



+7 (495) 988-00-40
Available 24/7

CERT-GIB

[Powers of CERT-GIB](#)

[About](#)

[Interaction policy](#)

[For LEA, IT-Security and Media](#)

[Communications policy](#)

[FAQ](#)



CERT-GIB - Information Security Incidents Response 24/7

Useful information
[What is CERT](#)

ABOUT CERT-GIB

CERT-GIB's Structure

Currently, CERT-GIB is the first and only private CERT in Russia.

CERT-GIB is a rapid response unit, created on the basis of Group IB.

To ensure a continuous operational cycle, information gathering and incident response is performed 24/7/365 from the three geographical locations of CERT-GIB in Moscow, New York, and Singapore.

Our mission:

- To coordinate the exchange of information regarding IT security incidents between law enforcement agencies, corporations, and individuals;
- To assist in maintaining cyber security within the Russian segment of the Internet and beyond;
- To assist in prompt cyber risk management and elimination of virtual threat sources.

As part of its mission, CERT-GIB provides free around-the-clock information security assistance and response for incidents occurring in the Russian-speaking segments of the Internet.

Examples of our activities include but are not limited to:

- Providing initial guidance and support for DDoS-related incidents and their victims;
- Informing the incidents victims - individuals or organizations - regarding the incurred risks;
- Assisting the victims in contacting registrars, hosting providers and LEA in Russia and the former USSR;
- Taking down fraudulent sites, such as phishing, fake banking, scam, brand infringement and other types of malevolent sites.

In executing its mission, CERT-GIB does not commit to managing and supporting the client's IT infrastructure.

Incident response

What constitutes an incident?

An IT security incident is an isolated or a continuing unwanted or unexpected event within the system of information security which has great potential to compromise the flow of business and jeopardize the security of the information.

These events may constitute:

- Denial of services attacks (DoS, DDoS);
- Unauthorized use of data processing and storage systems;
- Data compromise;
- Asset compromise;
- Internal/external unauthorized access;
- Creation and distribution of malicious software;
- Breach of information security policies;
- Phishing and unlawful brand use online;
- Fraud with online banking and electronic payment systems.

CERT-GIB's relationship with other CERT organizations

Worldwide there are approximately three hundred organizations using as part of their name the CERT, or similar, abbreviation, and most of them are teams which quickly respond to IT security incidents.

[Contact information](#)

[Report an incident](#)

[PGP Key](#)

[RFC 2350](#)

Tweets

Follow

CERT-GIB @CERTGIB 21h
 Владимир Путин подписал закон о введении уголовной ответственности за скимминг.
securitylab.ru/news/473250.php
 Expand

CERT-GIB @CERTGIB 2 Jun
 The twins: with the help of Group-IB two brothers on probation were arrested for online-banking theft in Russia.
group-ib.com/index.php/7-no...
 Expand

CERT-GIB @CERTGIB 2 Jun
 Братья-2: при участии Group-IB задержаны хакеры с условным сроком, похищавшие деньги пользователей интернет-банкинга.
group-ib.ru/index.php/7-no...

CERT-GIB @CERTGIB 21 May
 Hundreds of Cloud Services Potentially Vulnerable to Logjam Attacks
securityweek.com/hundreds-cloud...

Tweet to @CERTGIB



[Upload URL of malicious resource](#)

Although there is no direct relationship between CERT-GIB and other CERTs/CSIRTs, we are constantly in contact with most of these organizations, and, in case of need, we can coordinate actions related to IT security incidents directly with them.

Our partners

Our partners include:

- Russian telecommunication service providers;
- Banks and their clients;
- Insurance companies;
- Russian and international companies of the various sectors of the economy;
- Software developers;
- Information protection developers;
- Mass media;
- Law enforcement agencies;
- Learning institutions;
- Association of Certified Fraud Examiners (ACFE);
- CERT organizations;
- Numerous other members of the international anti-cybercrime community.



© Group-IB 2015, all rights reserved.

Phone: +7 (495) 984-33-64

E-Mail: info@group-ib.ru