2024

Unofficial translation

GUIDELINES on how to set up a UN technical PoC

NATIONAL COMPUTER INCIDENT RESPONSE AND COORDINATION CENTER | Russian Federation

Index

Introduction

Information and communication technologies (ICTs) are widely used in all social spheres making them subject to fundamental transformations. New opportunities are created for economic development. The efficiency and transparency of the government's functioning at various levels of interaction is ensured due to ICT.

At the same time the adoption of technologies does not only create opportunities for growth, but also leads to new challenges and threats to international information security.

Every year the number and sophistication of computer attacks are steadily increasing in the global information space. Criminals take advantage of the lack of regulatory mechanisms in information space between States and insufficient development of the institute of international legal assistance for criminal cases in this sphere to create a distributed infrastructure for computer attacks that are increasingly becoming cross-border in nature.

The speed with which information security threats materialize is constantly intensifying. It takes less than a few hours for the threats to become a reality since the moment any information about them becomes available.

Meanwhile, tools for conducting computer attacks, instructions on methods of organizing them and developing practical skills, as well as coordinating the relevant actions to launch computer attacks are becoming publicly available. Publication of source codes for attack tools has become regular. In addition, an independent branch of providing these tools as a service has been actually formed (Malware-as-a-service).

Effective interaction between diplomatic and technical points of contact should play a significant role in stabilizing the situation in the information space.

The second annual progress report of the UN Open-ended working group on security of and in the use of ICTs 2021–2025 contains the Elements for the development and operationalization of a global, intergovernmental points of contact directory.

Building upon the provisions for the establishment of a global intergovernmental points of contact directory, this Guide is intended to provide a minimally required set of recommendations for setting up a technical point of contact (technical PoC) to ensure effective participation of national authorities of UN Member States in this instrument.

Elements for the development and operationalization of a global, intergovernmental points of contact directory are contained in the second annual progress report of the OEWG, approved by UNGA decision No. A/ DEC /78/541 of December 22, 2023.

Basic terminology

“owner of information resource” – the owner of a website and (or) a website page on the Internet, and (or) information system, and (or) computer program using information technologies to provide information based on the collection, systematization and analysis of information located on the territory of a State;

“information resources” – information systems, information and telecommunication networks and automated control systems;

“computer attack” – the targeted impact of software and (or) software-hardware tools on an information resource aimed at disrupting and (or) ceasing its functioning and (or) creating a threat to security of information processed by this resource;

“computer incident” – a fact of disruption and (or) termination of functioning of an information resource, a telecommunication network used to provide interaction of information resources, and (or) a violation of security of information processed by an information resource, inter alia, resulted from a computer attack;

“mitigation of a computer incident” – a set of actions aimed at restoring the normal functioning of information resources after a computer incident and removing changes made by information security violator to an information resource;

“detection of computer attacks” – a set of measures aimed at identifying and analyzing indicators of computer attacks and determining their type;

“prevention of computer attacks” – a set of preventive measures aimed at strengthening protection of information resources against computer attacks;

“computer incident response” – consecutive implementation of computer incident response steps aimed at determining the technical reasons and conditions for computer incident and eliminating its consequences.

What is a UN technical PoC?

A technical PoC can be a national authorized body addressing ICT security issues and responsible for prevention and detection of computer attacks as well as computer incident response and restoring the normal functioning of an information resource (IR), for example, national computer emergency response teams and computer security incident response teams .

Description of a UN technical PoC

Depending on the capacity of authorized bodies in the field of detecting, preventing and mitigating computer attacks and responding to computer incidents at the national level, three types of technical PoCs can be distinguished:

- coordinator:

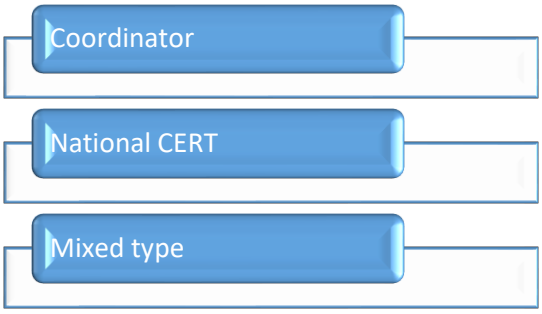
It functions as a single entry point exclusively to receive, process and distribute incoming information. This is particularly relevant if there are several computer emergency response teams operating in the country, for example, sectoral groups;

- national authorized body in the field of computer incident response:

It has the necessary technical competence in the field of detection, prevention and mitigation of computer attacks and to computer incident response.

