Highly reliable network topology at JINR. Monitoring. Vulnerabilities.

Kirill Angelov
Meshcheryakov Laboratory of Information Technologies
Joint Institute for Nuclear Research
Dubna, Russia
kirill@jinr.ru

Andrey Baginyan
Meshcheryakov Laboratory of Information Technologies
Joint Institute for Nuclear Research
Dubna, Russia
bag@jinr.ru

Andrey Dolbilov
Meshcheryakov Laboratory of Information Technologies
Joint Institute for Nuclear Research
Dubna, Russia
dolbilov@jinr.ru

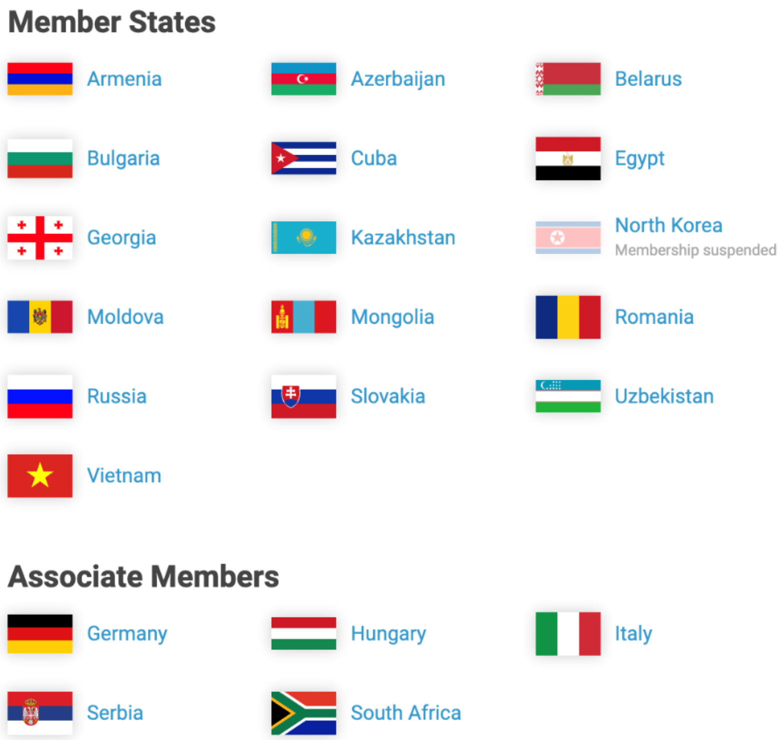
Ivan Kashunin
Meshcheryakov Laboratory of Information Technologies
Joint Institute for Nuclear Research
Dubna, Russia
miramir@jinr.ru

Vladimir Korenkov
Meshcheryakov Laboratory of Information Technologies
Joint Institute for Nuclear Research
Dubna, Russia
korenkov@jinr.ru

Dubna

https://www.atomic-energy.ru/news/2017/06/29/77310

The Joint Institute for Nuclear Research (JINR)



Member States

- Armenia
- Azerbaijan
- Belarus
- Bulgaria
- Cuba
- Egypt
- Georgia
- Kazakhstan
- North Korea
  Membership suspended
- Moldova
- Mongolia
- Romania
- Russia
- Slovakia
- Uzbekistan
- Vietnam

