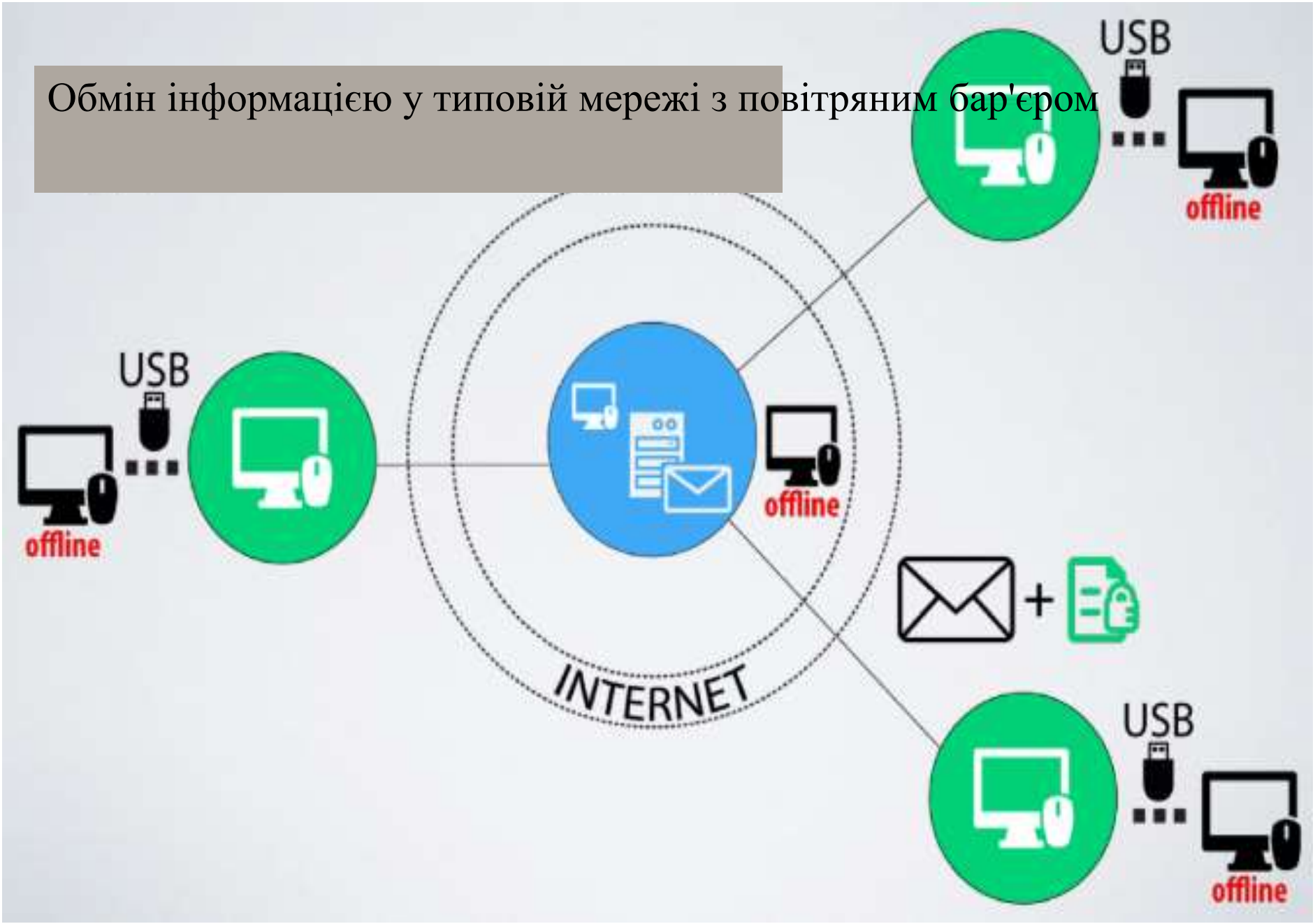
У 2015 році (протягом травня)

Направлені цільові атаки — 5

Розподілені атаки на відмову в обслуговуванні — 6

Цільові атаки

Обмін інформацією у типовій мережі з повітряним бар'єром



Цільова атака

Чи може хтось подолати це?

Як передавати безпечно?