- mixed type:

It combines the characteristics of two types of technical PoCs (for example, the Russian National Computer Incident Response and Coordination Center).



From our perspective, technical PoCs should be of a mixed type in order to build effective interaction between points of contact within the global Directory. However, those countries intending to create the first technical PoC to address the issues of detection, prevention and mitigation of computer attacks and build a national computer attack preventing system are welcome to set up a technical PoC of acoordinator-type a as a preliminary step.

Defining organizational structure

The establishment and operation of a technical PoC should be based on regulatory legal acts (legislative framework) and methodological documents formed as the framework of State function in the field of information security.

It is reasonable to legally regulate the responsibilities of all parties involved in the process to build a sustainable national system of detection, prevention and mitigation of computer attacks and computer incident response.

These parties may include a technical PoC itself, organizations providing services of detection, prevention and mitigation of computer attacks and computer incident response and the owners of IRs. One should consider to classify some as critical information infrastructure (CII) among the entire number of IRs. It is also appropriate to establish requirements for ensuring security of IRs and responsibility if failing to comply with them for the owners of CII IRs.

One should legislatively define the following provisions to ensure effective operation of a technical PoC:

1) the status of a technical PoC in the State information security system, its functions and powers;

2) the composition of other forces designed to detect, prevent and mitigate computer attacks and respond to computer incidents;

3) the procedures for informing a technical PoC on computer attacks and computer incidents, including the list of information transmitted to a technical PoC;

4) the procedures for responding to computer incidents, taking measures to mitigate computer attacks against the CII IRs;

5) the procedures for exchanging information on computer incidents among the owners of IRs, between the owners of IRs and the authorized bodies of foreign States and organizations;

6) the procedures for ensuring engagement of organizations that provide services of detection, prevention and mitigation of computer attacks and computer incident response on request of the owners of IRs, as well as the procedures for informing a technical PoC by these organizations;

7) liability for failing to comply with the established requirements and procedures.

The other forces designed to detect, prevent and mitigate computer attacks and respond to computer incidents can include, for example, departments and officials of government bodies, owners of IRs participating in these activities.

It is necessary to instruct a technical PoC to develop procedures for responding to computer incidents, for mitigating computer attacks in the State's information infrastructure, as well as procedures for exchanging information on computer attacks and computer incidents.

The procedures for informing a technical PoC on computer incidents should include:

- instruments for informing a technical PoC (for example, e-mail, telephone, special Internet portal);

- content and formats of the information provided (Appendix);

- deadlines for submission of information (for example, no later than 3 hours from the moment of computer incident detection for CII IRs, and no later than 24 hours for other IRs).

The procedures for responding to computer incidents and taking measures to mitigate computer attacks against the CII IRS can include the development of response plans by the owners of the CII IRs, including:

- technical characteristics and composition of the IRs, events (conditions) that can precede to result in implementation of measures provided by the plan;

- activities carried out during computer incident response and mitigation of computer attacks, as well as the time assigned for their implementation;

- composition of departments and officials of an IRs' owner (organization), responsible for taking measures to respond to computer incidents and mitigate computer attacks;

- conditions for engaging other forces to respond to computer incidents and take measures to mitigate computer attacks;

- the procedures for conducting training activities to practice response plan;

- the procedures for informing a technical PoC on the results of measures taken to respond to computer incidents and mitigate computer attacks.

It is very important that a technical PoC is authorized to exchange information with peer structures from other States. At the same time exchange of information on computer incidents among the owners of IRs, between the owners of IRs and the authorized bodies of foreign States and organizations should be centralized in nature to be done through the technical PoC.