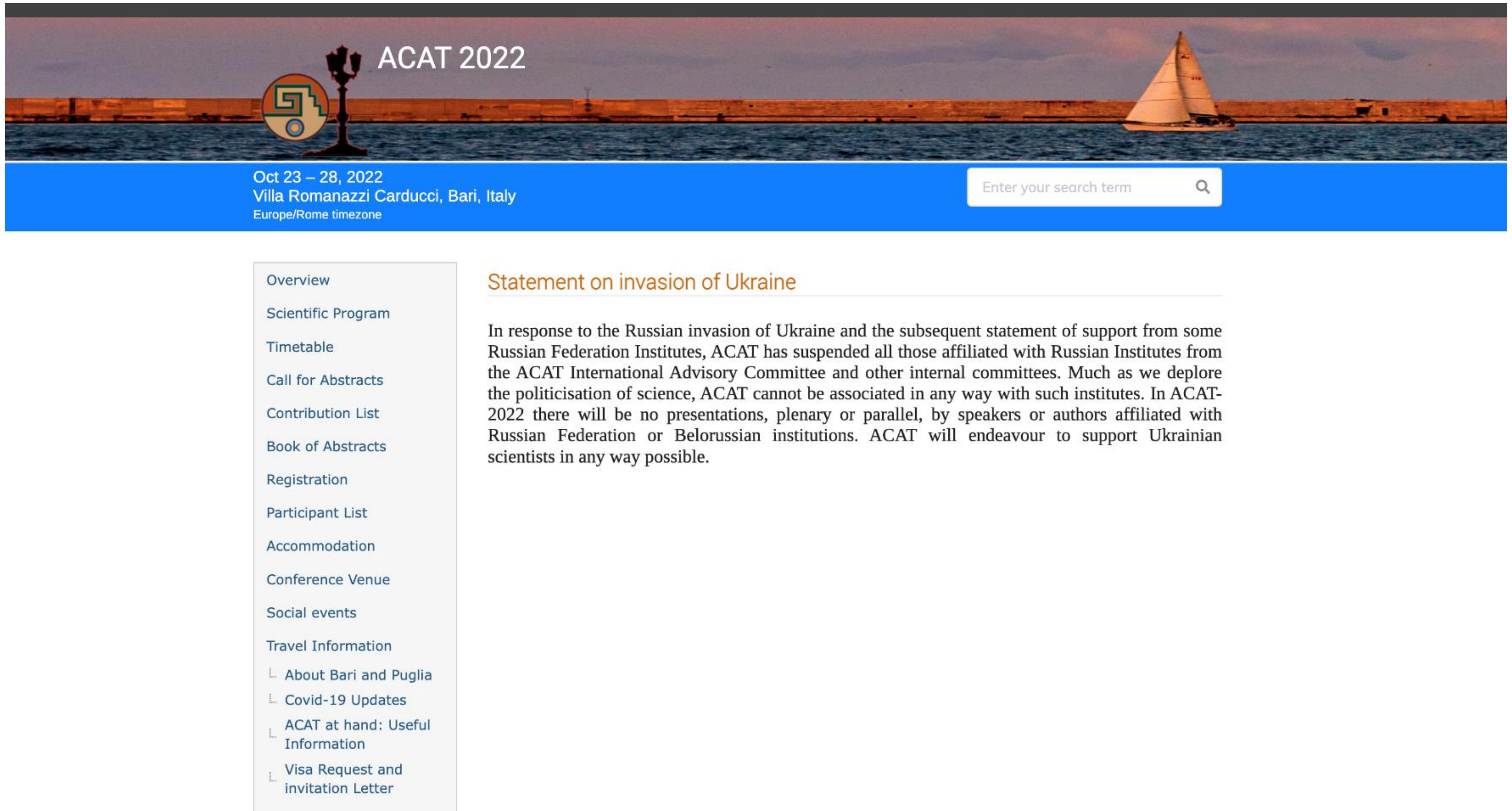
Associate Members

- Germany
- Hungary
- Italy
- Serbia
- South Africa

The JINR's Baykal lake neutrino program

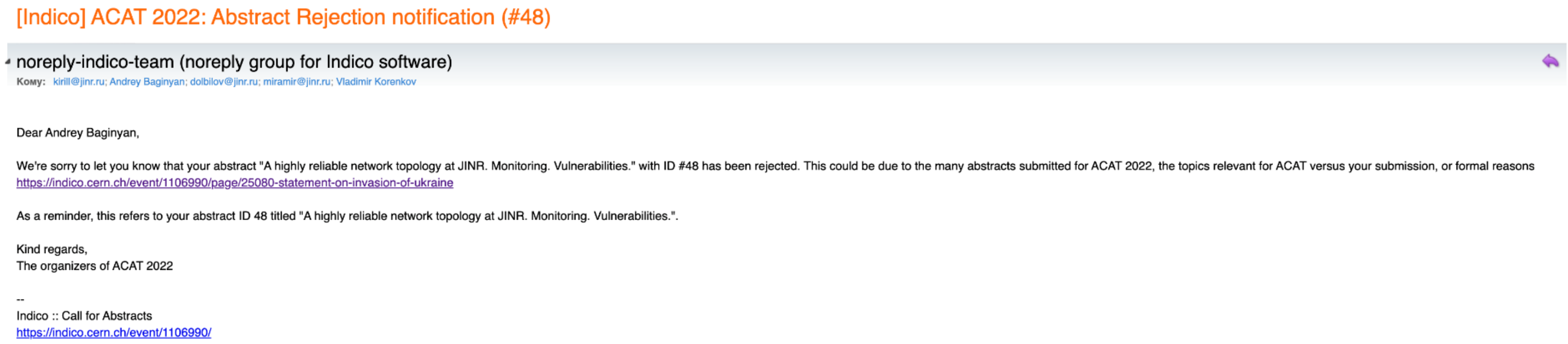
DC-280 cyclotron

Till 2025



Statement on invasion of Ukraine

In response to the Russian invasion of Ukraine and the subsequent statement of support from some Russian Federation Institutes, ACAT has suspended all those affiliated with Russian Institutes from the ACAT International Advisory Committee and other internal committees. Much as we deplore the politicisation of science, ACAT cannot be associated in any way with such institutes. In ACAT-2022 there will be no presentations, plenary or parallel, by speakers or authors affiliated with Russian Federation or Belorussian institutions. ACAT will endeavour to support Ukrainian scientists in any way possible.



[Indico] ACAT 2022: Abstract Rejection notification (#48)

noreply-indico-team (noreply group for Indico software)

Кому: kirill@jinr.ru; Andrey Baginyan; dolbilov@jinr.ru; miramir@jinr.ru; Vladimir Korenkov

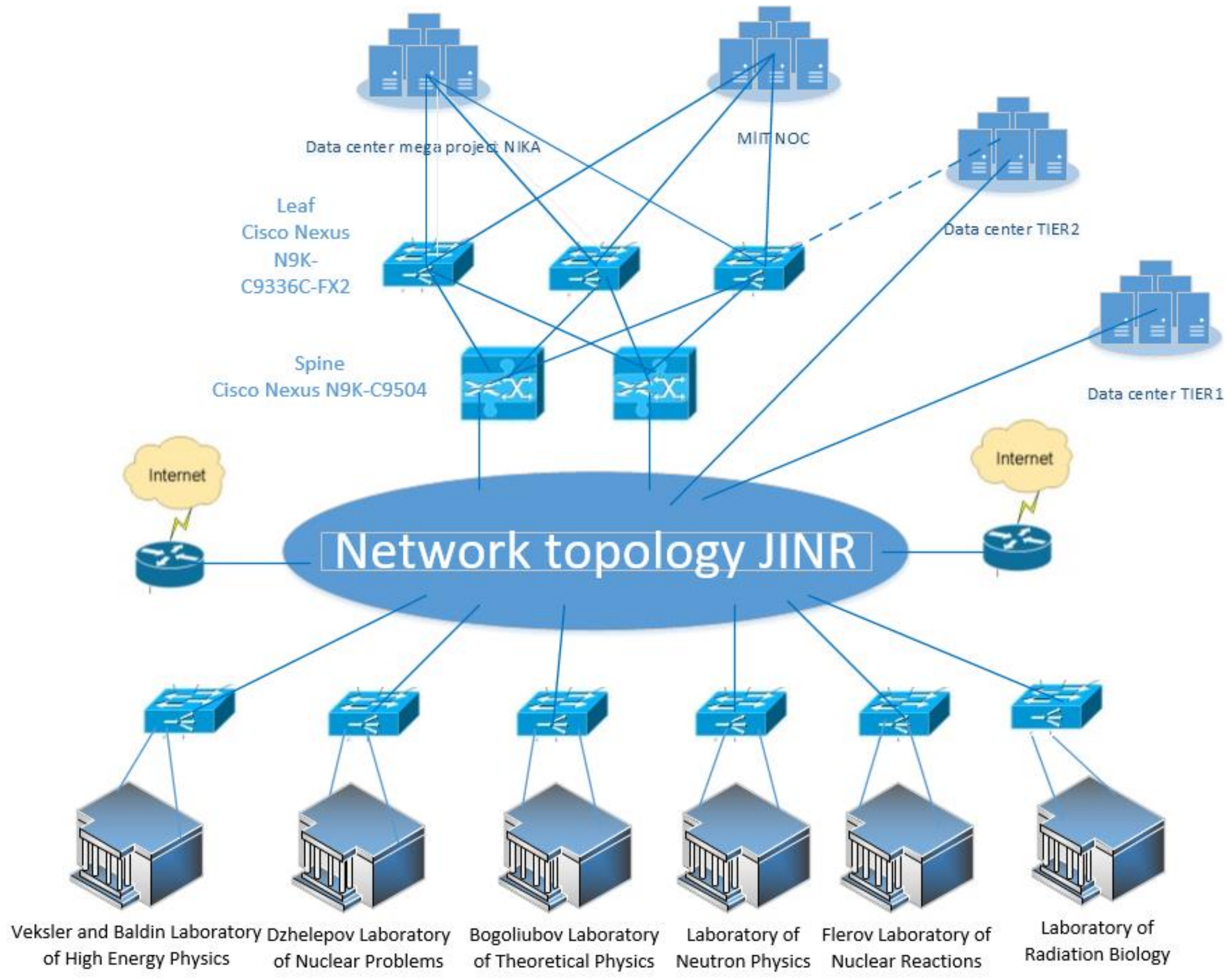
Dear Andrey Baginyan,

We're sorry to let you know that your abstract "A highly reliable network topology at JINR. Monitoring. Vulnerabilities." with ID #48 has been rejected. This could be due to the many abstracts submitted for ACAT 2022, the topics relevant for ACAT versus your submission, or formal reasons
https://indico.cern.ch/event/1106990/page/25080-statement-on-invasion-of-ukraine

As a reminder, this refers to your abstract ID 48 titled "A highly reliable network topology at JINR. Monitoring. Vulnerabilities.".

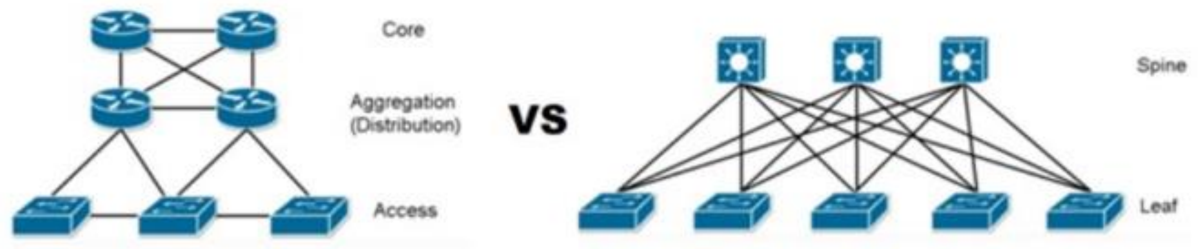
Kind regards,
The organizers of ACAT 2022

--
Indico :: Call for Abstracts
https://indico.cern.ch/event/1106990/



Since 2020, there has been a gradual migration of the network to the fabric based on Cisco Application Centric Infrastructure technology, and at present, all the laboratories of the Institute have already been integrated.