1. створити документ
2. зашифрувати документ
3. записати зашифрований документ на US
4. Перенести зашифрований документ на П
5. Надіслати поштове повідомлення з заши

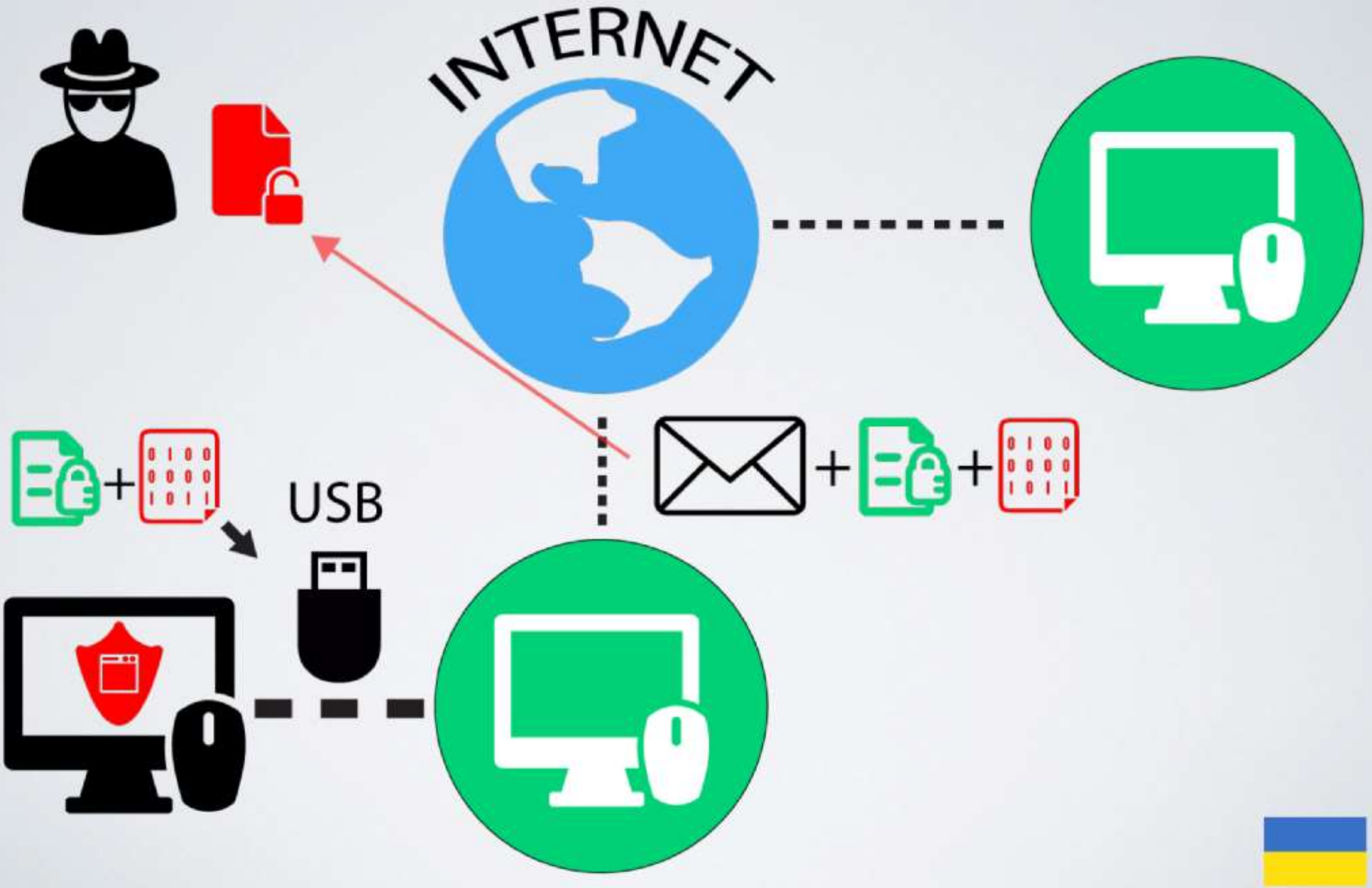
Цільові атаки

прометувати програмне забезпечення, яке використовується для ш

Але як це робиться?