In general, the national system for detecting, preventing and mitigating computer attacks and responding to computer incidents should be built in a hierarchical manner. The core of the system can be the technical PoC. The other organizations providing services in this field can follow it at the second tier. The third place is given to the owners of IRs.

Systematic interaction between the parties involved can be ensured by establishing requirements for the organizations providing services of detection, prevention and mitigation of computer attacks and computer incidents response, and ensuring control over their implementation (for example, using an accreditation mechanism).

These requirements may include:

- requirements for the organizational structure, staffing, specialist competence, existing technical infrastructure of the organization;

- requirements for the provision of information to the technical PoC on the organization’s area of responsibility (composition of IRs that are subject to measures taken to detect, prevent and mitigate computer attacks and respond to computer incidents).

It is appropriate to ban involvement of organizations that do not meet the requirements in the field of detection, prevention and mitigation of computer attacks and computer incident response invited by the owners of IRs.

The main tasks of technical PoCs include:

- detection, prevention and mitigation of computer attacks aimed at the controlled IRs;

- activities to assess protection of the controlled IRs;
- activities to determine the causes of computer incidents resulted from computer attacks against the controlled IRs;
- collection and analysis of data on the state of information security within the controlled IRs;
- interaction between computer emergency response teams;
- informing stakeholders on information security issues within the national information space of a technical PoC;
- generating and updating information on the controlled IRs.

When setting up a technical PoC, the following functions should be assigned:

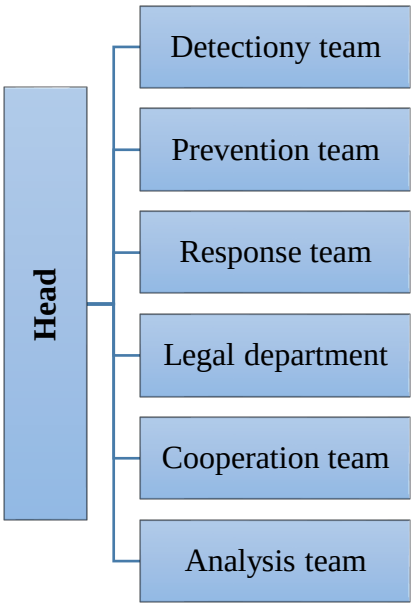
- stock-taking of IRs;
- identifying IRs' vulnerabilities;
- information security threat analysis;
- advanced training of IRs' personnel;
- receiving reports on the possible incidents from the staff and users of IRs;
- ensuring the process of detecting computer attacks;
- security event data analysis;
- registration of computer incidents;
- responding to computer incidents and its mitigating;
- identifying the causes of computer incidents;
- exchange of information on computer incidents;
- development of methodological recommendations designed for technical PoC's personnel and IRs located within the national information space;
- analysis of the results of measures to detect, prevent and mitigate incidents and evaluate their efficiency.

The technical PoC's area of responsibility is determined upon making a decision on its establishment and can be changed during its operation period.

Regulatory support for its activities is being improved throughout the operation of a technical PoC.

Technical PoC's structure:

- Head;
- Detection team collects and primarily processes events related to information security violations;
- Prevention team collects and processes information on infrastructure of the controlled IRs, vulnerabilities and software weaknesses, generates recommendations for minimizing threats to information security;
- Computer incident response team keeps records on and processes computer incidents ensuring computer incident response management and mitigation of computer attacks;



- Legal department provides legal and methodological support for technical PoC activities;
- Cooperation team organizes interaction with the national incident response centers of foreign States;
- Team for analyzing protection of infrastructure.

The main purpose of a technical PoC and the organizations controlled by a technical PoC is to ensure the protection of IRs located within the national information space from computer attacks, as well as to control recovery of normal functioning of these resources in the event of computer incidents caused by computer attacks.

Personnel qualifications

Head of technical PoC (1 person) is a technical PoC employee who manages its activities.

Lawyer (minimum 2 people) is a technical PoC employee who provides legal and regulatory support for its activities.

Technical expert (minimum 2 people) is a technical PoC employee who provides expert support in accordance with specialization (malware, use of specialized technical tools, security assessment, etc.), as well as proposal development for eliminating the causes and conditions conducive to computer incidents within the IRs.