Cisco ACI fabric and traditional hierarchical model

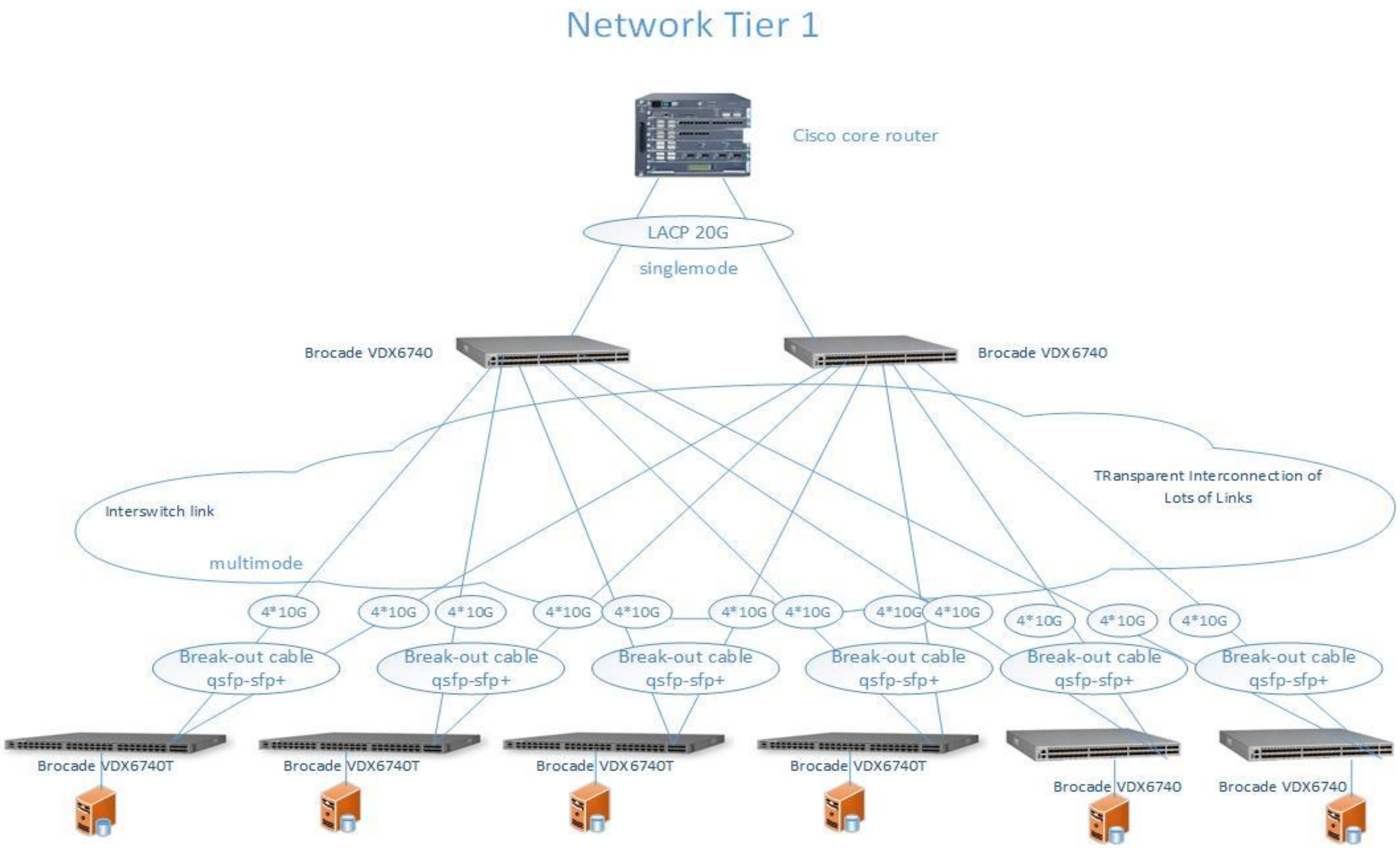


Software-defined Network

The major advantages of this fabric in comparison with the previously existing network hierarchy:

- the application-based policy enforcement enables the automation of the running software;
- the time intervals required for the provision of different services are significantly reduced;
- the processes of allocating network resources, troubleshooting, applying security policies are also automated;
- all the necessary conditions for the easy coordination of usage policies appear for cloud and local applications;
- automated monitoring functions are provided. Applications are monitored in real time;
- the implementation of the Cisco Application Centric Infrastructure allows one to provide the flexible horizontal scaling of systems. The hardware can be operated in multi-user mode.