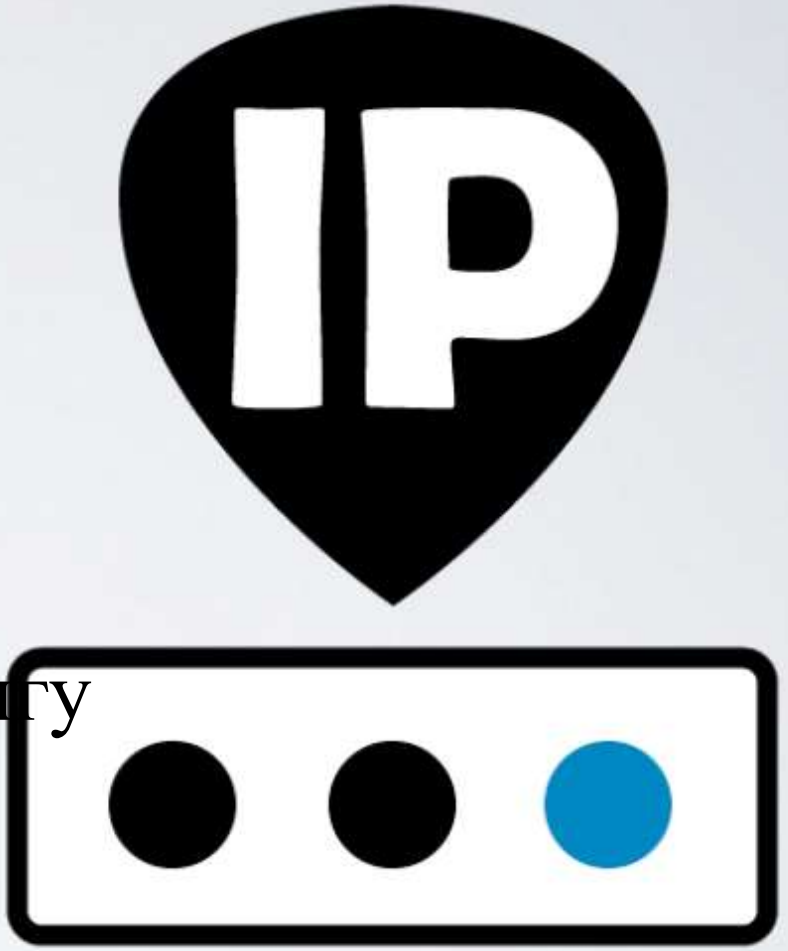
1. Отримується копія програмного забезпечення. Шукається вра
2. Розроблюється експлойт.
3. Компрометується звичайний електронний поштовий акаунт.
4. Компрометується електронна поштова скринька адміністрато