Methodology analyst (minimum 2 people) is a technical PoC employee who analyzes information on the registered computer incidents provided by detection, prevention and response teams; analyses the possibilities of threat implementation associated with computer attacks, assesses the situation, forecasts the development of threats of computer attacks, develops recommendations for eliminating the causes and conditions for computer incidents within the IRs; develops regulatory documents and methodological recommendations for performing the functions of a technical PoC.

Security assessment specialist (minimum 2 people) is a technical PoC employee who analyzes the possibility of using detected IRs' vulnerabilities to launch computer attacks.

Computer incident response specialist (minimum 3 people) is a technical PoC employee who coordinates actions to localize, identify and mitigate a computer incident (bringing the information infrastructure to normal operation/functioning).

A specialist in identifying the causes of computer incidents (minimum 2 people) is a technical PoC employee who analyzes computer incidents in order to determine the causes of their emergency, analyzes the consequences of incidents and forms a list of computer incidents.

Specialist in interaction with staff and users (minimum 2 people) is a technical PoC employee who receives messages from staff and users of the IRs, as well as interacts with technical PoCs of foreign States.

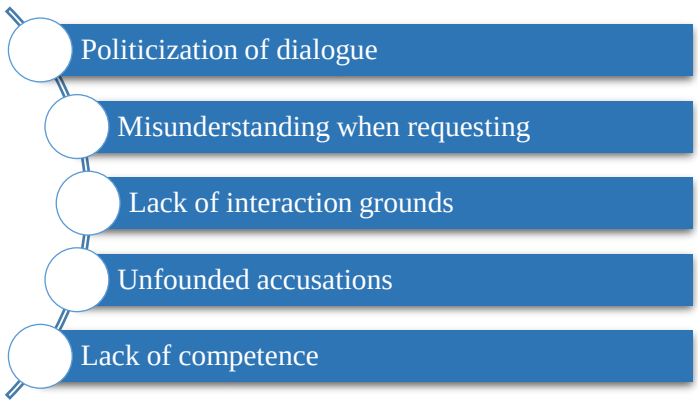
Detection specialist (minimum 2 people) is a technical PoC employee who analyzes information security events in order to detect computer attacks and incidents, as well as register computer attacks and incidents.

Responsibilities of a UN technical PoC

The technical PoCs, in line with their competence and depending on the available capacities and resources, could carry out:

- exchange of information on computer incidents within information resources under their responsibility and combating malicious activity emanating from their national information space;
- assisting other States in responding to computer incidents and detecting threats to security of information upon receipt of a corresponding request;
- exchange of data on existing and potential threats to security of and in the use of ICTs, as well as sharing best practices.

The main issues in building effective cooperation between technical bodies (usually national computer emergency response teams), apart from the politicization of dialogue, are caused by a lack of understanding, which organizations in other States are authorized to take measures to cease malicious activity emanating from the national information space.



At the same time, it should be noted that existing regional and private CERT/CSIRT networks cannot ensure representative and equal participation of all countries to address computer incident response issues due to their high politicization and unwillingness to be engaged in an open and pragmatic interaction with the technical experts from some countries.

In this regard, their solutions cannot be called universal and automatically applicable at the UN level.

Working principles of a UN technical PoC

When building interaction the participating States of the global intergovernmental PoC Directory should adhere to the following principles::

- **Communicability**

  The global intergovernmental PoC Directory should facilitate communication and interstate dialogue on security of and in the use of ICTs;

- **Neutrality**

  Regardless of the international situation, PoCs must remain politically neutral and must not be subject to sanctions;