TRILL fabric at Tier1

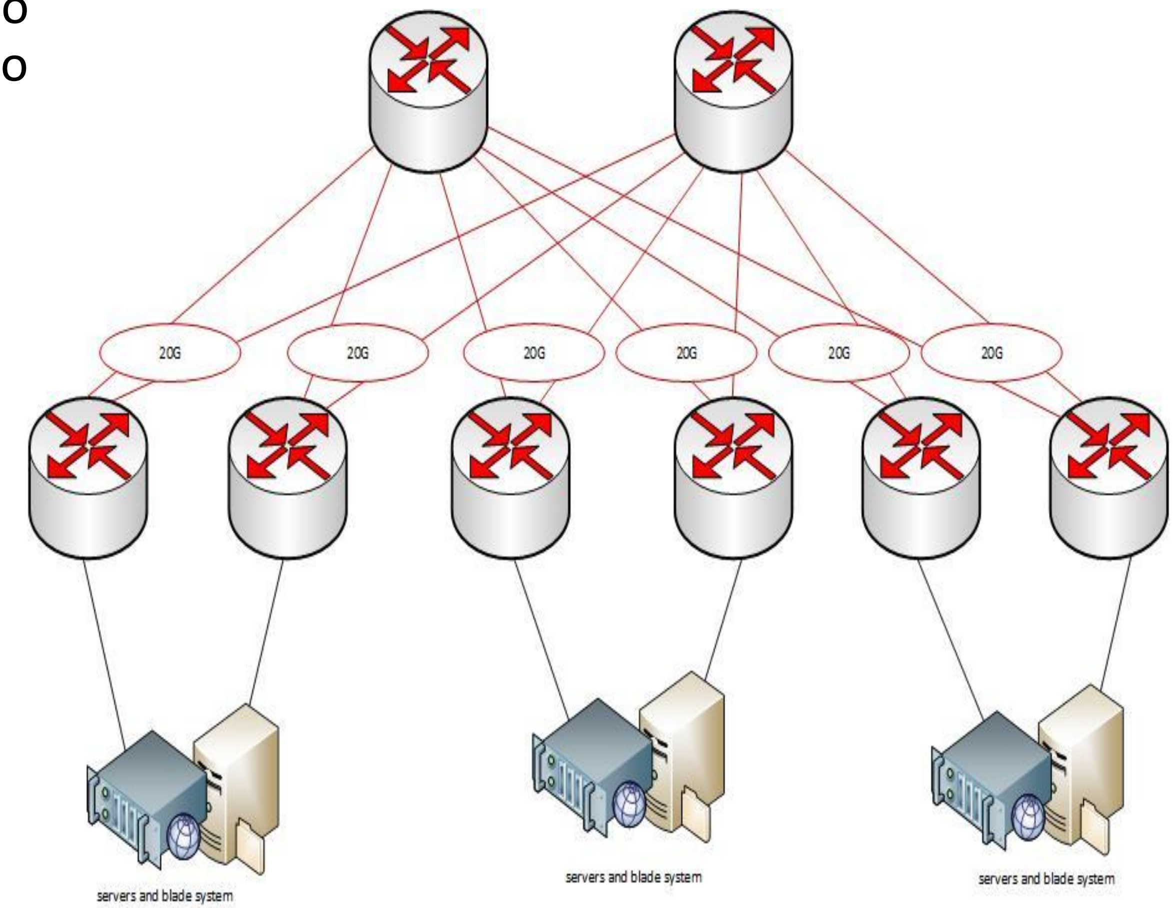


Both centers are built on top of the network fabric based on the TRILL (Transparent Interconnection of Lots of Links) protocol. The approximate scheme of the GRID sites Tier2 and Tier1 functioning on this technology has few visible differences; however, when routing package data transfer, different protocols are used. Cisco ACI uses MP-BGP as a routing protocol, which is run internal to the fabric. It allows the border leafs to redistribute external routes inside the fabric. MP-BGP is used to distribute the external routes to the other leaf switches. By default, this route redistribution is not actually enabled. It turns out that it is impossible to integrate one fabric into another.

Non-blocking architecture

Tim Berners-Lee
URL, HTTP, HTML

The network architecture of the fabric data center at JINR is designed with a dual route between the distributed level and the core level on the Cisco equipment. Each server will have access to the network segment with two equal-value connections of 10G with a total bandwidth o 20G.

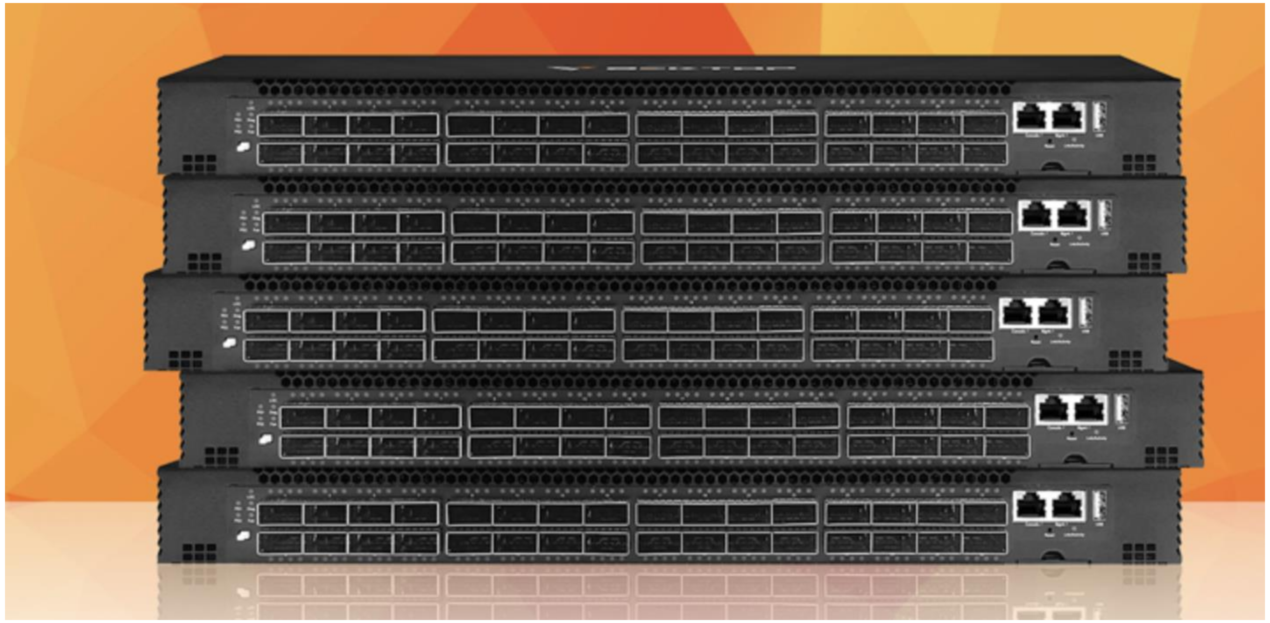


Radia Joy Perlman
1985 - Spanning tree
1992 - IS-IS
2010 - Transparent Interconnection of Lots of Links

H3C

H3C IRF2 intelligent fault-tolerant architecture technology
Excellent scalability: With IRF2, device aggregation can be done in a plug-and-play manner by simply adding one or more switches to an IRF2 stack and enabling IRF2 stacking on the new device. The new devices will be managed through the same IP address, providing a scalable, easy-to-manage networking platform for the data center.
High Reliability: The IRF2 stack backs up all control plane and data plane information to realize Layer 3 seamless forwarding, greatly improving the reliability and performance of the IRF2 group, eliminating critical elements that could cause the entire system to fail, and avoiding violations in the work of the organization.
Load Balancing: IRF2 supports cross-device link aggregation, allowing connection to higher and lower end devices using multiple physical links. This creates another layer of redundancy in the network and contributes to better utilization of network resources.