Схема цільової атаки



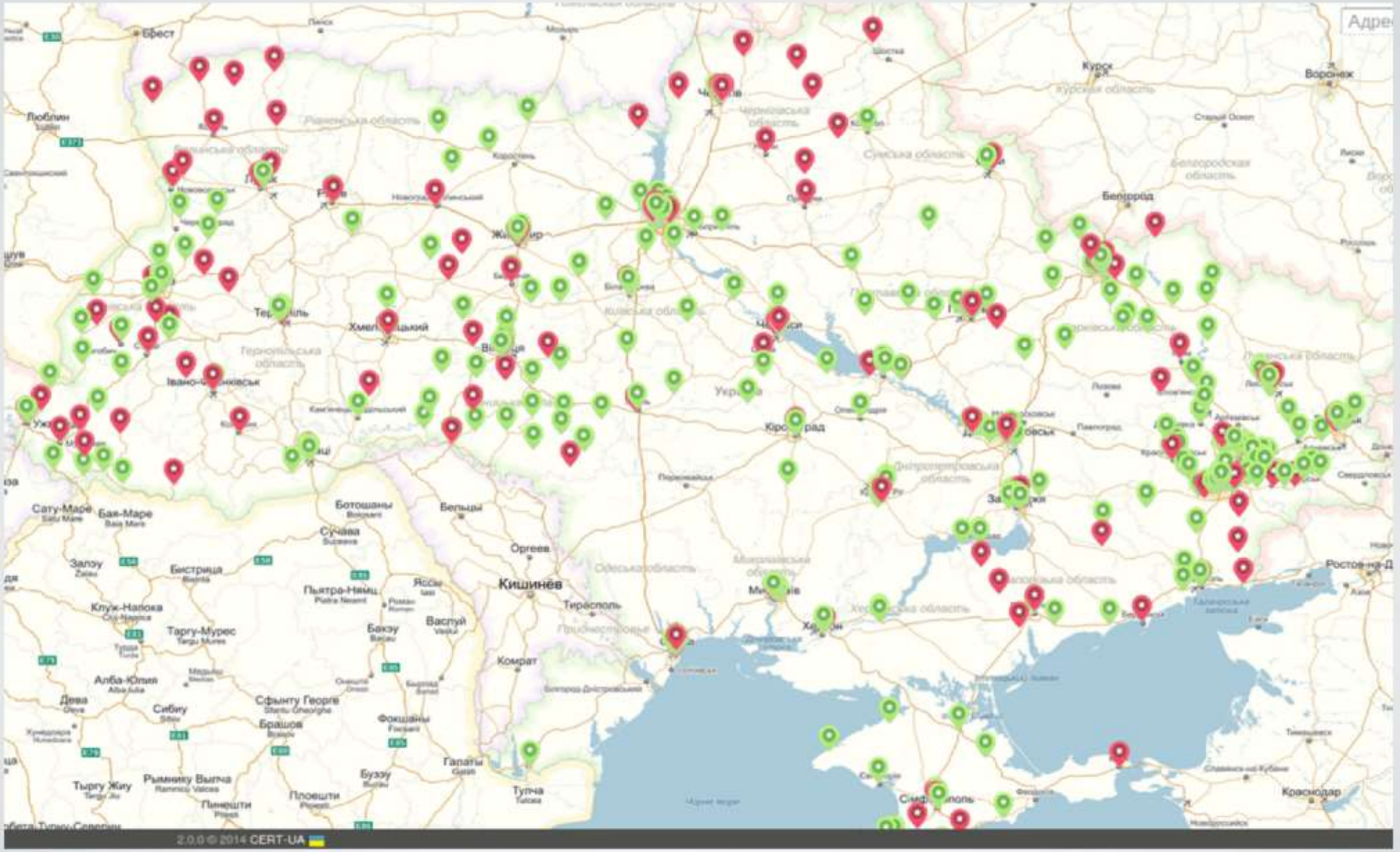
IPGUARD FEEDS

Пасивна система моніторингу