- **Pragmatism**

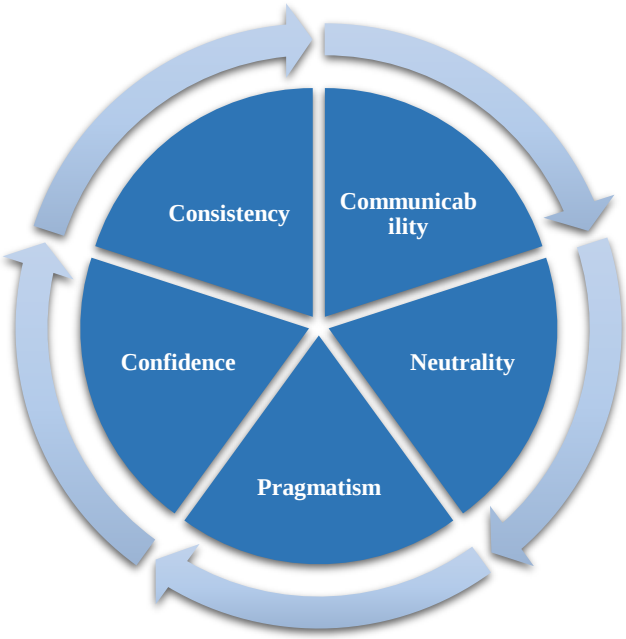
  When functioning PoCs will give preference to pragmatic interaction in order to avoid the risks of misperception, escalation and conflict that may stem from the use of ICTs;

- **Confidence**

  Information between PoCs should be exchanged in a confidential manner and can be made public only by mutual consent of all PoCs involved in such interaction;

- **Consistency**

  When functioning PoCs should take into account the recommendations of the OEWG and relevant UNGA resolutions.



Interaction between UN PoCs

The UN global intergovernmental PoC Directory plays a key role in consolidating existing directories at the regional and subregional levels and connecting new PoCs of other states.

The global intergovernmental PoC Directory is based on the necessary practices of these organizations, taking into account regional specifics. Thus, if interaction is planned to be carried out between States of the same regional organization, these States can cooperate both through the global intergovernmental PoC Directory and through the directory of a regional organization which they belong to. If interaction is supposed to take place between States from different regional organizations, as well as if one or both States are not members of any regional or subregional organization, they can cooperate through the global intergovernmental PoC Directory.

The diplomatic and technical PoCs are expected to have differentiated roles. Accordingly, diplomatic POCs would communicate with other diplomatic POCs and technical POCs would communicate with other technical PoCs. At the same time, if necessary, coordination between PoCs from the same State is ensured.

Exchange of information should be voluntary and in line with the respective domestic circumstances, requirements and legislation of the States involved. Any subsequent cooperation and/or information sharing, including the channel through which relevant communication would take place, would proceed according to mutual agreement. Initial acknowledgement of receipt of a communication does not imply agreement with the information contained therein nor prejudice the position of the responding State, nor does it prejudge any communication that may follow. Additionally, notifying a State that its territory is being used for a wrongful act does not, of itself, imply that it is responsible for the act.

Technical PoCs may use standardized procedures for interaction with other points of contact.

As an initial step to facilitate communication PoCs may consider using, on a voluntary basis, the Procedure for inquiry and the Procedure for responding to an inquiry contained in the second annual progress report;

Interaction between technical PoCs is set to establish the technical details of computer incidents through sending a request to the technical PoC of the UN Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs has been detected.

To mitigate the risks of misperception, escalation and conflict that may arise from the use of ICTs, the sequence of actions of UN Member States whose information infrastructure is maliciously affected includes two basic scenarios:

- malicious activity with the use of ICTs has not led to the risks of misperception, escalation and conflict, interstate interaction is carried out on a daily basis;
- malicious activity with the use of ICTs has caused tension in interstate relations, there is a risk of misperception, escalation and conflicts:

Technical – technical PoCs interaction

The technical PoC of the UN Member State whose information infrastructure is maliciously affected evaluates a computer attack / a computer incident at the national level and collects all necessary information available for transmission.

A list of comprehensive information necessary to study computer attack or computer incident is contained in Appendix.

Information is transmitted by e-mail and/or any other mean agreed upon by the involved PoCs.

Information, as comprehensive as possible, is transmitted to the technical PoC of the UN Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs has been detected.

Upon receipt of information, the technical PoC of the UN Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs has been detected:

- notifies the requesting side of its receipt as soon as possible, but no later than in 72 hours, and also evaluates the correctness and completeness of the data provided with the possibility of further clarification;
- if any measures need to be taken, informs of expected deadlines for their implementation;
- forwards information about the results of the measures taken to the requesting side.