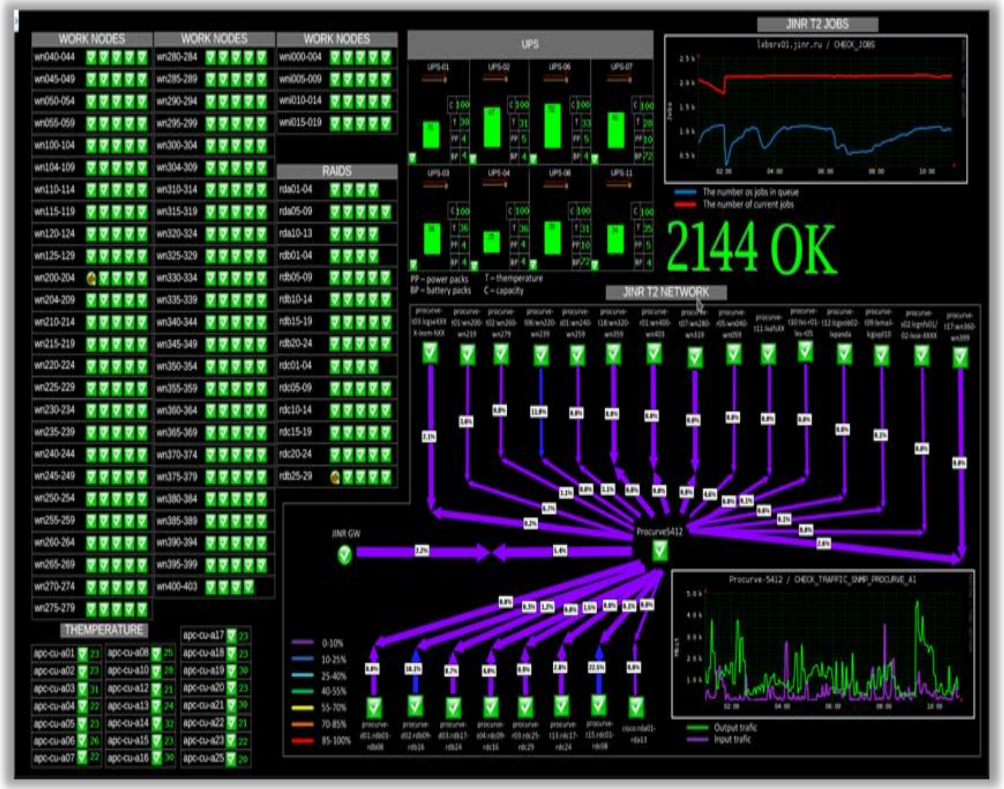
Vector

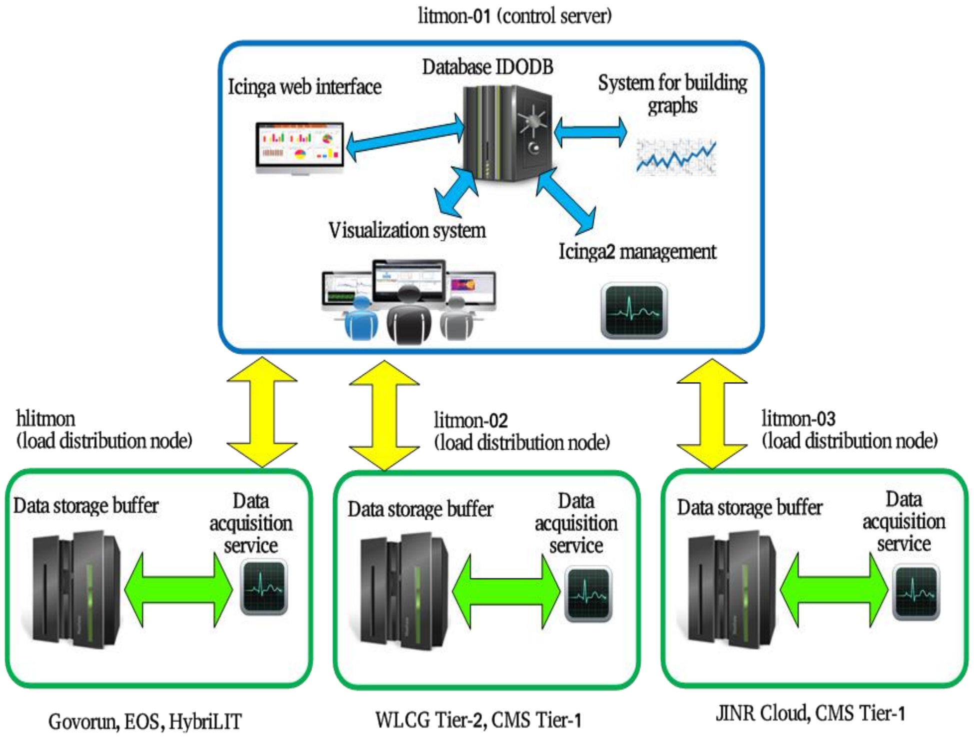


Vector Core Switch VC7200 series switches are compact, high-performance switches that provide connectivity at today's speeds of 10, 25, 40, and 100 Gbps, enabling flexible network core reconnaissance as well as use as ToR switches in high port density architectures. Key Features:

stacking support for up to 8 switches;
non-blocking switching architecture;
support for routing protocols RIP, OSPF, BGP, PIM;
support for RSTP, MSTP, ERPS, LACP, Loopback detection;
support for IP Source Guard, DAI;
quality of service (QoS) management;
support for VxLAN technology.

MONITORING




litmon-01 (control server)

Icinga web interface

Database IDODB

System for building graphs

Visualization system

Icinga2 management

hlitmon
(load distribution node)

litmon-02
(load distribution node)

litmon-03
(load distribution node)