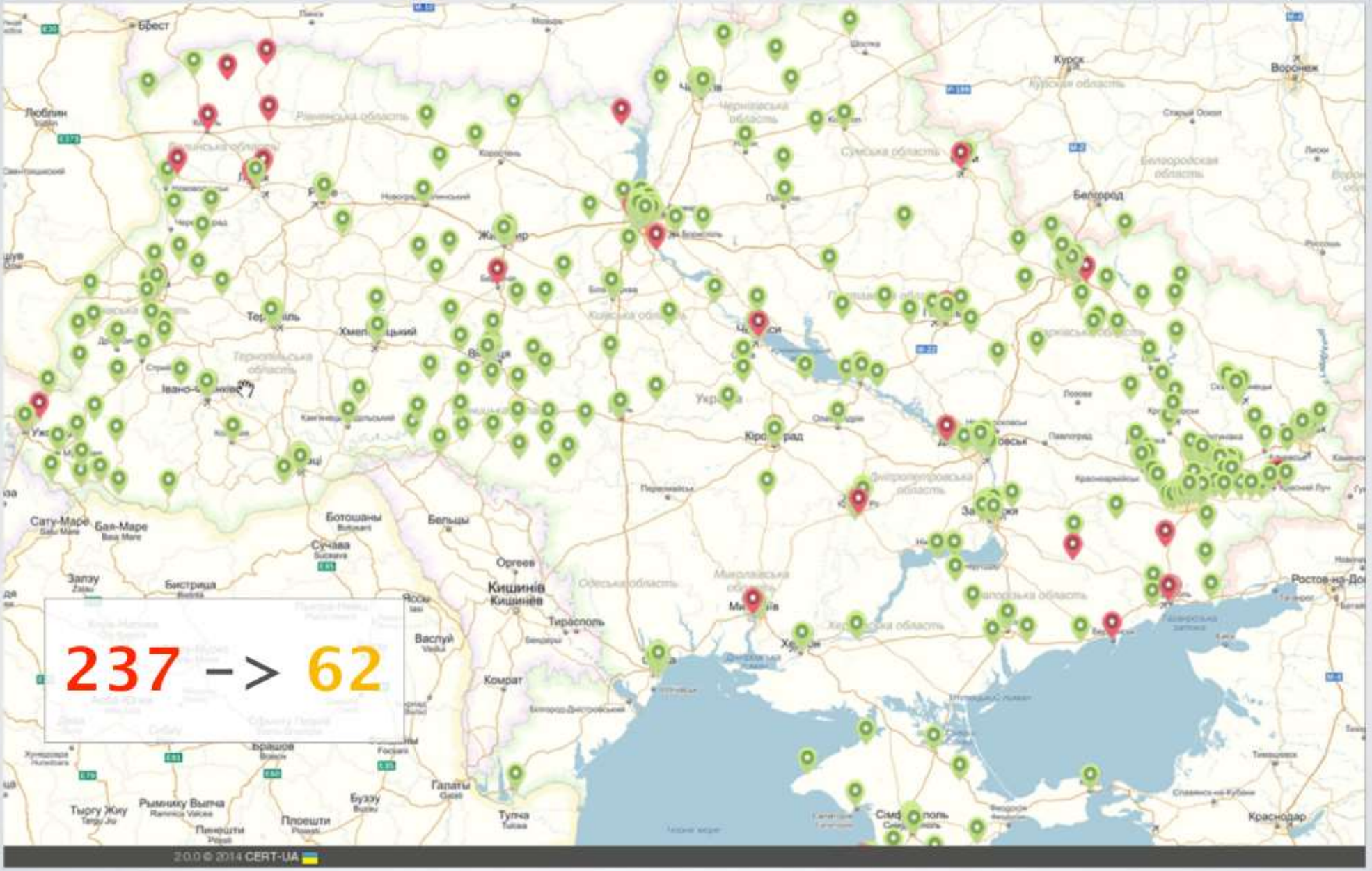


IPGUARD FEEDS

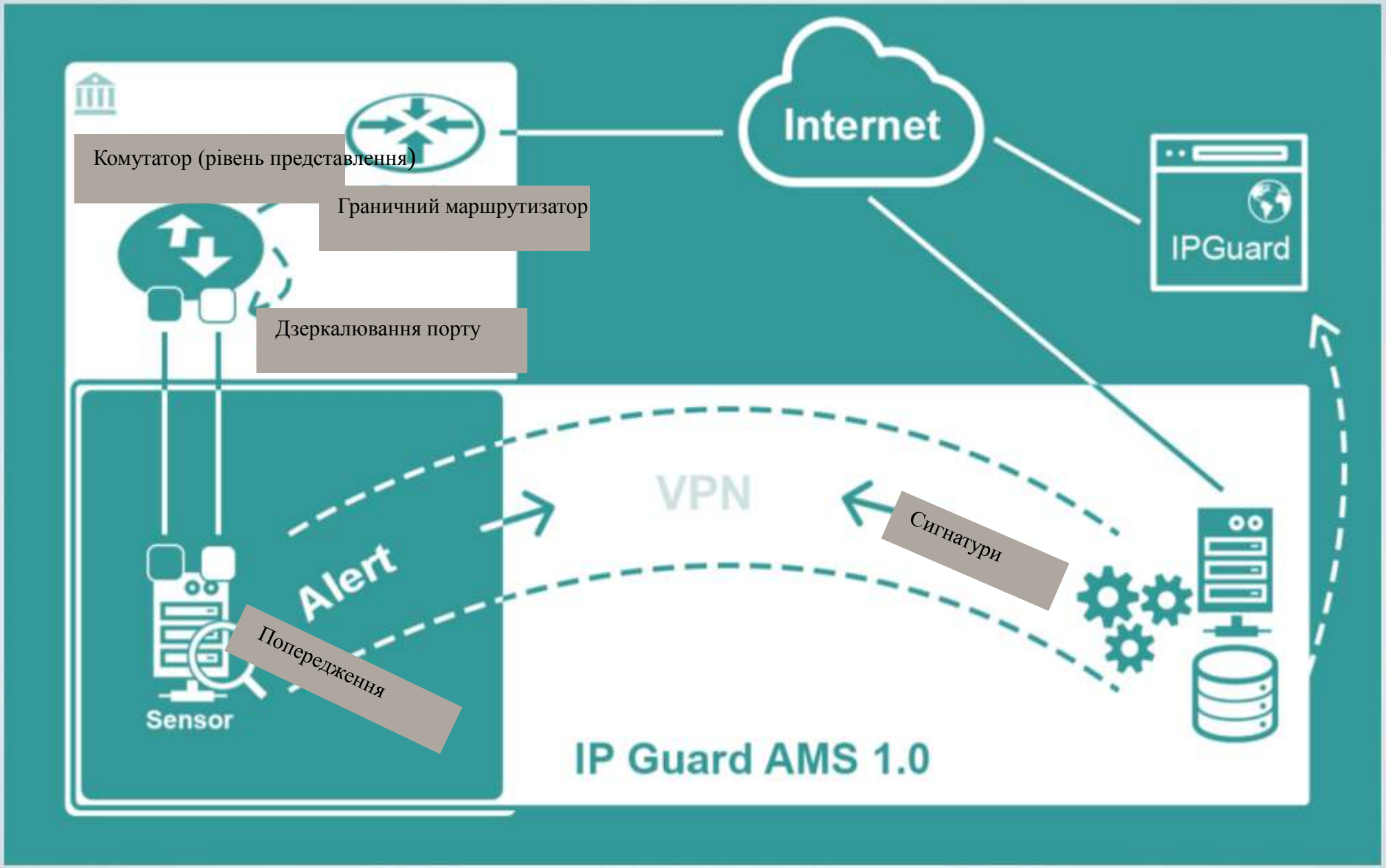
IPGUARD FEEDS (ДО)