Technical – diplomatic PoCs interaction

If there are objective reasons that impede interaction through technical PoCs, a UN Member State whose information infrastructure is maliciously affected evaluates the computer attack / computer incident at the national level and collects all the necessary information available for transmission.

The technical PoC of the Member State whose information infrastructure is maliciously affected sends as detailed information as possible to the national diplomatic PoC for subsequent transmission to the diplomatic PoC of the UN Member State from whose territory, as the requesting side assumes, malicious activity with the use of ICTs was detected.

Upon receipt of information, the diplomatic PoC of the Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs was detected notifies the sender of its receipt as soon as possible and promptly transmits the relevant information to national authorized bodies.

Having received information on the implementation of the necessary measures and other relevant information, the diplomatic PoC of the Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs was detected, forwards the relevant information to the requesting side.

Diplomatic – diplomatic PoCs interaction

A UN Member State whose information infrastructure is maliciously affected assesses computer attack / computer incident at the national level and collects all necessary information available for transmission.

The diplomatic PoC of the Member State whose information infrastructure is maliciously affected sends information as detailed as possible to the diplomatic PoC of the UN Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs was detected.

Upon receipt of information, the diplomatic PoC of the Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs was detected notifies the requesting side of the receipt as soon as possible and promptly transmits the relevant information to national authorized bodies, taking into account that the response time to the request should not exceed 15 days from the date of its receipt.

Upon receipt of information on the implementation of the necessary measures and other relevant information, the diplomatic PoC of the Member State from whose territory, as the requesting side assumes, the malicious activity with the use of ICTs was detected shall forward the relevant information to the sender.

At the same time UN Member States should take into account that a conclusion on the involvement in malicious activity with the use of ICTs should be based on objective verifiable information. UN Member States will endeavour to take appropriate steps to reduce the likelihood of misperceptions and the potential for conflict or political or military tension stemming from the use of ICTs.

A general recommendation for the sequence of actions in the event of a malicious activity is that the discussion of a computer incident should raise to the level of the diplomatic PoCs or national security and policy coordination bodies if all previous steps have failed.

Conclusion

This Document is intended to provide basic guidance on how to set up a technical PoC by UN Member States. It is not a comprehensive document and should not be regarded as a one-stop guide to action. Further interaction on the described issues, in case of interest, can be carried out on a bilateral basis.

Appendix. List of basic information required to study a computer attack and computer incident (template)

The working language of requests may be specified by participating States of the exchange.

Lack of information on the further mentioned items is explicitly indicated.

Computer attack notification (CA)

1. Information on CA.
    - 1.1. Restrictive indicator of information disclosure contained in CA Notification according to the Traffic Light Protocol (TLP):
        - 1.1.1. TLP: WHITE – «disclosure» is not limited;
        - 1.1.2. TLP: GREEN – «disclosure» is limited to the competent authorities, which are not engaged in responding to CA;
        - 1.1.3. TLP: AMBER – «disclosure» is limited only to the competent authorities, which are engaged in responding to CA;
        - 1.1.4. TLP: RED – information is limited to recipient only.
    - 1.2. Description of the information security event.
    - 1.3. The measures expected of the addressee State.
2. The name of information resource (IR) targeted by the CA.
3. Category and type of CA.
    - 3.1. Breach or slowing down IR's availability
        - 3.1.1. Denial-of-service (DoS) attack aimed at IR;
        - 3.1.2. Distributed Denial-of-Service (DDoS) attack aimed at IR.
    - 3.2. ICT-assisted information gathering
        - 3.2.1. IR scanning;
        - 3.2.2. IR traffic hijacking;
        - 3.2.3. Social engineering, aimed at compromising IR.
    - 3.3. IR intrusion attempts
        - 3.3.1. Exploit attempts;
        - 3.3.2. Login attempts.
    - 3.4. Malware distribution