Data storage buffer

Data acquisition service

Data storage buffer

Data acquisition service

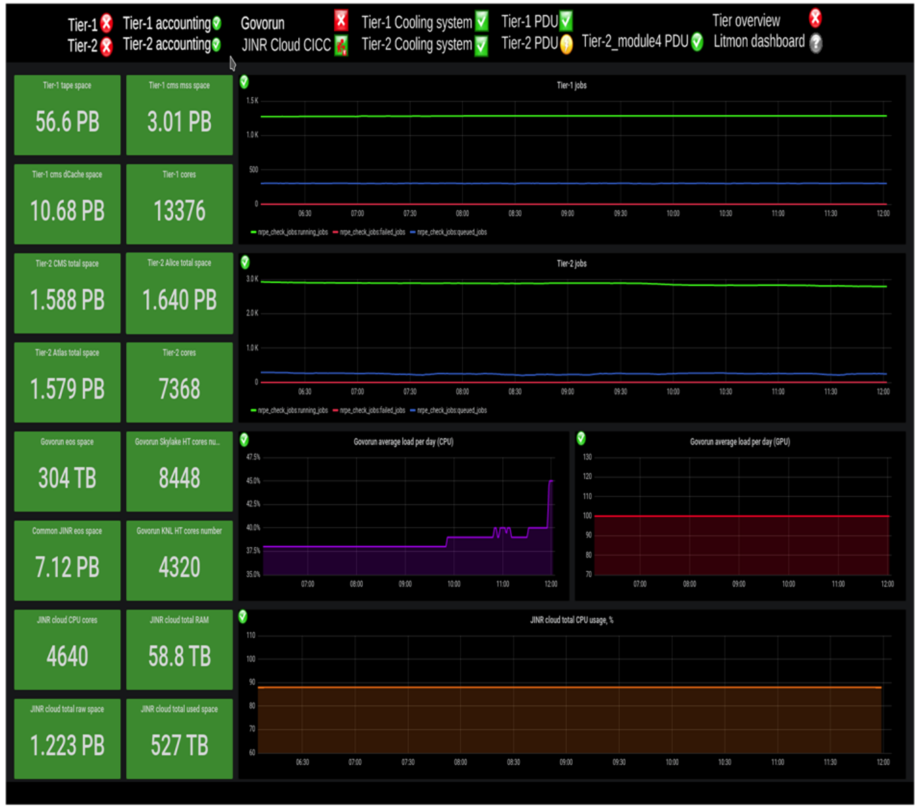
Data storage buffer

Data acquisition service

Govorun, EOS, HybriLIT

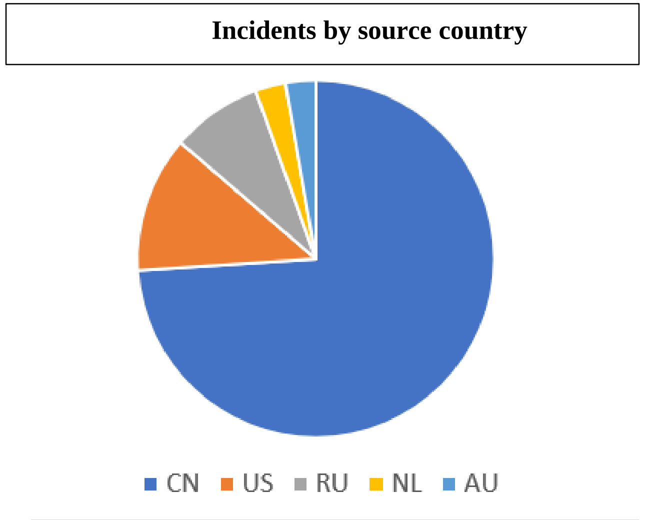
WLCG Tier-2, CMS Tier-1

JINR Cloud, CMS Tier-1

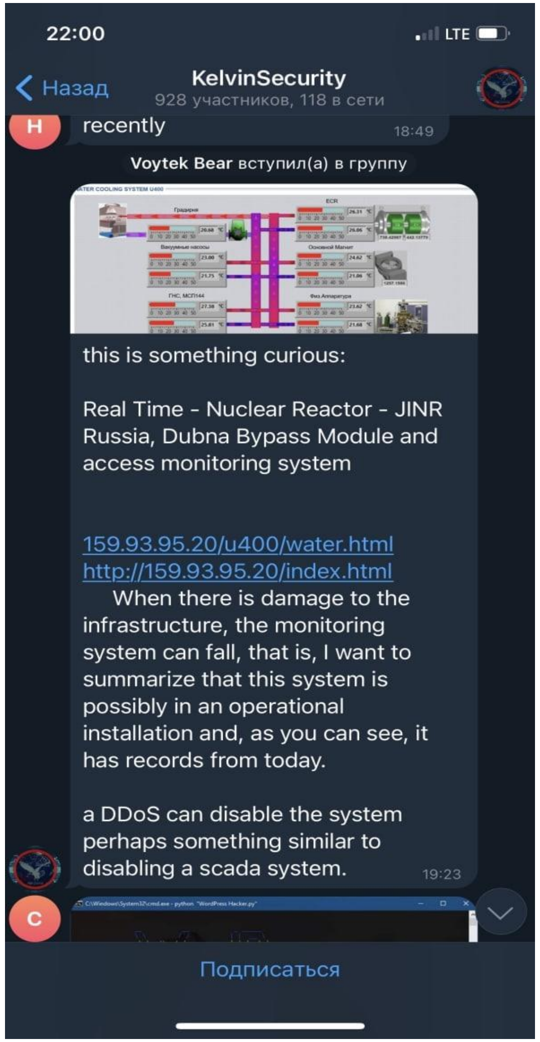


Apart from adding nodes and creating new data acquisition and processing plugins, novel visualization tools are being developed. In 2020, a visualization system, Grafana, was integrated in addition to NagVis. The combination of several visualization systems resulted in the significant expansion of tools for creating information screens. A general information screen displaying the characteristics of the computing complex was developed.

NETWORK VULNERABILITIES



Incidents by source country



recently 18:49

Voytek Bear вступил(а) в группу

this is something curious:

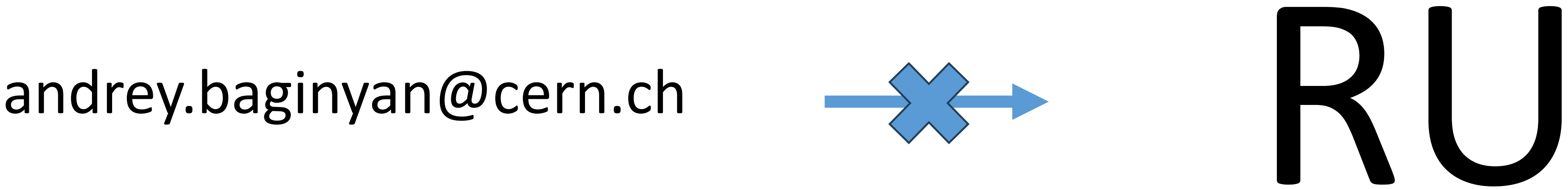
Real Time - Nuclear Reactor - JINR Russia, Dubna Bypass Module and access monitoring system

159.93.95.20/u400/water.html
http://159.93.95.20/index.html
When there is damage to the infrastructure, the monitoring system can fall, that is, I want to summarize that this system is possibly in an operational installation and, as you can see, it has records from today.

a DDoS can disable the system perhaps something similar to disabling a scada system. 19:23

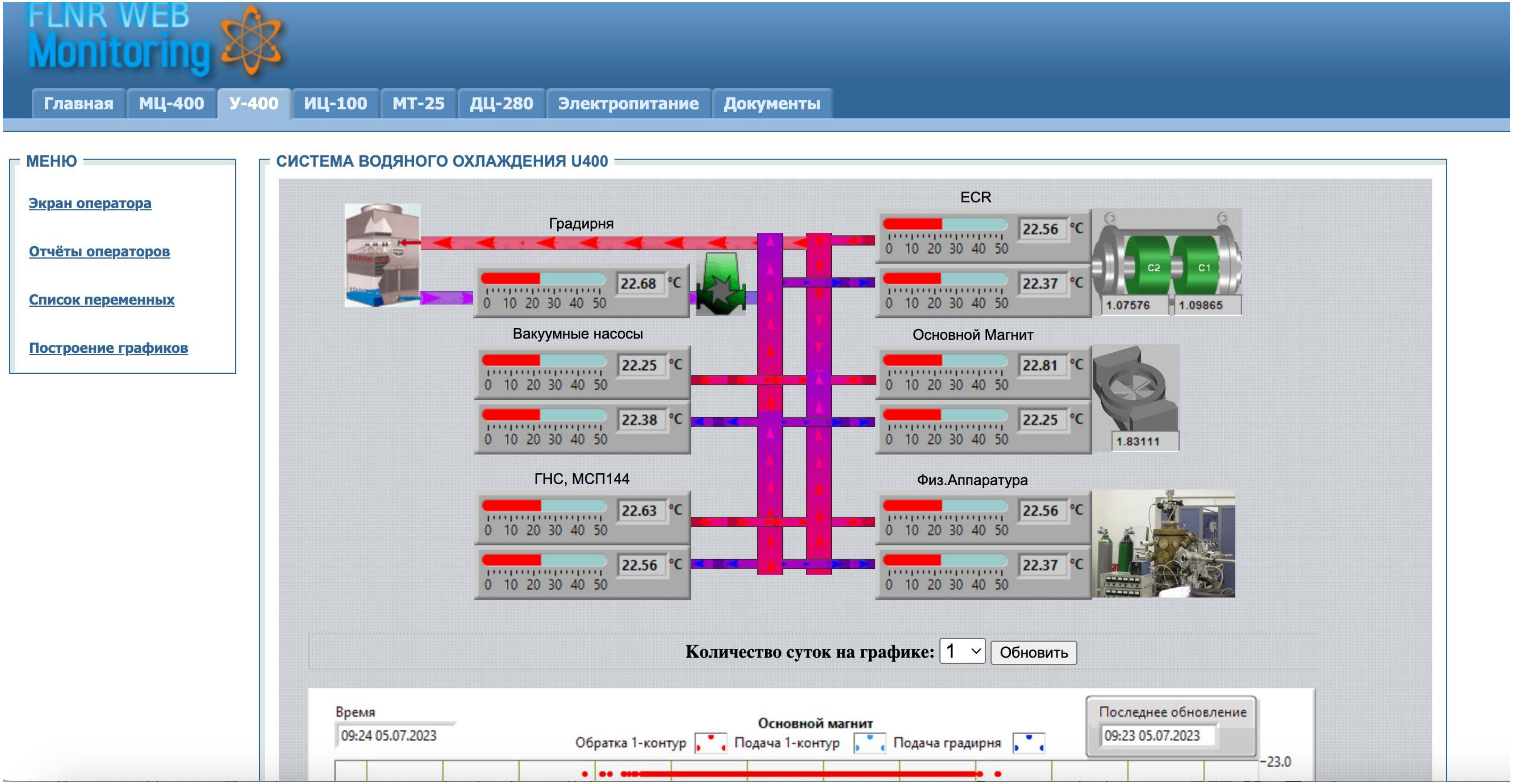
Over the past five months, more than 60,000 incoming attacks have been recorded. Attacks usually are classified in accordance with the two most popular features, these are password guessing and port scanning.