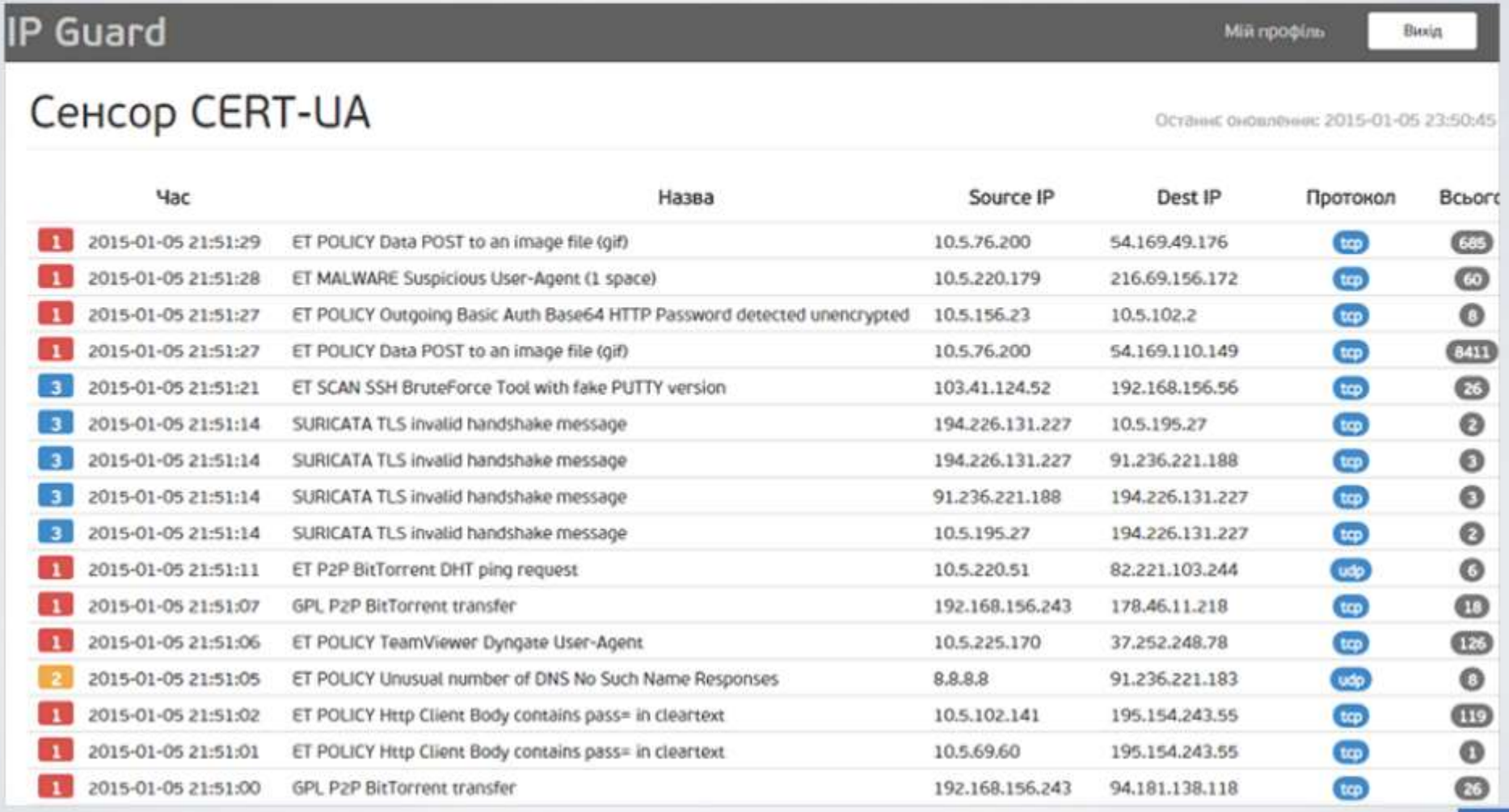
IPGUARD FEEDS (ПІСЛЯ)