3.4.1. Malware infection attempt;

3.4.2. Malware C&C;

3.4.3. Malware infrastructure.

3.5. Fraud

3.5.1. Phishing.

3.6. Abusive content

3.6.1. Spam.

3.7. Other (CA which do not fall into any of the given categories).

4. Date and time of CA starting (UTC+0).
5. Date and time of CA ending (UTC+0).
6. Technical data on the targeted IR
   6.1. IPv4-address of IR
   6.2. IPv6-address of IR
   6.3. IR's IP route subnet addresses (in the CIDR format)
   6.4. IR-associated domain name
   6.5. IR's URI address
   6.6. IR-registered e-mail address
   6.7. Attacked Autonomous System Number (ASN)
   6.8. Attacked network service, network port and protocol
   6.9. Exploitable vulnerabilities
7. Technical data on CA source
   7.1. IPv4-address (routable)
   7.2. IPv6-address (routable)
   7.3. Domain name associated with CA source
   7.4. URI-address
   7.5. Email-address
   7.6. Malicious Autonomous System Number (ASN)
   7.7. Information on malware modules

7.7.1. Hash value of the malware module;

7.7.2. Antivirus software verdict, name of the relevant antivirus software (if the malware module is identified).

8. Additional information on CA, including CA network traffic, malware modules, electronic images of e-mails, log files of the attacked network services, log files of the information protection tools, log files of the telecommunications equipment, etc.
9. Information referring CA to the addressee State.

Computer incident (CI) notification

1. Information on CI.
   1.1. Restrictive indicator of information disclosure contained in CI Notification according to the Traffic Light Protocol (TLP):
      1.1.1. TLP: WHITE – «disclosure» is not limited;
      1.1.2. TLP: GREEN – «disclosure» is limited to the competent authorities, which are not engaged in responding to CI;
      1.1.3. TLP: AMBER – «disclosure» is limited only to the competent authorities, which are engaged in responding to CI;
      1.1.4. TLP: RED – information is limited to recipient only.
   1.2. Description of the information security event.
   1.3. The measures expected of the addressee State.
2. Name of information resource (IR).
3. Category and type of CI.
   3.1. Dissemination of abusive content
      3.1.1. Spam-bombing from the IR.
   3.2. Breach or slowing down IR's availability
      3.2.1. Denial-of-Service (DoS) attack aimed at IR;
      3.2.2. Distributed Denial-of-Service (DDoS) attack aimed at IR.
      3.2.3. IR traffic hijacking.
   3.3. ICT-assisted fraud
      3.3.1. Use of IR for unauthorized purposes;

3.3.2. Phishing.

3.4. Breach of information content security

3.4.1. Unauthorized access to the IR-processed information;

3.4.2. Unauthorized modification of the IR-processed information.

3.5. System intrusion

3.5.1. IR's application compromise;

3.5.2. IR's account compromise.

3.6. Malware infection

3.6.1. Infection of the IR with malware modules.

3.7. Malware distribution

3.7.1. Use of IR for malware command and control;

3.7.2. Use of IR for malware distribution.

3.8. Other (CI which do not fall into any of the given categories)

4. Date and time of CI identification (UTC+0).

5. Technical data on the IR engaged in CI.

5.1. IPv4-address (routable) of IR

5.2. IPv6-address (routable) of IR

5.3. Subnet of the IR (in the CIDR format)

5.4. Domain name associated with IR

5.5. URI-address

5.6. Registered e-mail address

5.7. Attacked Autonomous System Number (ASN)

5.8. Attacked network service, network port and protocol

5.9. Exploitable vulnerabilities

6. Technical data on the source of malicious activity, involved in CI, from the Internet segment of the addressee State.

6.1. IPv4-address (routable)

6.2. IPv6-address (routable)

6.3. Subnet of the routable network addresses (in the CIDR format) involving the sources of malicious activity

6.4. Domain name associated with the malicious activity source

6.5. URI-address

6.6. Email-address

6.7. Malicious Autonomous System Number (ASN)

6.8. Information on malware modules

6.8.1. Hash value of the malware module;

6.8.2. Antivirus software verdict, name of the relevant antivirus software (if the malware module is identified).

7. Additional information on computer incident, including the records of network traffic of malicious activity, malware modules, electronic images of e-mails, log files of the targeted network services, log files of the information protection tools, log files of the telecommunication equipment, etc.