To maintain information support, it was decided to enhance staff members' awareness via mailing lists and news feeds. In the case of possible problems with the jinr.ru domain, a reserve domain in the "int" (international) zone was deployed.



andrey.baginyan@cern.ch

RU

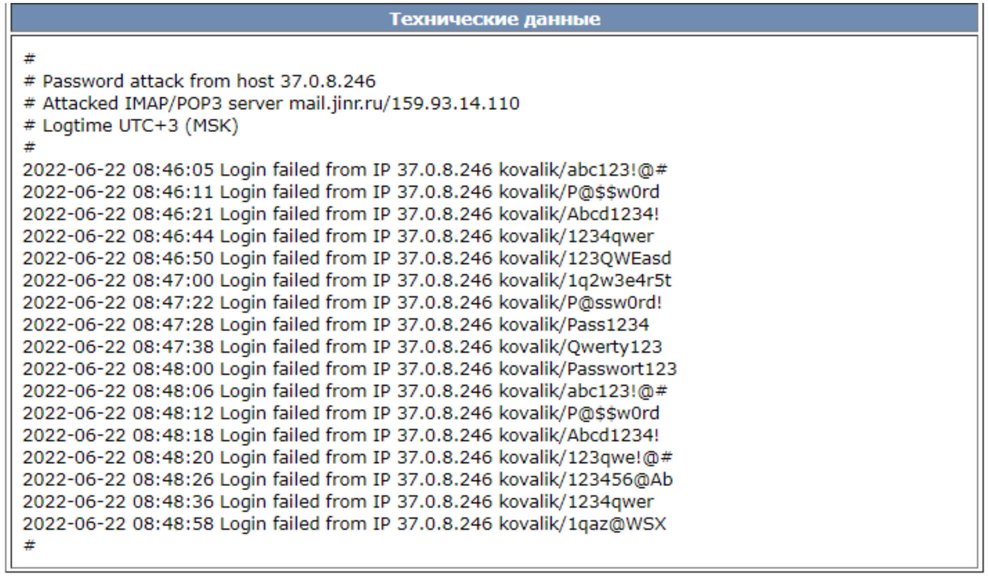


СИСТЕМА ВОДЯНОГО ОХЛАЖДЕНИЯ U400

Количество суток на графике: 1

Время: 09:24 05.07.2023

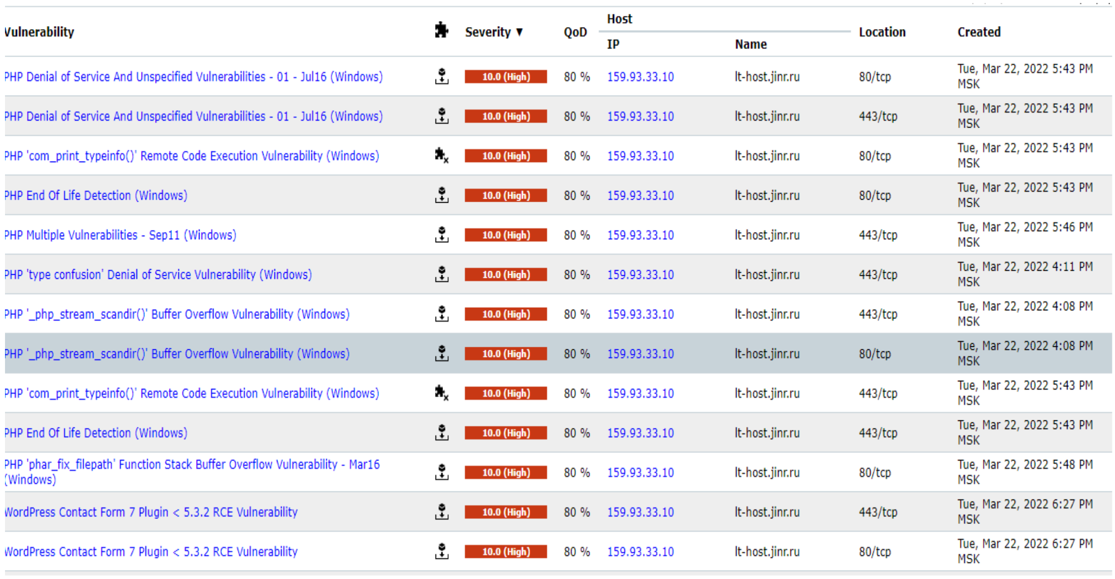
Последнее обновление: 09:23 05.07.2023



Технические данные

```
#
# Password attack from host 37.0.8.246
# Attacked IMAP/POP3 server mail.jinr.ru/159.93.14.110
# Logtime UTC+3 (MSK)
#
2022-06-22 08:46:05 Login failed from IP 37.0.8.246 kovalik/abc123!@#
2022-06-22 08:46:11 Login failed from IP 37.0.8.246 kovalik/P@$$w0rd
2022-06-22 08:46:21 Login failed from IP 37.0.8.246 kovalik/Abcd1234!
2022-06-22 08:46:44 Login failed from IP 37.0.8.246 kovalik/1234qwer
2022-06-22 08:46:50 Login failed from IP 37.0.8.246 kovalik/123QWEasd
2022-06-22 08:47:00 Login failed from IP 37.0.8.246 kovalik/1q2w3e4r5t
2022-06-22 08:47:22 Login failed from IP 37.0.8.246 kovalik/P@ssw0rd!
2022-06-22 08:47:28 Login failed from IP 37.0.8.246 kovalik/Pass1234
2022-06-22 08:47:38 Login failed from IP 37.0.8.246 kovalik/Qwerty123
2022-06-22 08:48:00 Login failed from IP 37.0.8.246 kovalik/Passwort123
2022-06-22 08:48:06 Login failed from IP 37.0.8.246 kovalik/abc123!@#
2022-06-22 08:48:12 Login failed from IP 37.0.8.246 kovalik/P@$$w0rd
2022-06-22 08:48:18 Login failed from IP 37.0.8.246 kovalik/Abcd1234!
2022-06-22 08:48:20 Login failed from IP 37.0.8.246 kovalik/123qwe!@#
2022-06-22 08:48:26 Login failed from IP 37.0.8.246 kovalik/123456@Ab
2022-06-22 08:48:36 Login failed from IP 37.0.8.246 kovalik/1234qwer
2022-06-22 08:48:58 Login failed from IP 37.0.8.246 kovalik/1qaz@WSX
#
```

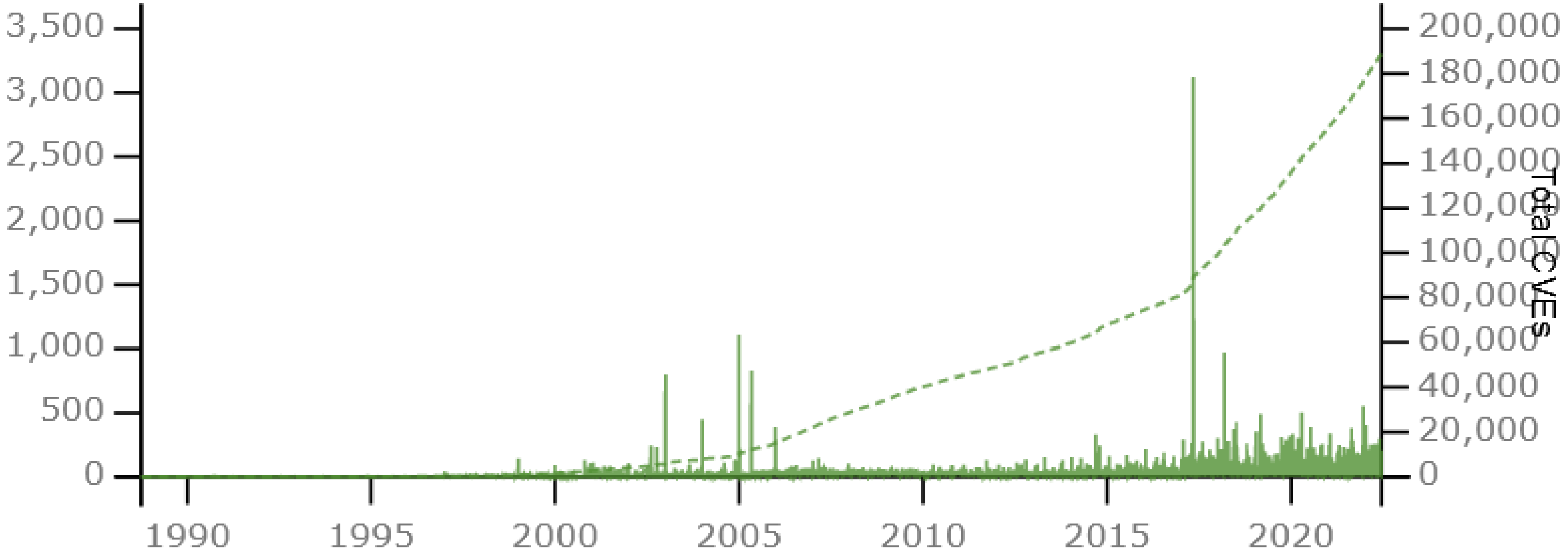
Example of guessing passwords when trying to hack an email account.



Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)		10.0 (High)	80 %	159.93.33.10	lt-host.jinr.ru	80/tcp	Tue, Mar 22, 2022 5:43 PM MSK
PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)		10.0 (High)	80 %	159.93.33.10	lt-host.jinr.ru	443/tcp	Tue, Mar 22, 2022 5:43 PM MSK
PHP 'com_print_typeinfo()' Remote Code Execution Vulnerability (Windows)		10.0 (High)	80 %	159.93.33.10	lt-host.jinr.ru	80/tcp	Tue, Mar 22, 2022 5:43 PM MSK
PHP End Of Life Detection (Windows)		10.0 (High)	80 %	159.93.33.10	lt-host.jinr.ru	80/tcp	Tue, Mar 22, 2022 5:43 PM MSK
PHP Multiple Vulnerabilities - Sep11 (Windows)		10.0 (High)	80 %	159.93.33.10	lt-host.jinr.ru	443/tcp	Tue, Mar 22, 2022 5:46 PM MSK
PHP 'type confusion' Denial of Service Vulnerability (Windows)		10.0 (High)	80 %	159.93.33.10	lt-host.jinr.ru	443/tcp	Tue, Mar 22, 2022 4:11 PM MSK
PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows)		10.0 (High)	80 %	159.93.33.10	lt-host.jinr.ru	443/tcp	Tue, Mar 22, 2022 4:08 PM MSK
PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows)		10.0 (High)	80 %	159.93.33.10	lt-host.jinr.ru	80/tcp	Tue, Mar 22, 2022 4:08 PM MSK
PHP 'com_print_typeinfo()' Remote Code Execution Vulnerability (Windows)		10.0 (High)	80 %	159.93.33.10	lt-host.jinr.ru	443/tcp	Tue, Mar 22, 2022 5:43 PM MSK
PHP End Of Life Detection (Windows)		10.0 (High)	80 %	159.93.33.10	lt-host.jinr.ru	443/tcp	Tue, Mar 22, 2022 5:43 PM MSK
PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Windows)		10.0 (High)	80 %	159.93.33.10	lt-host.jinr.ru	80/tcp	Tue, Mar 22, 2022 5:48 PM MSK
WordPress Contact Form 7 Plugin < 5.3.2 RCE Vulnerability		10.0 (High)	80 %	159.93.33.10	lt-host.jinr.ru	443/tcp	Tue, Mar 22, 2022 6:27 PM MSK
WordPress Contact Form 7 Plugin < 5.3.2 RCE Vulnerability		10.0 (High)	80 %	159.93.33.10	lt-host.jinr.ru	80/tcp	Tue, Mar 22, 2022 6:27 PM MSK

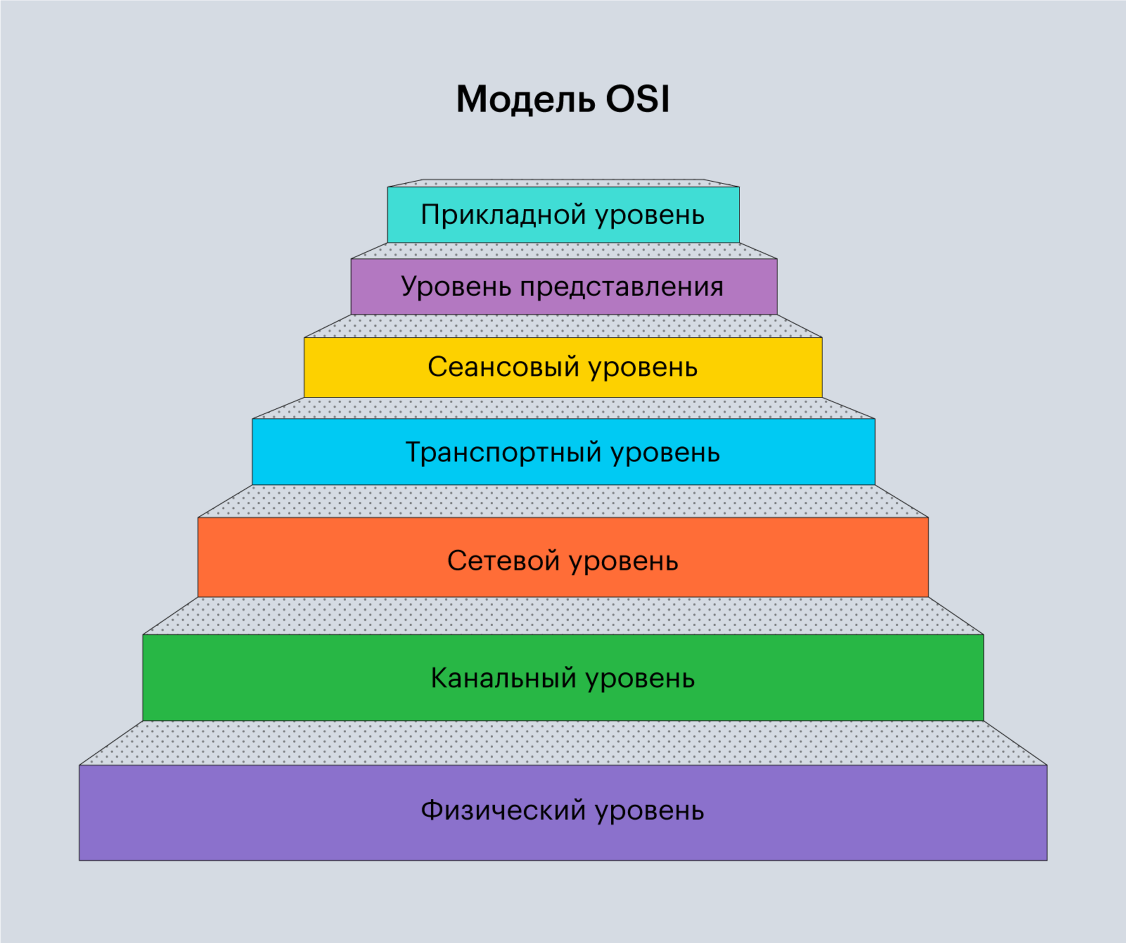
Example of scanning a host for vulnerabilities.

Growth in the number of known vulnerabilities by year.



DNS problems

AppStore → 1.1.1.1



USA, China, Russia….

USA, China

Thank you