IPGUARD AMS 1.0



IPGUARD AMS 1.0



	Час	Назва	Source IP	Dest IP	Протокол	Всього
1	2015-01-05 21:51:29	ET POLICY Data POST to an image file (gif)	10.5.76.200	54.169.49.176	tcp	685
1	2015-01-05 21:51:28	ET MALWARE Suspicious User-Agent (1 space)	10.5.220.179	216.69.156.172	tcp	60
1	2015-01-05 21:51:27	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted	10.5.156.23	10.5.102.2	tcp	8
1	2015-01-05 21:51:27	ET POLICY Data POST to an image file (gif)	10.5.76.200	54.169.110.149	tcp	8411
3	2015-01-05 21:51:21	ET SCAN SSH BruteForce Tool with fake PUTTY version	103.41.124.52	192.168.156.56	tcp	26
3	2015-01-05 21:51:14	SURICATA TLS invalid handshake message	194.226.131.227	10.5.195.27	tcp	2
3	2015-01-05 21:51:14	SURICATA TLS invalid handshake message	194.226.131.227	91.236.221.188	tcp	3
3	2015-01-05 21:51:14	SURICATA TLS invalid handshake message	91.236.221.188	194.226.131.227	tcp	3
3	2015-01-05 21:51:14	SURICATA TLS invalid handshake message	10.5.195.27	194.226.131.227	tcp	2
1	2015-01-05 21:51:11	ET P2P BitTorrent DHT ping request	10.5.220.51	82.221.103.244	udp	6
1	2015-01-05 21:51:07	GPL P2P BitTorrent transfer	192.168.156.243	178.46.11.218	tcp	18
1	2015-01-05 21:51:06	ET POLICY TeamViewer Dyngate User-Agent	10.5.225.170	37.252.248.78	tcp	126
2	2015-01-05 21:51:05	ET POLICY Unusual number of DNS No Such Name Responses	8.8.8.8	91.236.221.183	udp	8
1	2015-01-05 21:51:02	ET POLICY Http Client Body contains pass= in cleartext	10.5.102.141	195.154.243.55	tcp	119
1	2015-01-05 21:51:01	ET POLICY Http Client Body contains pass= in cleartext	10.5.69.60	195.154.243.55	tcp	1
1	2015-01-05 21:51:00	GPL P2P BitTorrent transfer	192.168.156.243	94.181.138.118	tcp	26

IPGUARD результати

- IPGuard FEEDs: 245 користувачів
- IPGuard AMS: 13 сенсорів

Вартість: безкоштовно

Розгорнуто: 3 місяці

Дякую за Вашу увагу!

Іван Соколов
www.cert.gov.ua
sio@cert.gov.ua
01/10/2015

CERT-UA
computer emergency
response team of Ukraine